EKRAN®

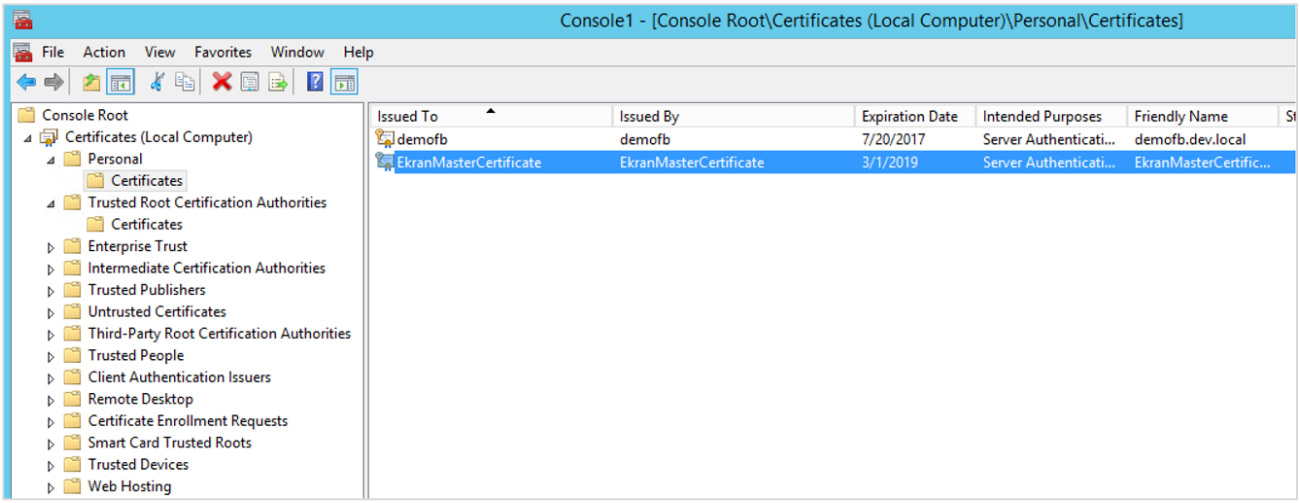
Ekran System

Encryption

Ekran System Encryption

General Information

On the first start, the Ekran System Server generates the Ekran Master Certificate and saves it to the Certificate Storage of Windows. The Ekran Master Certificate is the unique RSA-2048 Certificate without which Ekran System cannot get other keys and read encrypted data. If you need to move the database, you have to back up, import or export the Ekran Master Certificate. For more information, see the Ekran System Help File.



On the Server side, the encryption is implemented with Microsoft .Net framework. On the Client side, the encryption is implemented with Crypto++. All encryption algorithms use FIPS 140-2 certified encryption implementations.

Monitoring Results Encryption

Binary data (screenshots created during monitoring) is encrypted with AES-256. AES key is randomly generated for every binary file, and then it is encrypted with the public key of the Ekran Master Certificate. The encrypted AES key is attached to the encrypted binary data. The public key for encryption is extracted from the certificate and stored in the Client registry.

To decrypt the data, the AES key should be decrypted with the private key of the Ekran Master Certificate. Then the original data should be decrypted with AES key. On the Client side, the data is encrypted during its creation and decrypted by the Server when the authorized Ekran user views it via Management Tool.

The **logged keystrokes** are encrypted in the MS SQL database and the PostgreSQL database. The Symmetric key, which is stored in the database, is password-protected. The password is encrypted with the Ekran Master Certificate.

Connection Encryption

Client and Ekran Server connection is encrypted with AES-256. The key generation is based on the Deffie-Hellman key exchange algorithm. The encryption is implemented with Crypto++ 5.6.1.

Ekran Server and Management Tool establish TCP connection encrypted with the self-signed certificate. The encryption is implemented with WCF .NET.

Access to **Management Tool** is established over the encrypted HTTPS connection. The certificate is defined before the Management Tool installation. For more information, see the Ekran System Deployment Guide.

Connection string of database is stored in the registry. It is encrypted with Ekran Master Certificate.

Encryption of Other Data

The **initial vectors for the time-based one-time passwords** (**TOTP)** are encrypted in the database with the Ekran Master Certificate.

The Ekran System **internal users' passwords** are stored as SHA-256 hash values.

Secrets with credentials of privileged accounts are encrypted with AES-256.

The results of Forensic Export are encrypted with RSA-1024.