Application of Public Key Infrastructure to Smart Card for Blockchain Applications

Sebastien Armleder
sebastien.armleder@cryptnox.ch
www.cryptnox.com

Abstract. A smart card to be used for digital signatures is described. The smart card is factory set up with a unique identification number and digital certificate. The smart card is then associated with a user by a certification authority after successful verification of the identity of the user. Details that help in identifying the user are also transferred to the smart card by the certification authority. The smart card can then be used by the user to digitally sign documents. The smart card allows performing digital signatures with personal identification with an adjustable level of anonymity, traceability, and user-friendly private key management. It can also allow a robust, secure, and simple interaction with a blockchain.

1. Introduction

Digital transactions have been on the rise over the last decade. They comprise not only traditional transactions for purchases made over e-commerce website but also those made with cryptocurrencies. In the context of the latter, it is noteworthy that each transaction is recorded in a blockchain and contains details of the transaction including details that can help identify the participants of the transaction. This may be accomplished by each of the participants digitally signing the transaction using their own, unique signature. This signature can be generated using, for example, private keys held by the participants and can be verified using public keys corresponding to the private keys held by the participants. Storing the private keys securely, however, can be a problem. It may be preferable to not store them in an easy to read or copy format. Similarly, it should be possible to easily retrieve a copy of the key or regenerate it in case it gets lost. A device that allows key management is described here. It allows user-friendly key management and provides a secure, and forgery-proof method to perform digital signatures using the device. Further, it allows easy regeneration of a new private key after successful authentication of the user by a certification authority in case of theft or loss.

2. Solution

The solution we propose relates to a smart card that its setup and initialized in a particular manner to allow personal identification of the user of the smart card with adjustable level of anonymity, traceability and user-friendly key management. The solution therefore allows robust, secure, and simple interaction with a blockchain.

2.1 Setup

The proposed technology includes a factory setup for a smart card. The setup protocol is depicted in Fig. 1 and consists of a random number generator RNG generating a random serial number SN inside the secure element SE of the smart card. A first pair of asymmetric cryptographic keys, consisting of a private key K_{priv} and a public key K_{pub}, is also generated inside the secure element SE.

Next, the serial number SN and the public key K_{pub} are used to certify the authenticity of the smart card, by means of a factory certification. The generated serial number and SN public key K_{pub} along with a digital signing request SR are sent to a certification server. The certification server then generates and digitally signs a digital certificate CCERT that certifies the authenticity of the smart card. The digital certificate can be an X509 digital certificate signed by the root certificate of the certification server. It contains (in an encrypted form) the serial number SN and the public key K_{pub} from the smart card and potentially other identifying information about the smart card. This digital certificate CCERT is then sent to the smart card.

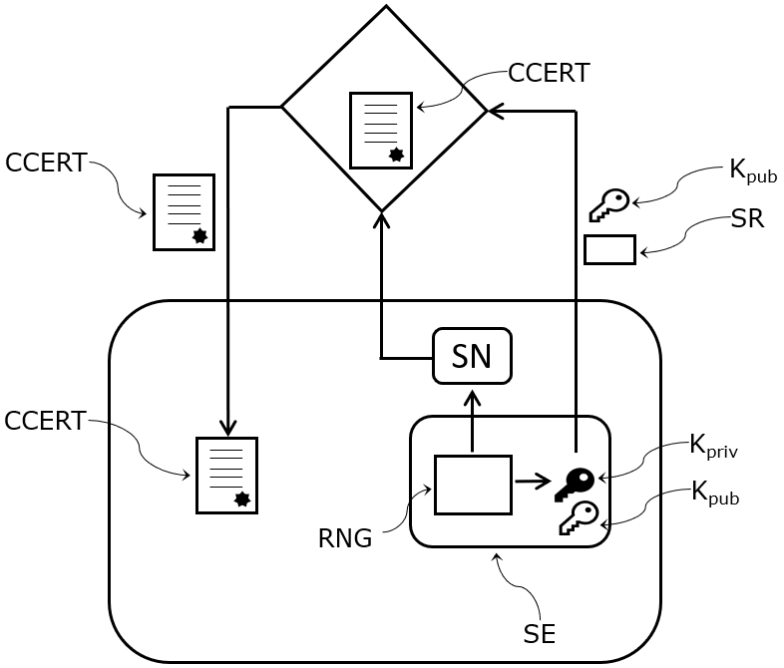

Fig. 1: Setting up the smart card

With the aid of the digital certificate CCERT and the unique random number SN generated inside the secure element SE, the smart card becomes robust against forgery. These steps complete a factory setup of the smart card.

