Designing and proving an EMV-compliant payment protocol for mobile devices

https://hal.inria.fr/hal-01408584/document

We devise a payment protocol that can be securely used on mobile devices, even infected by malicious applications. Our protocol only requires a light use of Secure Elements, which significantly simplify certification procedures and protocol maintenance. It is also fully compatible with the EMV SDA protocol and allows off-line payments for the users. We provide a formal model and full security proofs of our protocol using the TAMARIN prover.