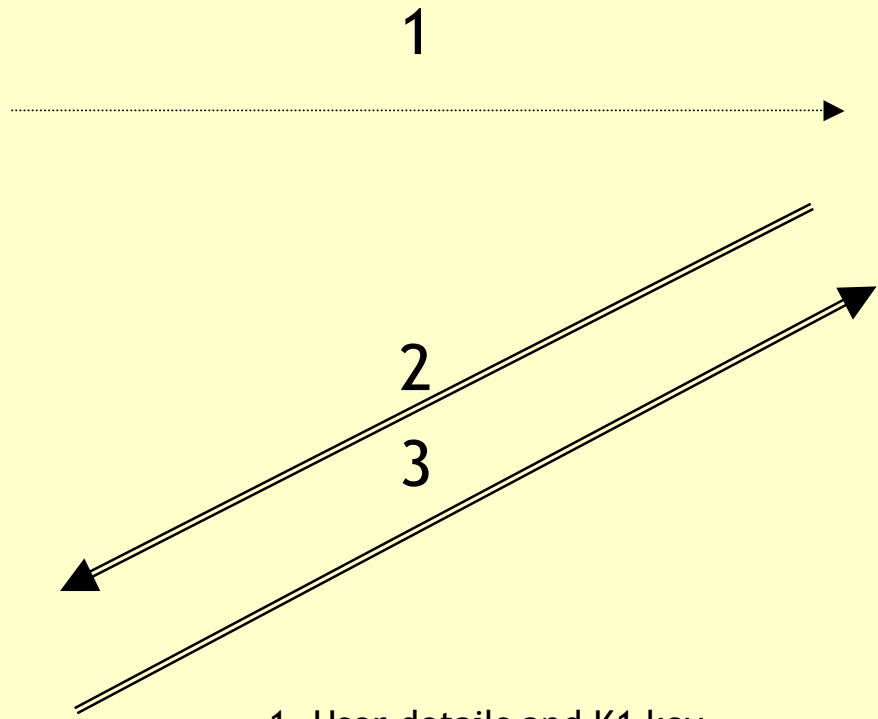


Some ways to apply Diversid Authentication Procedure

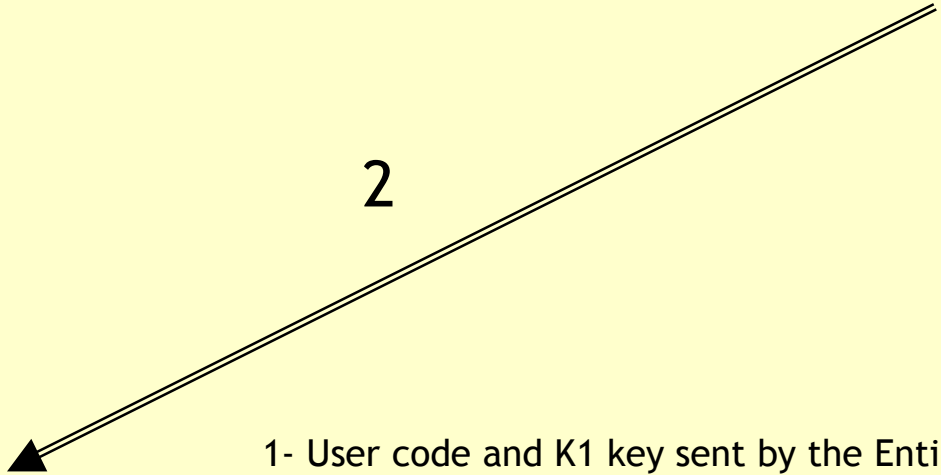
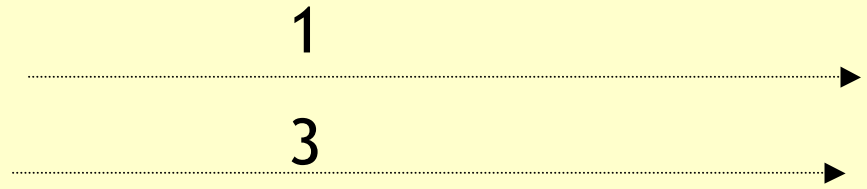
System registered under Patent # 02748876.6