2.2 Initialization

After the factory setup, the smart card is ready to be associated with a user. In order to enhance security, the smart card is initialized for a particular user USR using an initialization protocol.

The initial steps of this initialization protocol are depicted in Fig. 2. The first step of this initialization protocol consists in the identity of the user USR being verified by a certification authority CAUTH. The user USR provides personal data UDAT such as a social security number, or another identification number, to the certification authority CAUTH for verification.

Upon successful verification of the identity of user USR, the certification authority CAUTH generates a pair of keys – a public key CK_{pub} (also referred to as certificate public key) and a private key CK_{priv} (also referred to as certificate private key). Any suitable asymmetric cryptographic key generation algorithm can be used to generate this pair of keys. Next, the digital certificate CCERT is obtained from the smart card. The certification authority CAUTH uses the digital certificate CCERT together with the public key CK_{pub} and the user data UDAT to generate a digital signing request CREQ.

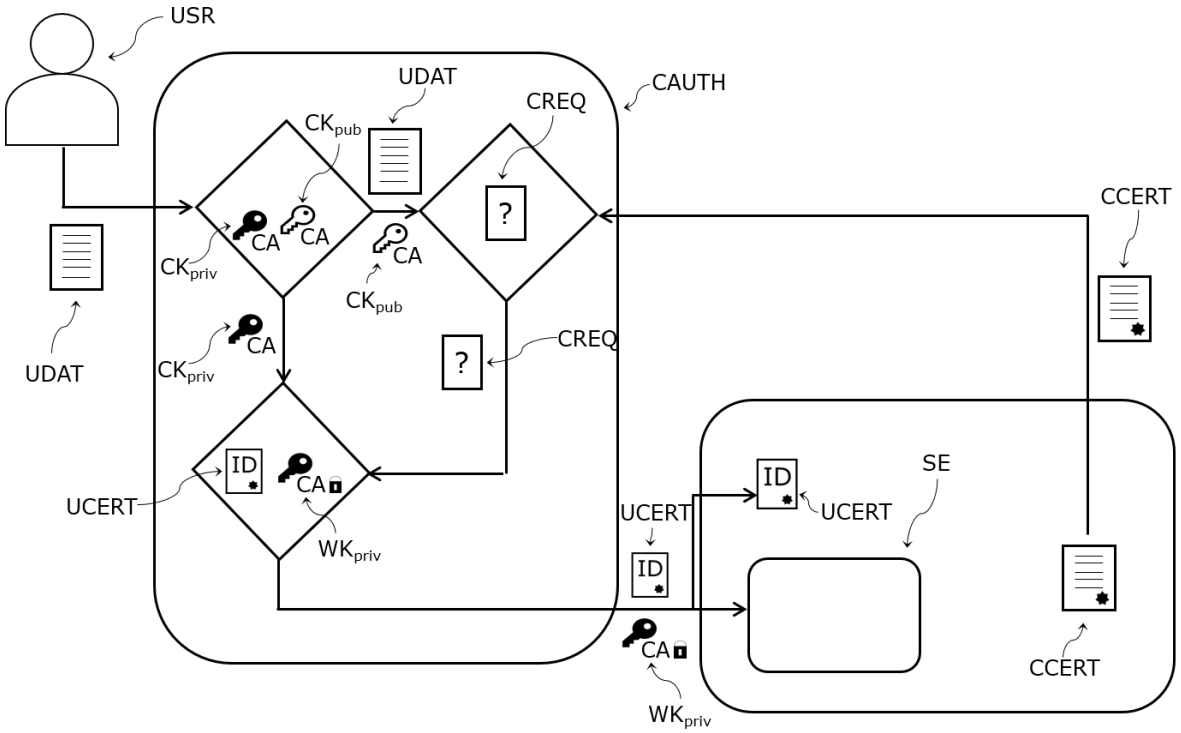

Fig. 2: Authentication of user

The digital signing request CREQ is used to generate a digital certificate UCERT establishing ownership of the smart card by the user USR as follows. After generation of the digital signing request CREQ, the certification authority CAUTH verifies the authenticity of the digital certificate CCERT obtained from the smart card. If the verification is successful, the certification authority CAUTH generates the digital certificate UCERT with the help of the public key CK_{pub}. The digital certificate UCERT may include the user identification data UDAT, the public key CK_{pub}, and the digital certificate CCERT. Each of these can also be encrypted appropriately for storage on the digital certificate UCERT.

