General TECHNICAL SPECIFICATION

## Chip module basic specification

* Contact chip module with JAVA OS
* EEPROM or FLASH technology with minimum of at least 130 kBytes of free user memory

***Explanatory comment****:* During the personalization of the chip, approx. 75kB of memory is consumed by creating of instances of PKI applet, by uploading of third-party applet and creating of other data structures on the chip. Another 55kB of memory has to be available for the user data (i.e. keys and certificates and other user data).

* Supported standards ISO 7816, in particular:
  + supported communication protocols
  + standard contact surface
* Chip module size/punching size:
  + 11.8mm x 13mm, R=2,2mm for 8 contacts modules

Buyer accepts both size options.

* Maximum module thickness: 580 µm
* Maximum Tape thickness: 210 µm
* Working temperature range: -10°C to + 50°C
* Short temperature peak allowed: 210°C less than 1 sec.

***Explanatory comment****:* This parameter refers to the manufacturing process of the card, not to its normal use by the cardholder.

The contracting authority requires this parameter because of the manufacturing technology, which puts such a strain on the contact chip when inserting it into the card body

* Storage for up to one year after delivery in standard conditions
* Modul reliability: 500 hrs. at 85°C, 85% HR
* Chip modules winded on the reel:
  + width of the inner surface of the reel for winding the belt 35-40mm
  + fixing hub diameter: Ø 13mm or 76.5mm
  + winding hub diameter: Ø 150mm -180mm
  + Quantity: 6 000 - 11 000 micromodules per reel
  + defective chips pierced by a 1,5-2mm punch in a defined position

***Explanatory comment****:* The contracting authority requires full compatibility with the technology of the Mühlbauer CML 3420 and Mühlbauer CMI 200 - contact chip insertion (milling and glue tape lamination) machines.

## Chip OS requirements

* JavaCard OS (JC min. version 3.1, compliant with GP min. version 3.0.4)
* Applet loading enabled (according to GP min. version 2.3)
* ATR management (full, partial change of ATR)
* Support of pre-computed HASH
* Compliancy with eIDAS regulation
* Compliancy with EN 419211, parts 1, 2, 4
* Following the Regulation EU 2019/881 (Cybersecurity Act) and the new EU CC scheme being deployed by ENISA, it is strongly recommended that the card operating system should be able to be patched in documents deployed in the field.

STC considers this as a mandatory requirement.

## On board applications (applets)

***Explanatory comment****: The Czech eID implementation hosts two instances of one PKI applet on the chip. The first instance of the PKI applet is configured for the purpose of electronical signature a authentication – standard PKI functionality. The second instance of the PKI applet is specifically configured for the purpose of authentication functionality which is used to access e-government services.*

*The possibility to create two instances of PKI applet is preferable functionality.*

**APPLET 1: Applet for authentication**

* Applet file system support (ISO 7815-4)
* Data objects support (ISO 7816-4)
* Applet PIN management support (ISO 7816-4) (verify, un-verify, change, unblock)
* Global PIN object support (compliance with GP min. version v.2.3)
* Local PIN objects management using GPIN
* RSA key management (on board key generation, import, erase) up to 4096 bits
* RSA asymmetric cryptography (sign, decrypt)
* ECC keys management ((on board key generation, import, erase) up to 521 bits
* Support of standard ECC curves (preferably NIST P-521) defined by its oid
* Support of generic ECC curves, defined by domain parameters
* Asymmetric cryptography with ECC keys (TR-03111: Elliptic Curve Cryptography), Sign + KeyAgreement
* Symmetric Secure Messaging with AES-128,192 or 256 bits
* Asymmetric Secure Messaging (preferable with ECC keys)
* Access rights support for key objects, controlled by Asymmetric Mutual Authentication via CV certificate (Certificate Holder Authorization attribute in CV certificate specified in BSI TR-03110 or similar)

**APPLET 2: Applet for electronic signature**

* Applet file system support (ISO 7816-4)
* Data objects support (ISO 7816-4)
* Applet PIN management support (ISO 7816-4) (verify, un-verify, change, unblock)
* Support of MS Session PIN (at least for one PIN object) – preferable feature
* Global PIN object support (compliance with GP min. version 2.3)
* Local PIN objects management using GPIN
* RSA key management (on board key generation, import, erase) up to 4096 bits
* RSA asymmetric cryptography (sign, decrypt)
* Support of HASH algorithm: SHA-1, SHA-256, SHA-384 and SHA-512 (FIPS 180-2)
* ECC keys management ((on board key generation, import, erase) up to 521 bits
* Support of standard ECC curves (preferably NIST P-521) defined by its oid
* Support of generic ECC curves, defined by domain parameters
* Asymmetric cryptography with ECC keys (TR-03111: Elliptic Curve Cryptography), Sign + KeyAgreement
* Symmetric Secure Messaging with AES-128,192 or 256 bits
* Asymmetric Secure Messaging (preferable with ECC keys)
* Prove of QSCD keys origin – mechanism allowing to prove that the keys were generated on-board, support of cryptographical verification

***Explanatory comment****: Our ID card solution assumes any cryptographic mechanism, even non-standard, on the basis of which it is clearly demonstrable that the key was generated by card generation (and not import). The preferred variant is based on asymmetric algorithms.*

*The principle of the existing ID card is that symmetric session key is established using asymmetric keys and subsequent key pair generation is performed using this SM key. The entire operation is recorded in the APDU trace, on the basis of which this operation can be traced back in the card.*

*This functionality is required to prove the key pair origin in case when the user is on-line communicating with the qualified certification authority in order to get the qualified certificate for the qualified electronic signature.*

*Qualified certification authority issuing the qualified certificate must verify (on-line) that the keys were generated in the chip of the smart card, in order to issue the qualified certificate with the QSCD flag enabled.*

**APPLET 3: 3rd party applet**

***Explanatory comment****: The Czech eID implementation hosts one 3rd party applet with specific functionality. This applet is sharing the PIN with other applets (GPIN functionality required).*

## CC and SSCD certification requirements

* Java Card – minimum EAL 5+
* On board applications – minimum EAL 5+
* Chip - minimum EAL 6+
* SSCD certification – Secure Signature-Creation Device Type 2 and Type 3
* QSCD certification - Qualified Electronic Signature Creation Device (QSCD) in accordance with the European Regulation 910/2014 – eIDAS
* OPTIONAL REQUIREMENT: The chip module should be listed in the list of qualified devices: <https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD>