

# NATIONAL ID SOLUTION



ELECTRONIA



## NATIONAL ID SOLUTIONS

As the world gropes against terror and fraud on a grand scale, governments and businesses race against time to contain the ever increasing threats. Smart cards in large part have become key to the solution.

Electronia constantly strives to use the most advanced cryptographic algorithms on its smart cards, in keeping with the security requirements of recognized establishments of the world.

Its expertise in handling national ID implementation comes from decades of closely working together with partners and clients in coming up with the most optimal solutions, from the simplest to the most daunting tasks that require smart card technology.

EISmart national Smart Card ID solution transforms existing, divergent ID systems for personal identification into a highly secure, unified Smart Card system complete with different applications such as Personal identification, Biometric verification, Driving License, etc.

The EISmart solution is a robust, large-scale implementation of a National ID program fully covering the management of card issuance, customer service, acceptance infrastructure and transaction processing.

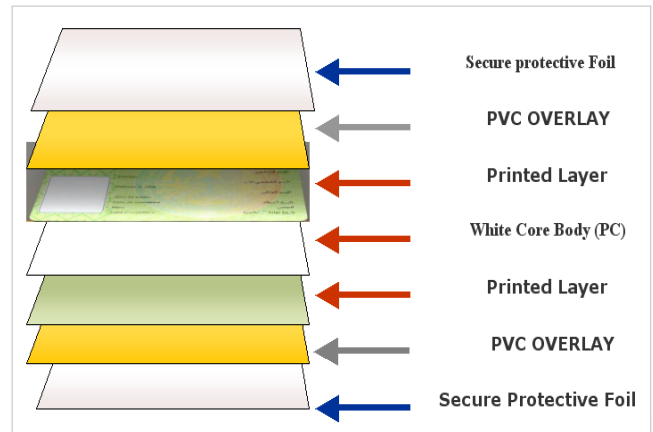
It will also include the selection of appropriate card technology, development of card applications, card personalization set up, card and application life cycle management, complete issuance and re-issuance processes, and the management of the card life cycle and business rules between applications.

To ensure that the staff will be qualified in operations and maintenance of the whole system, Electronia will provide professional training to assigned staff and workforce, in native language or English.

Electronia's National ID solution constitutes the most cost-effective, reliable, secure, and fully integrated identification Smart Card system, capable of expanding to multiple applications as the need arises in the future.

## Benefits

- State-of-the art, highly secure architecture, durable 4KB Contactless Smart Card, capable of future enhancement and upgrades
- USB read/write devices with Secure PIN pad compliant to open standards and supporting bilingual user interface
- Smart card supports contactless interfaces
- Data Card Centralized Printer capable of double sided printing at 3000 cards/day including lamination
- Envelope and form printer (1000 cards/hour) that prints an envelope and KMS PIN
- Card delivery system inserts card, creates audit trail and tracks rejected cards
- Middleware custom designed for data integration
- Open platform framework CMS including a personalization manager for the personalization preparation process
- Multi-application, centrally controlled system
- EISmart Kiosk that integrates a high-end Pentium PC, touch sensitive screen, Windows OS, Smart card reader, application software, fingerprint verification module and connectivity option such as Ethernet TCP/IP or dial-up modem
- Branded Pentium PC with 17" LCD monitor
- Digital camera with tripod assembly and PC based Control
- Flatbed scanner
- Electronic signature capture and verifier pad



*National ID Card Security Layers*

- **Encryption** - Provides confidentiality across networks.
- **Authorization** - Grants access to identify individuals to system resources or services.
- **Digital Signature** - Ensures that a transaction between two parties is binding.
- **Identity and Security Management** - Automates security seamlessly and transparently across applications and platforms.

## Unique Features

- Off-the-Shelf Hardware and Software
- Exceptional Print Durability
- User Friendly, Durable Kiosk Configuration
- Custom-Designed Middleware
- Implementation Phases
- Detailed Requirement Analysis

## SECURITY: KMS Security Features

The Key Management System (KMS) used in EISmart National ID is based on the most comprehensive, robust, and scalable suite of enhanced security products developed by ENTRUST. This includes a wide range of products that are fully integrated within a single infrastructure.

KMS provides end-to-end security solutions for the following:

**Authentication** - Provides the ability to uniquely identify participants or recipients of an electronic transaction.

## KMS Key Components

The main components of the KMS, including the supporting applications are as follows:

- **KMS Authority Security Manager** - The Certification Authority that provides the core capability of the Public Key Infrastructure.
- **Authority Security Manager Administration** - The Registration Authority that performs KMS-related administrative tasks that can be scaled to meet specific requirements.
- **Authority Self-Administration Server** - Allows users to register and recover, suspend, reactivate their PKI digital identities in a scalable and cost-effective way via a simple web interface.
- **Enrollment Interface** - An optional interface between the Certification Authority and the Smart-card Bureau.
- **Third Party Directory Product** - The repository for digital certificates, revocation and policy information.