cryptovision

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/PACE Logical Data Structure (LDS), Active Authentication (AA), Basic Access Control (BAC), and Password Authenticated Connection Establishment (PACE) according to ICAO Doc 9303 • **ISO File System** File system and access condition handling according to ISO 7816-4/5/6/8/9/11/15 • **ISO Driving License** with BAC/BAP/PACE ISO electronic Driving License according to ISO 18013 with BAC, Basic Access Protection (BAP), and PACE • **ICAO MRTD** with EACv1 (includes BAC/PACE) Logical Data Structure (LDS) with Extended Access Control (EAC) according to ICAO Doc 9303 • **ISO Driving License EAC/EAP (includes BAC/BAP/PACE)** ISO electronic Driving License according to ISO 18013 with EAC or Extended Access Protection (EAP) • **PKI/SSCD** PKI/electronic signature application (Secure Signature Creation Device, SSCD) with fingerprint Match-on-Card[1] • **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 [1] Based on an ISO 19794-2 compliant 3rd party native fingerprint matching package (platform dependent)

Functions and Features	• ICAO and ISO 18013 Logical Data Structure (LDS) • ICAO Active Authentication (AA) • ICAO Basic Access Control (BAC) • Password Authenticated Connection Establishment (PACE) • ISO 18013 Basic Access Protection (BAP) • ISO File System • ICAO/BSI Extended Access Control (EAC) • ISO 18013 EAP • PKI / Electronic Signature (ePKI) • Electronic Voting (eVoting) • Electronic Vehicle Registration (eVR) • European Health Insurance (eHIC)
Scope of Supply	ePasslet Suite Edition 2 is provided as custom ROM mask or pre-loaded in Flash on the following platforms: **Version 3.0[2]** • NXP JCOP 3 on P60-StepUp with 80k and 145k of free EEPROM • Veridos Sm@rtcafé Expert 7 on Infineon SLE78 with 268k of free Flash **Version 2.1[3]** • NXP JCOP 2.4.2 R3 on P5 with 80k and 120k of free EEPROM • Veridos Sm@rtcafé Expert 7 on P60-StepUp with 80k of free EEPROM [2] These variants are certified according to Common Criteria EAL 4+ [3] These variants are certified according to Common Criteria EAL 5+ Please refer to the detailed product specification for details on available platform configurations and certification
Supported Standards	• ISO7816-4/5/6/8/9/11/15, PKCS#15 • BSI TR03110 v1.11/v2.10/v2.20 • ICAO Doc 9303 • ISO 18013 • ISO 19794-2 • ISO 24787

Supported Algorithms	Mechanisms based on Elliptic Curves over GF(p) with 128 - 320 bit (version 2.1) and 128 – 521 bit (version 3.0), respectively • EC-DSA signature generation and verification • EC-DH key agreement Integer Factorization/Discrete Logarithm with 1024 - 2048 bit (version 2.1) and 1024 – 4096 bit (version 3.0), respectively • 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 • SHA-384 with 384 bit, SHA-512 with 512 bit (version 3.0 only)
Expendability	ePasslet Suite provides applets for common eID applications according to international and European standards. These applets can be instantiated into EEPROM/Flash 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/Flash or included into a custom ROM mask. Applets can be activated post-issuance to cover upcoming applications and to provide a smooth migration. The above mentioned Java Card platforms also allows for post-issuance applet loading according to Global Platform.

Editions	Apart from ePasslet Suite Edition 2 there are the following other editions: **Edition 1:** • ICAO MRTD with AA, BAC, and PACE • ISO File System • ISO 18013 Driving License with BAC/BAP **Edition 3:** Edition 2 plus the following applications: • EU Residence Permit • European Citizen Card / German eID • Custom eID application

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

81022082