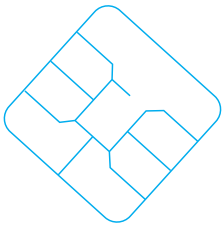
ID TRUST
KEY TO E BUSINESS



IDentity Suite

a multi-purpose smart e-ID, PKI platform

ID&Trust Ltd.
www.idandtrust.com

IDentity is a multi-purpose Global Platform smart card solution for a wide area of e-Services following the relevant EU and worldwide standards. It has been specifically designed for electronic identity and government market needs: national ID cards, health cards, electronic passports, driving licenses or employee ID cards.

The major target areas of using IDentity:

e-Government
Qualified Signature
Multi-purpose PKI

IDentity Suite

a multi-purpose
smart e-ID, PKI platform

Features

- **Compliant with all relevant eID specifications**
  Required functionality is configured during personalization (i.e. ePassport, IDL, eID or PKI...)
- **Dual-interface support**
  Flexible role based access control on each interface
- **Secure centralized / de-centralized personalization**
  Online / offline Post Issuance Personalization
- **Multi-application feature**
  Post issuance download of card applications
- **Support of PINPAD readers with Secure Messaging**
- **Different functionality on each interface**
  Multiple instances and logical chanels
- **Compliant with the European Citizen Card standard**
- **Compliant with ePassport standards (ICAO, BSI)**
- **Compliant with International Driving License standard**
- **Fingerprint Match-on-Card verification**
- **Common Criteria EAL 5+ platform**
- **Common Criteria EAL 4+ certified**
- **More than 20M instances issued**

ID&Trust Ltd.
www.idandtrust.com
H-1117 Budapest, Gábor Dénes u. 2. Infopark, building D. | Tel: +36 1 464 9560 | Fax: +36 1 700 2709 | e-mail: info@idandtrust.com

IDentity Suite

a multi-purpose
smart e-ID, PKI platform

USE CASES

Public Selector

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 SSCD PP

e-Government Solutions

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

- Compliant with the relevant standards
- Dual-interface support
- Multi-application feature
- Secure centralized / de-centralized personalization
- Common Criteria EAL 5+ platform certificate
- Common Criteria EAL 4+ certificate

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

ID&Trust Ltd.
www.idandtrust.com
H-1117 Budapest, Gábor Dénes u. 2. Infopark, building D. | Tel: +36 1 464 9560 | Fax: +36 1 700 2709 | e-mail: info@idandtrust.com

IDentity is Fully Compliant With

IDentity Suite

a multi-purpose
smart e-ID, PKI platform

- 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
- ISO/IEC 24727-2 – Generic card interface
- CEN/CWA 15974 – eEHIC
- Fully compliant with IAS-ECC 1.0.1
- CNS v1.1.6
- DDU v1.1.0
- ICAO Doc 9303 (PA, AA, BAC, SAC)
- BSI TR-03110 2.10 Part 1/2/3 (EAC 1.11, EAC 2.0, PACE2, German-eID)
- ISO/IEC 18013-3:2012 ISO-Compliant Driving Licence
- EU driving license (383/2012/EC)
- Fingerprint Match-on-Card (ISO/IEC 19785, ISO/IEC 19794)

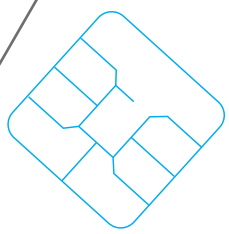
ID&Trust Ltd.
www.idandtrust.com
H-1117 Budapest, Gábor Dénes u. 2. Infopark, building D. | Tel: +36 1 464 9560 | Fax: +36 1 700 2709 | e-mail: info@idandtrust.com

Additional Functionality

IDentity Suite

a multi-purpose
smart e-ID, PKI platform

- 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



ID&Trust Ltd.
www.idandtrust.com
H-1117 Budapest, Gábor Dénes u. 2. Infopark, building D. | Tel: +36 1 464 9560 | Fax: +36 1 700 2709 | e-mail: info@idandtrust.com

Supported Algorithms & Protocols

IDentity Suite

a multi-purpose
smart e-ID, PKI platform

- **Digital Signature** (PKCS#1, ISO/IEC 9796-2, PSS, ECDSA)
- **Client/Server authentication**
- **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, EAC, EAP)
- **Asymmetric device authentication with role validation**
- **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)
- **Card-to-card authentication**
- **Secure Messaging with 3DES** (112, 168), **AES** (128, 192, 256)
- **Public key cryptography** (RSA up to 2048 bit - 4096 on request, ECDSA up to 320 bit - 521 on request)
- **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, Integrated Mapping)
- **ISO/IEC 18013 ISO-Compliant Driving License**
  (BAP1-4, EAP RSA, ECDSA)

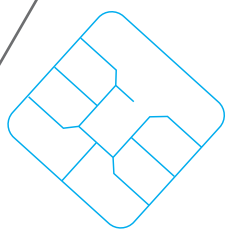
ID&Trust Ltd.
www.idandtrust.com
H-1117 Budapest, Gábor Dénes u. 2. Infopark, building D. | Tel: +36 1 464 9560 | Fax: +36 1 700 2709 | e-mail: info@idandtrust.com

Other Features

IDentity Suite

a multi-purpose
smart e-ID, PKI platform

- Implementation based on Java Card 2.2.2 / 3.0.1 and Global Platform 2.1.1 / 2.2.1 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



ID&Trust Ltd.
www.idandtrust.com
H-1117 Budapest, Gábor Dénes u. 2. Infopark, building D. | Tel: +36 1 464 9560 | Fax: +36 1 700 2709 | e-mail: info@idandtrust.com

Hardware features

IDentity Suite

a multi-purpose
smart e-ID, PKI platform

- **Available on various NXP platforms**

  J2A040, J3A041, J2A080, J3A081, J2D/E081, J3D/E081, J2D/E145, J3D/E145, J2E082, J3E082, J2E120, J3E120
- **Dedicated Secure_MX51 Smart Card CPU**
- **PKI co-processor FameXE**
- **High Speed Triple-DES / AES co-processor**
- **DES/TDES** (56/112/168 bit)
- **AES** (128/192/256 bit)
- **RSA up to 8192 bit**
- **ECC GF(p) up to 521 bit**
- **ECC Standardized domain parameters** (sec2/brainpool/ANSI)
- **SHA-1/SHA-224/SHA-256**
- **ISO/IEC 7816 contact interface**
- **ISO/IEC 14443 contactless interface**
- **Common Criteria EAL 5+ certified**
- **Secure Random Number Generator**

ID&Trust Ltd.
www.idandtrust.com
H-1117 Budapest, Gábor Dénes u. 2. Infopark, building D. | Tel: +36 1 464 9560 | Fax: +36 1 700 2709 | e-mail: info@idandtrust.com

Evaluation Status

IDentity Suite

a multi-purpose
smart e-ID, PKI platform

- Based on CC EAL 5+ certified chip and OS
  - NXP JCOP v2.4.1 R2/R3, v2.4.2 R2/R3 Secure Smart Card Controller
- Common Criteria CC EAL4+ evaluation
  - BSI-CC-PP-0056-V2-2012
  - BSI-CC-PP-0068-V2-2011
  - BSI-CC-PP-0059-2012
  - BSI-CC-PP-0071-2012
  - BSI-CC-PP-0072-201

ID&Trust Ltd.
H-1117 Budapest
Gábor Dénes u. 2. Infopark, building D.
Tel: +36 1 464 9560
Fax: +36 1 700 2709
www.idandtrust.com
e-mail: info@idandtrust.com

Specifications subject to
change without notice