Authentication when accessing an internet portal by entering K1 at the portal



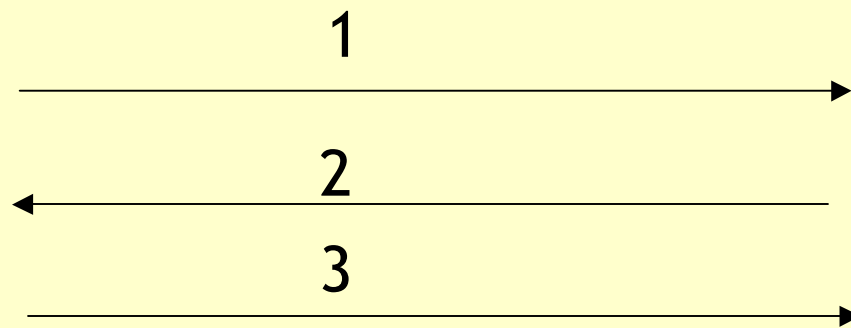
- 1- User details and K1 key
- 2- K2 key asking for access request confirmation
- 3- K3 key and, if OK, authorization to access the operations

Authentication when accessing an internet portal by entering K1 and K3 at the portal



- 1- User code and K1 key sent by the Entity
- 2- The mobile receives K2 key and confirms the match; then presents K3
- 3- Visualization of K3; user enters K3 key at the portal

Authentication when accessing an internet portal by entering K1, K2 y K3 at the portal

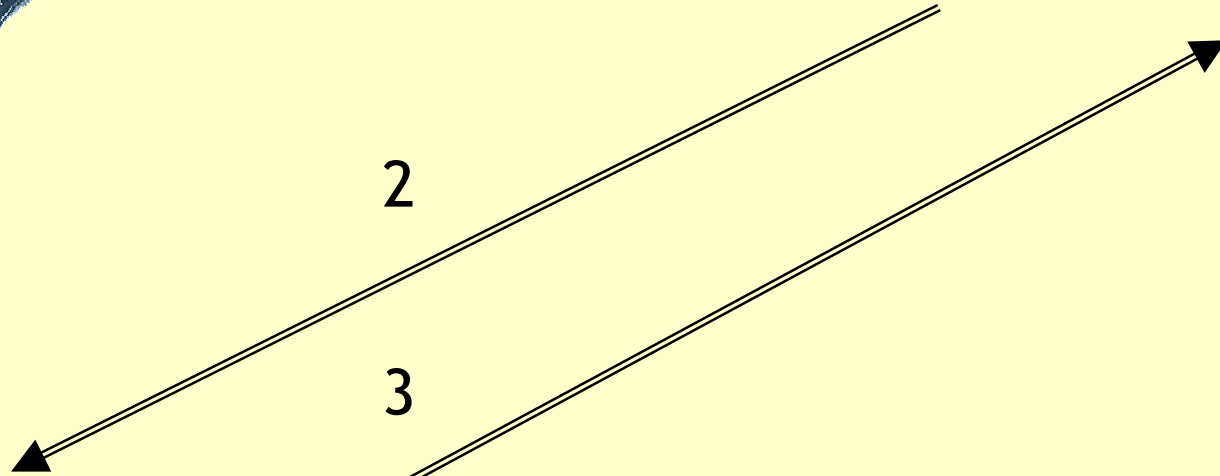
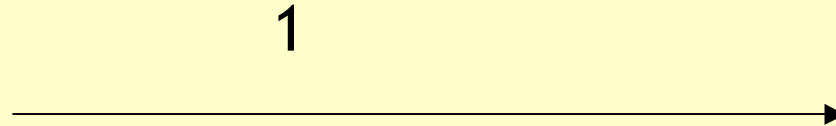


- 1- User enters code and K1 key and sends them to the Entity
- 2- Entity receives K1 key and confirms match; then sends K2
- 3- User checks K2 and enters K3 key at the portal

Authentication when paying at e-commerce with a credit card by entering K1

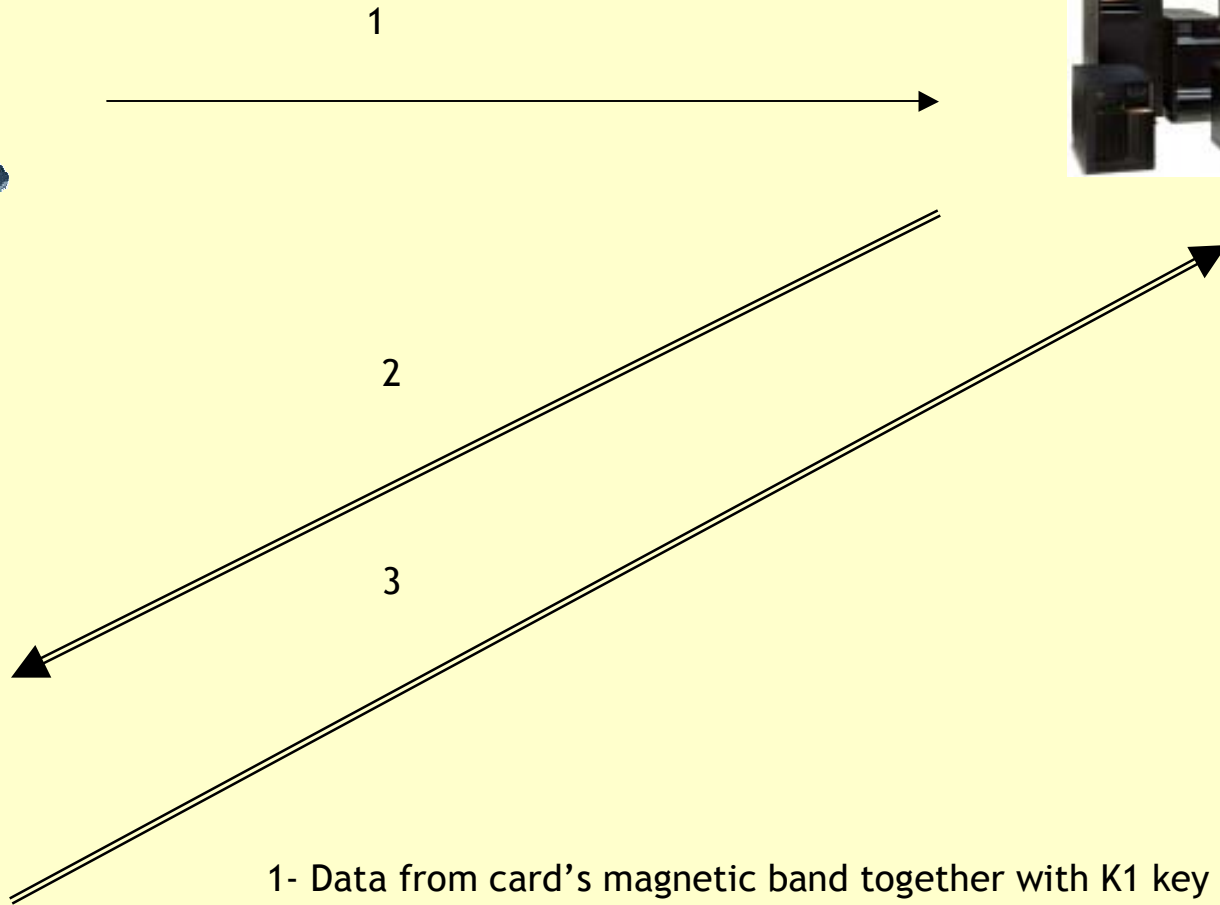


E-commerce's virtual PoS



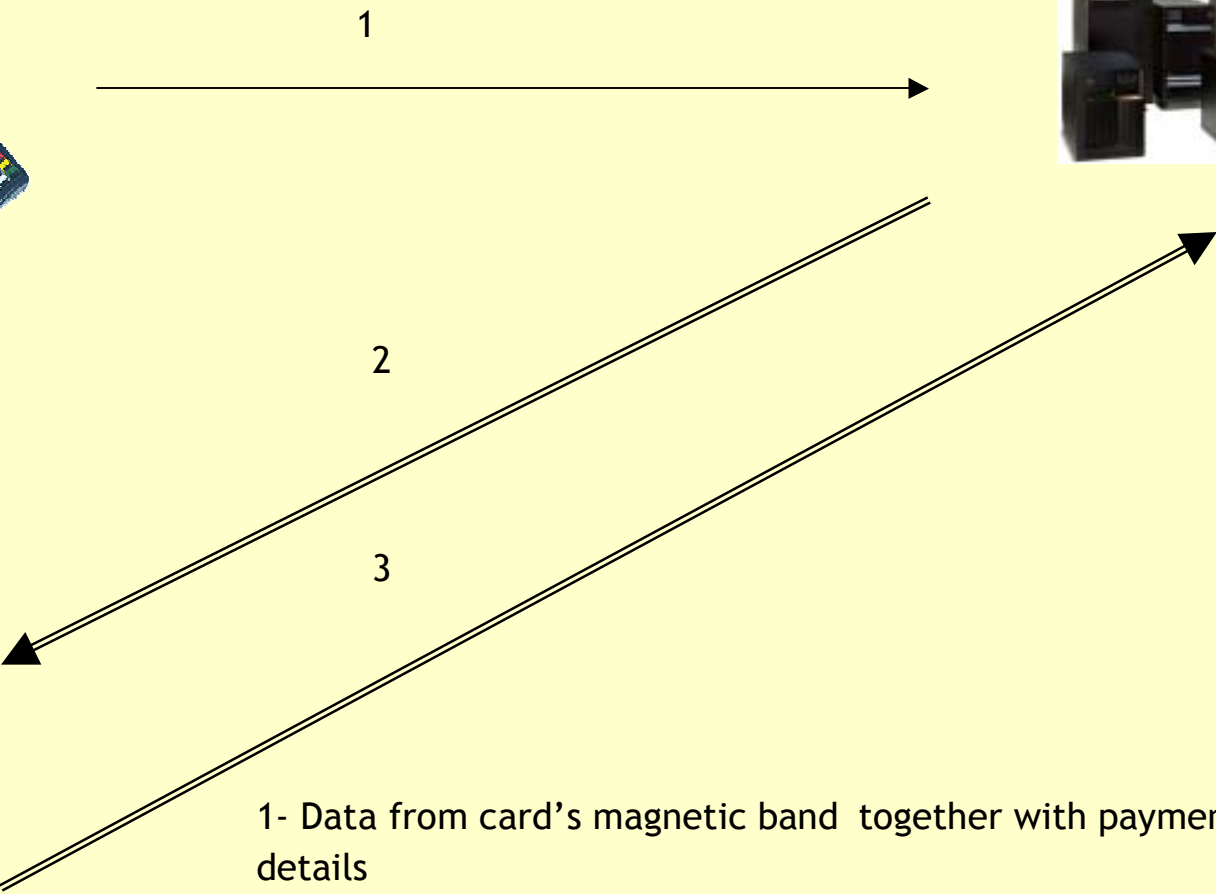
- 1- Card number plus K1 key and payment details
- 2- K2 key together with operation details
- 3- Operation details, K3 key and OK

Authentication when paying at e-commerce from a PoS by entering K1



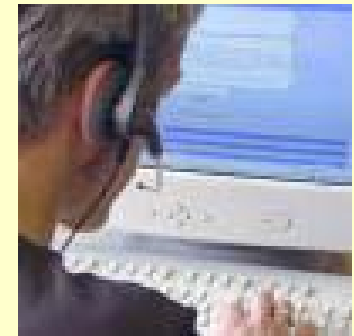
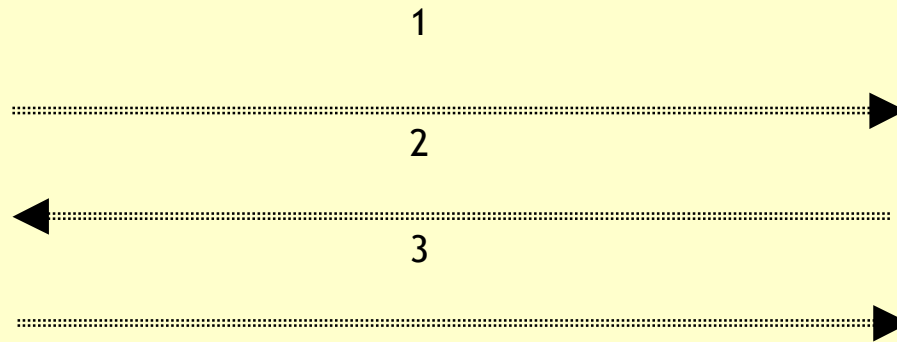
- 1- Data from card's magnetic band together with K1 key and payment details
- 2- K2 key together with operation details
- 3- Operation details with K3 key and OK

Authentication when paying at e-commerce from a PoS without entering any keys



- 1- Data from card's magnetic band together with payment details
 - 2- K1 key together with operation details
 - 3- Operation details and K2 key
- Messages 2 and 3 will be sent encrypted with K3 key

Authentication for telephone operations



- 1- User number and K1
- 2- K2 key (K1's pair)
- 3- Operation to perform and K3 key