OTHER FEATURES

- Implementation based on Java Card 3.0.5 and Global Platform 2.3 standard APIs
- T=0, T=1 and T=CL protocols
- Extended Length protocol
- Plain or CRT RSA, ECDSA key generation / import
- Customizable CV certificate profiles
- Customizable application profiles
- Issuer defined chip numbering schemes
- Issuer defined objects
- Issuer defined personalization scenario

HARDWARE FEATURES

- Available on various NXP platforms
- SmartMX3 P71D351 (J3R)
- Dedicated Secure_MX51 Smart Card CPU
- PKI co-processor FameXE
- High Speed Triple-DES / AES co-processor
- TDES (112/168 bit)
- AES (128/192/256 bit)
- RSA up to 4096 bit
- ECC GF(p) up to 521 bit
- ECC Standardized domain parameters (sec2/brainpool/ANSI)
- SHA-1/SHA-224/SHA-256/SHA-384/SHA-512
- ISO/IEC 7816 contact interface
- ISO/IEC 14443 contactless interface
- Common Criteria EAL 6+ certified
- Random number generation according to class DRG.3 or DRG.4 of AIS.

EVALUATION STATUS

- Based on CC EAL 6+ certified chip and OS
- NXP JCOP 4 P71
- Common Criteria CC EAL4+ certifications:
- IDentity Applet v3.4/BAC EAC4+ - BSI-CC-PP-0055
- ID&Trust IDentity Applet v3.4/eIDAS – Electronic Identity Card with PACE-GM, PACE-CAM, Extended Access Control v1 and v2, Restricted Identification and Active Authentication - - BSI-CC-PP-0056-V2-2012, BSI-CC-PP-0068-V2-2011-MA-01, BSI-CC-PP-0086, BSI-CC-PP-0087, EN 419211-2:2013,
- ID&Trust IDentity Applet v3.4/PACE-EAC1/AA – ePassport with PACE-GM, PACE-CAM, Extended Access Control v1 and Active Authentication - BSI-CC-PP-0056-V2-2012, BSI-CC-PP-0068-V2-2011-MA-01
- ID&Trust IDentity Applet v3.4/QSCD - Qualified electronic signature compliant with IAS ECCv2 and eIDAS - EN 419211-2:2013, EN 419211-4:2013
- ID&Trust IDentity-J with SAC (BAC+PACE) and AA JISEC C0500
- ID&Trust IDentity-J with SAC (PACE) and AA JISEC C0499
- ID&Trust IDentity Card 3.2/BAC - BSI-CC-PP-005
- ID&Trust IDentity Card 3.2/PACE-EAC1, BSI-CC-PP-0056-V2-2012, BSI-CC-PP-0068-V2-2011
- ID&Trust IDentity Card 3.1/BAC - BSI-CC-PP-005
- ID&Trust IDentity Card 3.1/PACE-EAC1, BSI-CC-PP-0056-V2-2012, BSI-CC-PP-0068-V2-2011
- ID&Trust HTCNS Applet v1.03 BSI-CC-PP-0059

ID&Trust Ltd.
www.idntrust.com

H-1026 Budapest, Riadó utca 7. |
Tel: +36 1 464 9560 | Fax: +36 1 700 2709 | Email: info@idandtrust.com

IDENTITY SUITE SMART ID PLATFORM

A multi-purpose smart card, e-document and e-signature platform, IDentity Suite meets all relevant EU and international standards and allows central and local authorities and organisations to issue cards compliant with Java Card and GlobalPlatform specifications.

Use IDentity Suite to issue eID documents such as electronic and biometric identity cards, electronic passports, vehicle registrations, driving licences, health cards, residence permits or eIDAS tokens.

WHERE TO USE IDENTITY SUITE

- Electronic identity
- E-signature identity
- Commercial applications
- Issue e-administration and bank signature cards with qualified electronic signature.
- Create multi-purpose smart cards and PKI solutions such as company ID, PC login, secure email, e-purse or loyalty cards

WHY CHOOSE IDENTITY SUITE

Secure

The IDentity applet has earned 11 Common Criteria certifications and national references.

Easy to configure

Thanks to the all-in-one architecture of our IDentity applet, card issuers can purchase card chips and then decide later what to use them for.

Versatile

Passport, eID and e-signature functions can be handled by a single applet, which means more space left on the card chip.

DISCOVER FEATURES

- Common Criteria EAL 6+ platform
- Compliant with all relevant standards and specifications, including IAS-ECC, ICAO, BSI-EAC, BSI-PACE, ISO/IEC 7816, ISO/IEC 24727-2, ISO/IEC 18013, CEN/TS 15480-1/2 and the European Citizen Card standard
- Contact, contactless or dual-interface support
- Multi-application cards: download card applications after issuance
- Secure centralized or decentralized personalization
- Online or offline post-issuance personalization
- Multiple applet instances for different uses
- GlobalPlatform-compliant personalization components
- Match-on-Card fingerprint verification

USE CASES

Public Sector

IDentity provides Qualified Signature solutions in order to be used for Electronic Administration, Banking signature cards.

- Support of PINPAD readers with Secure Messaging
- Additional PKI functions on the same card
- Standard middleware is available
- Common Criteria EAL 4+ certified against QSCD PPs

e-Government Solutions

Use IDentity to issue various e-ID products as Identity cards, Health cards, Electronic passports & Driving License cards.

