Java-applet support for cryptographic authentication of transactions with EMV-application smart cards

Purpose
The Crypto applet allows you to perform cryptographic functions, necessary for the authorization of transactions with EMV-application smart cards. The crypto applet provides secure storage of the issuer center’s cryptographic keys and performs cryptographic functions of symmetric cryptography (Triple DES) of the issuers center and EMV-application smart cards as well as an asymmetric cryptography function (RSA) of the POS-terminal.

In the EMV-application smart card transaction authorization part, the functionality of the crypto applet is similar to high-performance cryptographic adapters (Eracom, Thales e-Security, etc.).
**Functionality**

The crypto applet supports both symmetrical (Triple DES), and asymmetrical (RSA) cryptography operations, and convolutions calculation (Digest).

**Symmetrical cryptography**

- Loading 3DES-key at simultaneously or component wise;
- Diversification of the card’s 3DES-key and get its encrypted value;
- Diversification of the operation’s 3DES-key;
- 3DES-encryption/decryption (ECD,CBC);
- Verification code messages calculation (MAC) or cryptograms based on 3DES-encryption (MAC4/MAC8).

**Asymmetrical cryptography**

- Loading secret (private) RSA-key (2 or 5 components) in encrypted form;
- Loading open (public) RSA-key;
- Generates a pair of two or five componential secret (private) RSA-key;
- Получение значения открытого RSA-ключа;
- Getting the secret value of two or five componential RSA-key (of the card or issuer) in encrypted form;
- Encryption/decryption of the RSA-key certificate.

**Convolutions calculation (Digest)**

- Calculation of hash-function SHA-1.

---

**Advantages of the solution and sphere of use.**

| Wide range of opportunities at a low price | The cost of Java-applet crypto card is twice the price cheaper of the high -performance cryptographic equipment. Run-time cryptographic functions in the Java-applet are greater than the crypto adapter, which is not critical to operations not requiring mass card servicing. Due to its low price and wide functionality, the Java-applet crypto card can have a variety of use, but it is most often used to test the quality of personalized EMV-cards with the help of EMV Insight 2. |
| Security | Along with Java-card security arrangement, the applet has the built in two-level security arrangement providing authorized access to its functions. |
| Integrability | The crypto applet is run from an external application using the APDU-commands. Loading and managing cryptographic keys is performed using CA_DKL. Performance of cryptographic functions authorize transactions carried out under the control of EMV Insight 2. |
Modes and function terms

Interacting with the crypto applet is possible in two modes: administrative and application. Application mode is designed to perform cryptographic authorization procedures. It is accessed by an application access password. Administrative mode is designed to load and manage cryptographic keys. Performance of administrative functions is possible only after the entering the administrative password.

Crypto applet is loaded into the smart card, with the compliance of JavaCard 2.1 API specifications. Supported length and format of the secret asymmetric keys depend on the specific Java-card API implementation used. The functionality of the crypto applet does not depend on the type of Java-card.

Working with symmetric and asymmetric keys

Symmetric keys

Symmetric keys are combined into groups that are identified by the index of DKI (Derivation Key Index) in the range from 0 to 0xFE.

Крипто апплет позволяет различным смарт-карт приложениям использовать различные значения ключей с одинаковыми DKI в рамках одного приложения.

Asymmetric keys

Asymmetric RSA-keys can be one of the three types:

• Open - open, 2-component RSA-key;
• Secret 2-component - the secret RSA-key format view: base (modulus) and the degree of (exponent);
• Secret 5-component - a secret RSA-key presented in the following formats: P, Q, DP, DQ, PQ.

Asymmetric keys are in groups that are identified by the index of PKI (Public Key Index) in the range of 1 to 99. The same index key PKI can be used for different payment systems, but have different values. Identification of the payment system to which the key is carried out by using an identifier RID (Registered Application Provider Identifier). Thus, to uniquely identify a key, you must specify three parameters: the RID identification, the index of PKI and the key type.

Related software

| CA_DKL | Uploading the 3DES- and RSA-key into the crypto applet. |