The final step of the initialization protocol consists in sending the digital certificate UCERT and the wrapped private key CK_{priv} to the smart card. CK_{priv} needs is wrapped (i.e., encrypted) before it is transferred to the smart card for greater security. The encryption is carried out using the public key K_{pub} generated by the smart card. K_{pub} is contained in the digital certificate CCERT and so, also in the signing request CREQ. Thus, a wrapped private key WK_{priv} is also generated. Finally, the wrapped private key WK_{priv} and the digital certificate UCERT are sent to the smart card, wherein the wrapped private key WKpriv is sent to the secure element SE of the smart card.

The further processing inside the secure element SE is depicted in Fig. 3. Using the private key K_{priv} corresponding to the public key K_{pub} already present in the secure element SE of the smart card, the wrapped private key WK_{priv} is unwrapped to reveal the private key CK_{priv}. Then, based on the private key CK_{priv} received from the certification authority CAUTH, a random seed SEED is generated inside the secure element SE of the smart card. The seed SEED can be generated using an SHA256 or AES encryption algorithm. This seed may be used to digitally sign transactions using the smart card.

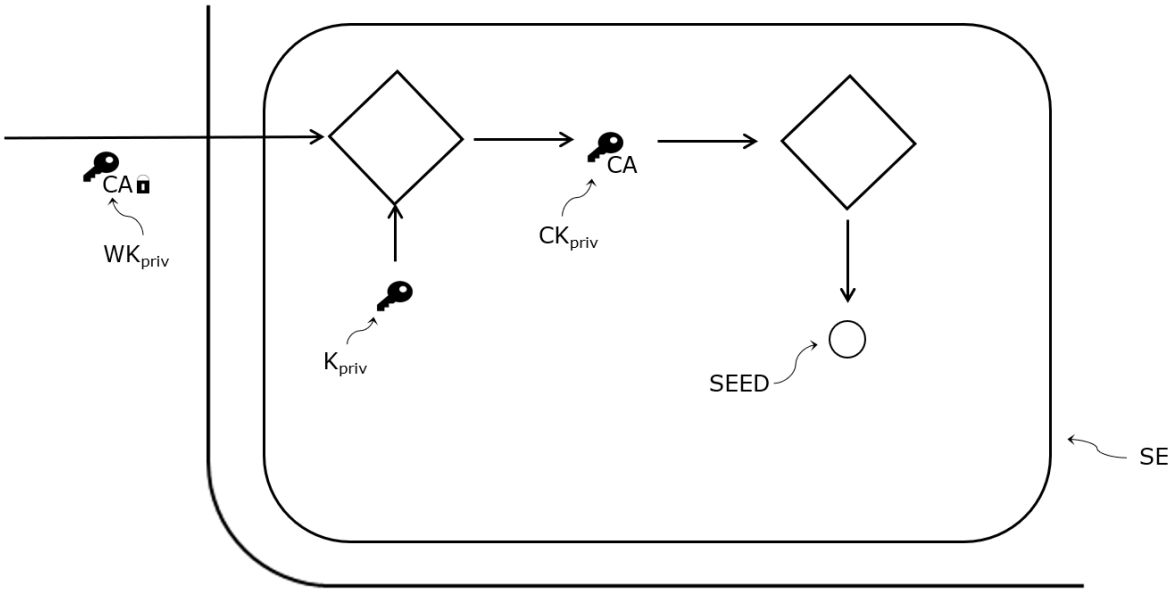

Fig. 3: Initialization of the smart card for a particular user

Thus, the smart card is set up initially with its own security features (digital certificate CCERT and unique serial number SN) and only after it is successfully set up, can it be associated with a user USR. The digital certificate UCERT and the private key CK_{priv} further serve to ensure the authenticity of the smart card and the user. At this stage, the secure element SE of the smart card contains the private key K_{priv} generated inside it, the private key CK_{priv} provided by the certification authority CAUTH, and the random seed SEED generated inside the smart card

using the private key CK_{priv} provided by the certification authority CAUTH, and the smart card is ready for digital signing.

