EMV CERTIFICATION AUTHORITY

MULTIPERSO

Issue and manage your own digital certificates in local payment projects

The EMV CA component can be used as a root Certification Authority for issuing and managing digital certificates in local payment projects, where interaction with international payment systems is not required.

OVERVIEW

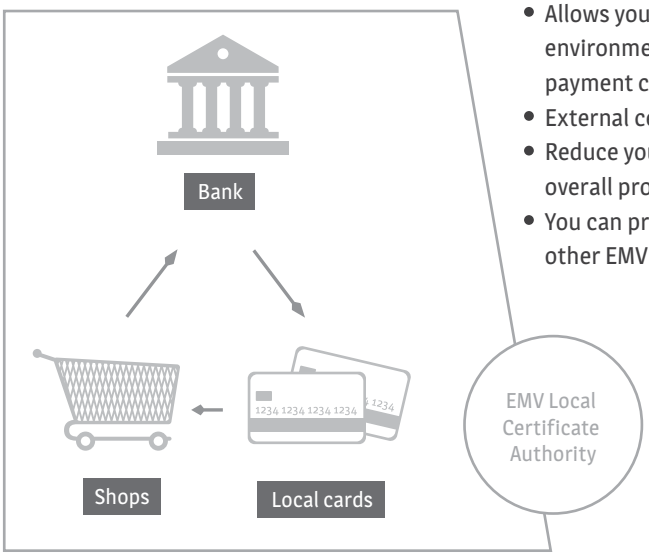
MultiPerso EMV CA allows banks or other financial institutions to build a dedicated in-house PKI environment and enables encryption, digital signature, and certificate authentication capabilities to be applied to a broad range of applications and platforms.

MultiPerso EMV CA provides the capabilities of a traditional Certification Authority (CA) with its key and certificate management services, including encryption and digital signature capabilities. It generates and protects the private keys via the use of FIPS 140-2 level 2/3 cryptographic devices (HSM) providing the maximum protection for such highly-sensitive objects as root certificates.

First, the self-signed Root Certificate is generated by MultiPerso EMV CA and securely stored in HSM memory. This certificate is treated as trusted in dedicated in-house PKI environment, and can be used for signing of all other issued subordinate certificates. For extended security, HSM device with Root Certificates can be disconnected and physically stored in the safe – hence eliminating possibilities for any network-related breaches.

Second, public key of new Root Certificate is loaded into MultiPerso Key Management System (or any other 3rd party KMS). Then KMS generates new RSA key pairs and creates a self-signed certificate request, formatted according to Visa or MasterCard specifications. Instead of sending to international payment organizations, this request is processed locally by MultiPerso EMV CA and then signed certificate is loaded back into the Key Management System. Once a certificate is loaded into KMS, it can be used for issuing new EMV cards in local payment projects.

With MultiPerso EMV CA you can sign your EMV certificate requests and start issuing local payment cards, without going to international payment organizations, and therefore reducing your expenses for licenses and overall project costs.



FUNCTIONALITY

- Provides generation and storing of self-signed Root Certificates in a highly-secure environment, using FIPS 140-2 level 2/3 hardware cryptographic devices
- Supports certificate requests formatted according to Visa and MasterCard specifications
- Provides integration with the MultiPerso KeyManagement System, as well as with other third-party Key Management Systems
- Enables secure auditing of all actions carried out in the system. Users can monitor keys and certificate status information and immediately get reports.

BENEFITS

- Allows you to build a dedicated in-house environment and to issue your own local payment cards
- External certification is not needed
- Reduce your expenses for licenses and overall project costs
- You can provide local root CA service for other EMV issuers

X INFOTECH secure identity and payments

X INFOTECH // Address: Daugavas iela 38-3 // Marupe, LV-2167 // Latvia
Tel.: +371 67930171 // Fax: +371 67930172 // info@x-infotech.com // www.x-infotech.com