Secure Drag&Drop Key Exchange
Christian Rohner, Henrik Andersson, Ioana Ungurean

The problem in key-exchange is how to do authentic transport of key material from one device to another. The transportation should also be intuitive and easily understandable for a non-expert user and it should involve as little interaction as possible from the user.

Our approach is to "drag&drop" key material from one device to the other.

This approach is also suitable for small devices that don’t have display or keyboard.

Visual codes can be used as authentic channel:

We use the visual codes for representing the bluetooth addresses of the devices. For the future the public keys could be coded.

We have transformed an insecure channel between the devices A and B in an authentic channel, A→B, by using the visual channels A→SM and B→SM, and the channel SM→B, which we make authentic by asking B to confirm that he trusts SM.

Legend:
P K - public key
Addr - bluetooth address
A - the device that owns the PK
B - the device that will get the PK
SM - security manager, transports the keys

B*→SM not relevant. SM*→B: checking that message comes from SM on dialogue (?). Trust cannot generate authenticity on a channel, but it allows to combine two authentic channels into an authentic channel.