ePasslet Suite Edition 2

Modular Java Card applet suite for eID document applications

ePasslet Suite is a solution for electronic ID documents. It supports various applications such as: national identity cards, electronic passports, drivers licenses, security access badges, or health cards.

Applications	• **ICAO MRTD** with BAC/SAC Logical Data Structure (LDS) and Basic Access Control (BAC) according to ICAO Doc 9303 • **ISO File System** File system and access condition handling according to ISO 7816-4/5/6/8/9/15 • **ISO Driving License** with BAC/BAP ISO electronic Driving License according to ISO 18013 with BAC/BAP • **ICAO MRTD** with EAC1 Includes BAC/SAC Logical Data Structure (LDS), Basic Access Control (BAC), Extended Access Control according to ICAO Doc 9303 • **ISO Driving License EACv1/EAP** ISO electronic Driving License according to ISO 18013 with EACv1/EAP • **ePKI/SSCD** Electronic signatures according to Secure Signature Creation Device (SSCD) • **Vehicle Registration** Vehicle Registration according to European electronic Vehicle Registration specifications (eVR) with EAC • **Health Insurance** eHIC Type 1, Type 1.alt and Type 2 according to CWA 15974

Functions and Features	• ICAO Logical Data Structure (LDS) • ICAO Basic Access Control (BAC) • ICAO Extended Access Control (EAC) • ICAO Basic Access Protection (BAP) • ICAO Supplemental Access Control (SAC) • ISO File System • ICAO Active Authentication (AA) • ISO Driving License BAP (IDL-BAP) • Supplemental Access Control (SAC) • ISO Driving License EAP (IDL-EAP) • PKI / Digital Signature (ePKI) • Electronic Voting (eVoting) • Electronic Vehicle Registration (eVR) • European Health Insurance (eHIC) • Extended Access Control v2 (EACv2)
Scope of Supply	ePasslet Suite Edition 2 is provided as a ROMized standard product based on NXP JCOP available on the following chip variants: **Version 2.1 (JCOP 2.4.2 R3)** • J3E120 – 120 kbyte EEPROM* • J3E082 – 80 kbyte EEPROM* • J2E120 – 120 kbyte EEPROM* • J2E082 – 80 kbyte EEPROM* **Version 1.1 (JCOP 2.4.1 R3)** • J3A128 – 128 kbyte EEPROM • J3A081/J2A081 – 80 kbyte EEPROM* • J3A041/J2A041 – 40 kbyte EEPROM • J3A080/J2A080 – 80 kbyte EEPROM* • J2A040/J2A040 – 40 kbyte EEPROM* * These variants are certified according to Common Criteria EAL 4+ Please refer to the detailed product specification for details on available platform configurations and certification
Supported Biometry	Fingerprint Match-on-Card with: • Biomatch package by Precise Biometrics, proprietary in v1.1 • Biomatch package by Precise Biometrics, ISO 19794-2 and ISO 24787 compliant in v2.1 • MegaMatcher package by Neurotechnology, ISO 19794-2 and ISO 24787 compliant in v2.1

Supported Standards	• ISO7816-4/5/6/8/9/15, PKCS#15 • BSI TR03110 v1.11/v2.10 • ICAO Doc 9303 • ISO 18013 • ISO 19794-2 • ISO 24787
Supported Algorithms	Mechanisms based on Elliptic Curves over GF(p) with 128 - 320 bit • EC-DSA signature generation and verification • EC-DH key agreement Integer Factorization/Discrete Logarithm with 1024 - 2048 bit • RSA CRT key generation • RSA signature generation with PKCS#1 Message Encoding • DH key agreement Symmetric ciphers and hash algorithms • DES and Triple-DES with 56, 112 and 168 bit • AES with 128, 192 and 256 bit • SHA-1 with 160 bit • SHA-224 with 224 bit • SHA-256 with 256 bit
Expendability	ePasslet Suite provides applets for common eID applications according to international and European standards. These applets can be instantiated into EEPROM individually, even combining more than one applet to allow for a multi-application scenario. The provided applets can be configured to meet customers' requirements. All applets are based on a common core library that can also be used by custom applets for additional applications like ticketing, payment, storage of additional data and many others. This approach allows for easy customization and reduces the memory footprint of additional applets. Custom applet development is provided by cryptovision upon request but can also be done by customers or system integrators based on API documentation of the core library. Custom applets can be stored into EEPROM or included into a custom ROM mask. Instantiated applets can be activated post-issuance to cover upcoming applications and to provide a smooth migration. The JCOP platform also allows for post-issuance applet loading[1]. [1] Please see JCOP guidance manual for further details and additional certification requirements.

Editions	Apart from ePasslet Suite Edition 2 there are the following other editions: **Edition 1:** • ICAO MRTD with BAC/SAC • ISO File System • ISO Driving License with BAC/BAP **Edition 3:** Edition 2 plus the following applications: • EU Residence Permit • European Citizen Card / German eID • Custom eID

cv cryptovision GmbH | T: +49 (0) 209.167-24 50 | F: +49 (0) 209.167-24 61 | info(at)cryptovision.com

61021041