PAKE protocol not implemented correctly

Shared secret is computed without the use of the protocol transcript

The implementation does not protect against small subgroup attacks

Newer draft of the protocol should be used

Correct applet code execution order is not ensured

APDU commands execution on the card is not automata based

Some commands have certain prerequisities, e. g. the PAKE protocol

Possible attack vector: misuse can lead to exception or leak of secrets

Lacking failure checks

Checksum of stored secrets should be validated at each startup

Applet keeps running even with wrong PIN, resulting in exchange of incorrect messages.

Possible attack vector: misuse can lead to exception or a leak of secrets

Thanks for your work

IMRO & DANIEL