



# **IDeal Citiz™ - All ID Inside**

## ■ **IDeal Citiz™**

**IDeal Citiz™ is Sagem Orga's latest smart card with the answers to the global identity needs of the public sector. For years, government agencies have demanded ever higher security and greater functionality as they work to improve their services for their citizens. They need a fast and efficient product to facilitate all transactions – Internet in e-government and e-commerce as well as border control.**

What are the concerns of today's governments? Strengthening national security, reducing ID fraud and theft and establishing secure Internet access for their e-services, for example. By addressing these issues, governments are also seeking to improve public services and cut administrative costs.

In keeping with national requirements, and allowing governments to continue their security and electronic applications deployment, the European Committee for Standardization (CEN) published the European Citizen Card standard in 2007 to meet these government needs and concerns.

The European Citizen Card is designed to provide the following services:

- Identification and strong Authentication for e-services with or without biometrics,
- Qualified digital signature
- Citizen identification and cross border control

Sagem Orga's development approach is based on a methodology that first meets application and use case requirements and ensures the integration of standards, provision of security and privacy protection on the strength of its design and innovative features. The result of this approach is Sagem Orga's IDeal Citiz™, an all-in-one product that meets the full range of ID requirements, including e-services, digital signature and travel applications. It addresses all ID application needs:

- National e-ID and Corporate e-ID
- Healthcare/welfare Card
- Driver License
- Resident permit
- Qualified signature

### **IDeal Citiz™ complies with the following standards:**

- IAS ECC v1.0.1
- ICAO 9303 7th Edition
- EAC v1.11
- CEN 14890
- CENT/TS 15480
- ISO/IEC 7816 part 1 to 6, 8, 9, 11
- Java Card™ API 2.2.2
- Global Platform 2.1.1
- e-EHIC: CEN CWA 15974:2009

**IDeal Citiz™ enables identification, online authentication and electronic signature with maximum security (IAS ECC Specification, Common Criteria security certification).**

**IDeal Citiz™ is a travel document and a means of citizen identification (ICAO/EAC standards).**

**IDeal Citiz™ enables strong multi-biometric authentication (fingerprints, iris, facial) thanks to the most high-performance Match-On-Card technology available on the market (MINEX II).**

### **IDeal Citiz™ is an ALL ID INSIDE solution:**

- With proven interoperability thanks to the IAS ECC and ICAO/EAC ecosystems
- Evolves to handle future applications – and has the necessary performance – thanks to Java™ and Global Platform
- Secured with an EAL5+ Common Criteria certification\*



\* on going

# ■ Key benefits of the IDEal Citiz™

## Beyond the standards

First, IDEal Citiz™ conforms to the latest standards in terms of security and applications. These are published by:

- CEN and GIXEL <sup>(1)</sup> : CEN15480 and IAS ECC v1.01: an application meeting the needs of the European Citizen Card for identification as well as for e-government services.
- ICAO and EAC : for travel and resident permit applications.
- ISO (ISO 7816 / 14443), the foundation of the smart card specification.

But IDEal Citiz™ goes beyond these standards by offering the potential to migrate and enhance the security of the system. IDEal Citiz™ already offers the opportunity to use the largest cryptographic keys, including RSA keys of up to 3072 bits and elliptic curves up to 521 bits.

Finally, IDEal Pass™ provides customers with an open product during the personalization stage thanks to the use of the common personalization specification (CPS), a standard published by Global Platform.

## Optimized memory

For even greater convenience, IDEal Citiz™ is available in two versions: a 48 KB and an 80 KB EEPROM. In both versions, the IAS ECC application is directly ROMed, thus leaving the EEPROM memory for application-specific use. The decision made between the two versions will depend on data storage needs for personalization as well as possible evolution to enable new application uploads, for example.

This optimized memory is a must for enhanced e-service capabilities, enabling governments to tackle their new Identification projects in a more confident way – without memory constraints.