- Multi-application feature
- Secure centralized / de-centralized personalization
- Common Criteria EAL 6+ platform certificate
- Common Criteria EAL 4+ certificates

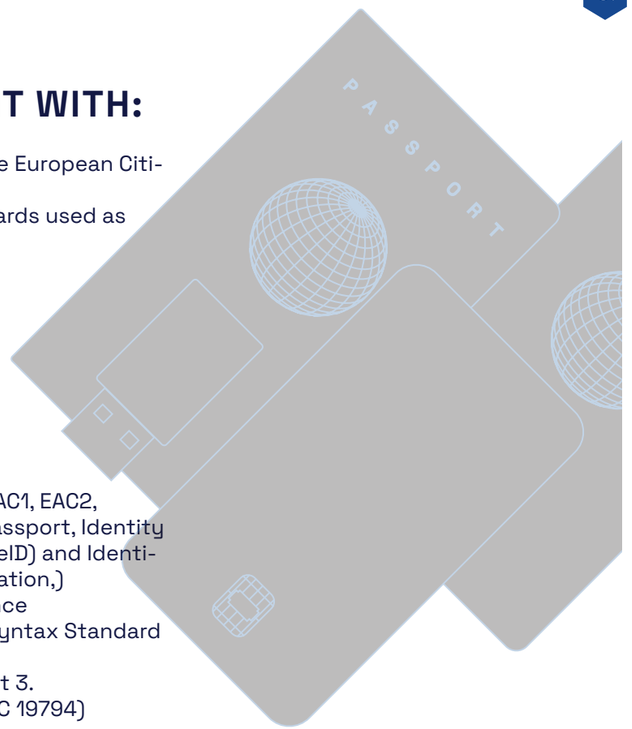
Multi-purpose PKI Products

IDentity can be used for various other cases, such as Company ID, PC logon, Secure e-mail combined with Loyalty cards, e-Purse.

- Support of multiple applet instances for different usage
- Contact and / or contactless interface
- Additional applets for Loyalty and electronic purse functionality

IDENTITY IS FULLY COMPLIANT WITH:

- All mandatory features of CEN/TS 15480-1/2 – the European Citizen Card Standard
- EN 14890-1/2 – Application Interface for smart cards used as secure signature devices
- ISO/IEC 7816-3/4/8/9/15
- ISO/IEC 24727-2 – Generic card interface
- CEN/CWA 15974 – eEHIC
- ISO 21549-1 Patient healthcard data
- Fully compliant with IAS-ECC 1.0.1
- CIE 3.0
- CNS v1.1.6
- DDU v1.1.0
- ICAO Doc 9303 (PA, AA, BAC, SAC)
- BSI TR-03110 v2.20 Part 1 and v2.21 Part 2/3/4 (EAC1, EAC2, PACE2, RI, Auxiliary Data Verification European Passport, Identity card with Protected MRTD Application (German-eID) and Identity Card with optional EU-compliant MRTD application,)
- ISO/IEC 18013-3:2012 ISO-Compliant Driving Licence
- PKCS#15 v1.1: Cryptographic Token Information Syntax Standard
- EU driving license (383/2012/EC)
- ISO/IEC 18013-3 ISO compliant driving licence Part 3.
- Fingerprint Match-on-Card (ISO/IEC 19785, ISO/IEC 19794)



ADDITIONAL FUNCTIONALITY

- Support of extended length APDUs
- Up to 4 logical channels according to ECC
- ECDSA and various padding algorithms
- Device authentication with key transport protocol according to EN 14890-1
- Key generation counter (proof of key-pair is generated on-board)
- Multiple compulsory algorithms per Security Data Object
- Asymmetric device authentication with Role validation
- Offline Secure Messaging with implicit authentication (offline PIP)
- GP Issuer Security Domain CVM management by PIN SDO
- Card-to-card authentication and access control
- Support of elementary files with record and TLV structures acc. to ISO/IEC 7816-4
- IAS-ECC with AES, ECDSA
- Other extensions on request

SUPPORTED ALGORITHMS & PROTOCOLS

- Digital Signature (PKCS#1, ISO/IEC 9796-2, PSS, ECDSA)
- Client/Server authentication (IASECC 1.0.1)
- Encryption key decipherment (PKCS#1, ISO/IEC 9796-2, RSA-OAEP, ECDH)
- RAW-RSA encryption / decryption
- Asymmetric device authentication with key agreement (DH with privacy, key transport, EAC1, EAC2, EAP)
- Asymmetric role authentication (IASECC 1.0.1, EAC1, EAC2, EAP)
- Symmetric device authentication (IASECC 1.0.1, BAC, SAC)
- Symmetric role authentication (IASECC 1.0.1)
- Secure Messaging according to IDL, ICAO and IASECC with 3DES (112, 168), AES (128, 192, 256)
- Public key cryptography (RSA up to 4096 bits, ECDSA up to 521 bits)
- Secure Hash algorithms, SHA-1 and SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)
- ICAO Doc 9303 PA, AA, SAC (BAC + PACE2): 3DES, AES, DH, ECDH
- BSI TR-03110 EAC1, EAC2, PACE2 (Generic Mapping, Chip Authentication Mapping)
- ISO/IEC 18013 ISO-Compliant Driving License (BAP1-4, EAP RSA, ECDSA)