

# eIdentity



**eIdentity provides an innovative platform to biometrically verify identities and transactions in the internet for everyone, everywhere and anytime in a simple, fast and cost effective way.**

The platform has an open architecture based on standard WebServices (WS\*) Technology that allow amongst others an easy Integration of the eidentity process in any Identity Management Solution (IMS).

\*The eidentity consists of a personal authentication token (InternetPassport™) and a server side authentication platform.

By providing a secure channel between the protected zone of the operator and a dedicated tamper resistant personal device in form of a thick smart card, called the InternetPassport™; eidentity is able to bridge the most insecure components of the communication infrastructure. The InternetPassport™ contains numerous digital identity credentials that can be used to establish independent connections to different operators that run using eidentity, and controls the access to the credentials through a 2- or 3-factor authentication of the user.

*Note: The security level of the authentication protocol that verifies the identity of the card owner may be adapted according the transaction type on request of the operator*

## Core Differentiators

### Optical Interface



The Internet Passport™ receives messages from the operator through a communication scheme that does not need electrical or radio connection between the card and the local computer or additional infrastructure. Instead, it reads and decrypts the displayed encrypted flickering code generated by the operator. Upon authentication, the Internet Passport™ shows the user the message content and generates some one-time codes ["OTC"] on its internal display screen. The transaction is finalized when the OTC is returned to the operator.

## User side identity federation

The Internet Passport™ contains a practically arbitrary number of secured channels that can be activated whenever necessary. The user decides which operators get access to the identity credentials in his card. This shared control of the communication channels allows a very flexible realization of identity federation. By providing a user side identity management that can handle the proliferation of identity credentials for the user, eidentity is able to secure e-business both for the user and the operator.

## Encapsulated biometrics

The storage of the biometric reference template, the measurement and the comparison process are completely integrated in the InternetPassport™. The EAL4 secure chip manages on board biometric and 128 identity credential, and the card keeps the biometric data encapsulated under the full control of the owner. These remove all fears about irreversible corruption of the biometric data. Thus, the privacy of these data in the InternetPassport™ is fully protected; differentiating eidentity's solution from most other biometric identification or verification systems.

## eIdentity Technology

- High authentication security:
  - Up to 3-factor, adaptable to customer's needs
  - Closed system performs relevant computation (trusted computing device)
  - Encapsulated biometry, protecting the user's privacy
- High usability for customers and end users:
  - Simple biometric fingerprint – no complex password required
  - Operates on any terminal, anywhere – no installation of specialized hard-/software on the user client infrastructure.
  - One card manages secure transactions to multiple providers using different and independent credentials for each provider