## Enhanced security standards and certificates

Sagem Orga is a leader in the secure development of smart cards (secure banking, health and Identity card evaluation). IDEal Citiz™ will be evaluated by the end of 2009 according to:

- Common Criteria EAL4+ for travel applications compliant with the BAC and EAC protection profiles
- Common Criteria EAL5+ for IAS ECC, compliant with SSCD type 2 and 3 protection profiles – FIPS 140-2 level 3 <sup>(2)</sup>
- MINEX II for Match On Card

IDEal Citiz™ relies on the latest evaluated silicon platform available on the market.

## Multi- biometry

IDEal Citiz™ is leveraging the biometrics expertise of Sagem Orga and Sagem Sécurité to implement the first Multi-Match On Card feature on a smart card (fingerprint, facial and iris on request). The MOC feature is the best possible combination of privacy and security, as the biometrics template is stored securely on the card.

IDEal Citiz™ MOC is the most interoperable and fastest product as stated by the NIST during the Minex II phase II benchmark.

## Java Technology and Global Platform

The implementation of the latest versions of Java technology and Global Platform gives IDEal Citiz™ the following advantages:

- Post-issuance processes that allow the product to evolve by adding features and applications. It enables management of the card content, including the creation and deletion of applications.
- A high-level programming language that is well known and in common use makes it possible to develop applications at reduced cost.

## Flexibility and adaptability

IDEal Citiz™ is available for all interfaces: contact, contactless, DUAL or hybrid (contact and contactless chip on one card).

There is also a choice of card bodies to meet a variety of needs regarding service life and personalization modes. Generally based on the smart card (ID1 format) form factor, IDEal Citiz™ is available in polycarbonate or PET with state-of-the-art secure printing and use of specific inks.



<sup>(1)</sup> defining the IAS ECC specification as well as the eco-system around electronic ID cards <sup>(2)</sup> in 2010

# ■ IDeal Citiz™ Technical Overview

## Technical characteristics

- Java Card™ 2.2.2.
- Open Platform 2.1.1
- 8/16 bits micro Controller.
- e-Services, identity and travel applications ROMed, freeing up entire EEPROM for customer needs
- 80 and 48 KBytes EEPROM available

## Communication protocol

- ISO T=0 and ISO T=1
- ISO T=CL

## Cryptographic features

- Signature, Authentication and Confidentiality based on DES, 3DES, RSA, SHA-1, SHA-256
- RSA generation keys embedded up to 3072 bits
- Protected against SPA, DPA et DFA

## Certifications

- Chip certified CC EAL5+.
- EAC application certified EAL4+ according to PP 055 (BAC) and PP 056 (EAC)
- IAS ECC application certified EAL4+ minimum according to PP SSCD type 2 and type 3

## Standards compliance

- ISO 7810, ISO 10373-1
- ISO 14443
- ISO 7816-1, -2, -3, -4, -8, -9, -11, -15
- PKCS#1, #11, #15
- IAS ECC v1.0.1
- ICAO 9303
- EAC v1.11

## Form factors

- Smart card (ID1) format with secure material polycarbonate and PET
- Contact
- Contactless
- Dual or hybrid

## Match On Card

- ISO/IEC 19794-2
- Minex II phase II  
[see http://fingerprint.nist.gov/minexII/minex\\_report.pdf](http://fingerprint.nist.gov/minexII/minex_report.pdf)
- Facial
- Iris (on request)



is a global leader in the smart card industry. Its portfolio includes hardware, software, consulting and services, all focused on smart cards for the telecommunications, health, identification and banking sectors. As a subsidiary of Sagem Sécurité (SAFRAN Group), the world's No. 1 in identification, Sagem Orga offers comprehensive integrated solutions designed to secure the digital and mobile community. The company has a workforce of over 2,100 people around the world. Production and R&D facilities incorporating the latest technology are based in France, Germany, Brazil, Russia, Mexico and India.