2.3 Digital Signing

Fig. 4 depicts the process of digital signature using the smart card. A signing request SREQ is sent to the smart card. The signing request SREQ is transferred to the secure element SE of the smart card where a signature SSIGN is generated based on the request SREQ and the random seed SEED generated inside the smart card. Additionally, a certificate signature CSIGN based on the certificate private key CK_{priv} and the signature SSIGN, and a signature KSIGN based on the private key K_{priv} and the signature SSIGN are generated. All three signatures, SSIGN, CSIGN, and KSIGN are then output from the smart card and serve as the digital signature from the smart card.

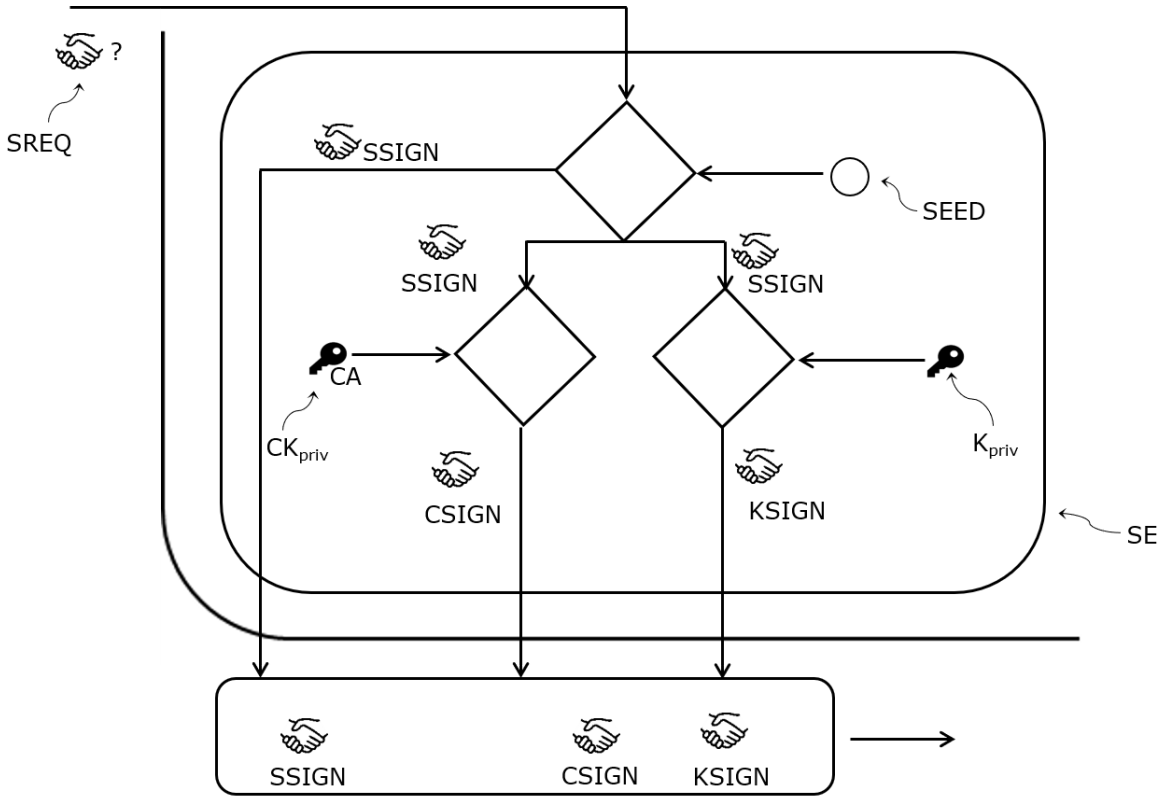

Fig. 4: Digital signature using the smart card

Because of the dependence of SSIGN on the random seed SEED, that in turn depends on a successful verification of the user USR by the certification authority CAUTH, and the dependence of the two other signatures CSIGN and KSIGN on successful authentication by the certification authority CAUTH and successful factory set up respectively, the smart card provides a robust, secure, and traceable method to enable digital signatures.

3. Conclusion

The smart card presented here thus combines within a secure element of a smart card various secrets with strictly limited computation possibilities. It is centered around fundamental concepts of public key infrastructure such as X509 digital certificates and certificate authorities. Moreover, the concepts presented here can be easily extended to secure elements belonging to other devices such as NFC smart cards. The technology described here can be applied to diverse areas such as whitelisting applications, identification, seed recovery, signing of blockchain transactions, and lost or stolen card identification. Thus, it provides an easy, secure, user-friendly solution for identification that is robust to forgery or hacking.