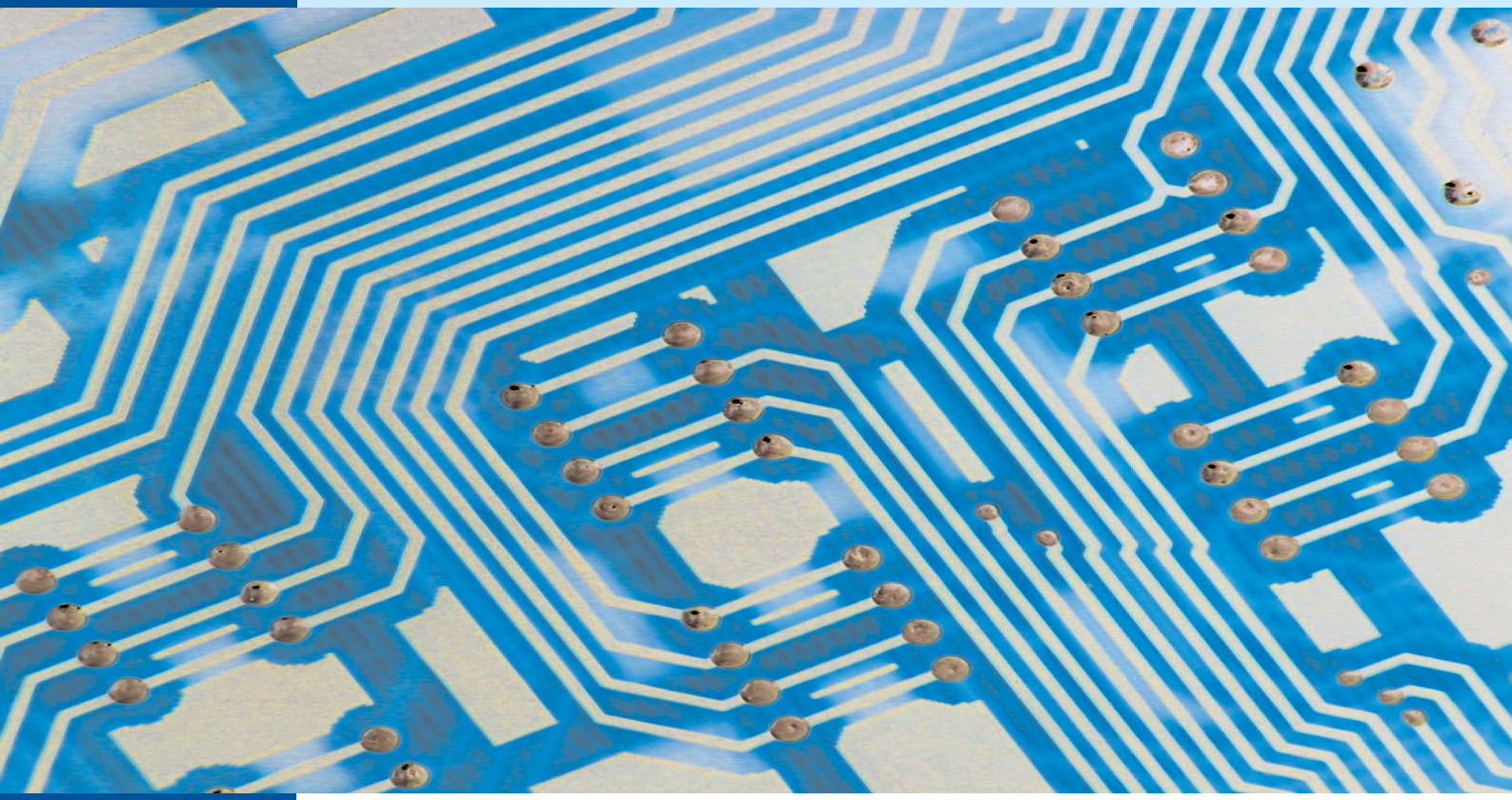
Iteon



Comyt

Smart card based authentication in an OATH environment

Strong authentication, which requires users to possess a second, physical factor in addition to a password or PIN, is essential to protect against the various forms of security attacks prevalent today.

However the lack of standardisation for two-factor technologies made it too expensive and inflexible for broad-based deployment.

To address these issues industry leaders decided to collaborate, endorsed the Open Authentication Reference Architecture (OATH) and developed a new algorithm for the generation of One Time Passwords.

Comyt products are the first available smart cards to propose this new algorithm.

Comyt smart cards are highly secure, easy to use products making it possible to generate OATH compliant One Time Passwords on a large variety of devices such as personal computers, handheld tokens or mobile phones, and to verify them in authentication servers. They embed security mechanisms such as secure messaging and PIN protection.

The Comyt smart card can be used on any device capable of reading a smart card to securely generate OTPs.

Comyt can also be embedded in a mobile phone SIM Toolkit technology, allowing users to use their standard handset as a, authentication device.

To authenticate users, *myHSM* - a low cost, easy-to-use security module - can be integrated in authentication servers to securely store secret data.

oath
initiative for open authentication

Java Card applet

The Comyt application is the first available implementation of the OATH HOTP standard algorithm in a smart card environment.

The algorithm used to generate one-time passwords is based on SHA-1 and HMAC known, standardised and proven primitives and uses a shared secret key.

In addition to OATH HOTP standard, Comyt also offers secure key provisioning, authentication in challenge - response mode, PIN code protection and resynchronisation mechanism.

myHSM OATH extensions

myHSM, the smart card based security module, provides all the characteristics of a standard Hardware Security Module for only a fraction of the price of other HSMs. The use of a standard smart card platform instead of proprietary hardware allows *myHSM* to offer great security at a low price.

myHSM is based on a flexible architecture allowing for the integration of new cryptographic algorithms or security methods.

myHSM OATH extensions, extend *myHSM* features in order to make it possible to verify the validity of an OATH HOTP.

Comyt SIM Toolkit applet

Comyt is available as a totally customizable Java Card SIM Toolkit applet ready to be loaded on SIM Toolkit capable cards.

In addition to standard Comyt advantages, Comyt SIM Toolkit applet is an easy to deploy, stand alone product, with a minimal footprint.

Technical characteristics

- ISO 7816 smart cards
- Java Card 2.1, Open Platform 2.0.1'
- OATH HOTP Algorithm, October 2004

OATH

The Initiative for Open AuTHentication (OATH) is a collaboration of leading device, platform and application companies. OATH participants hope to foster use of strong authentication across networks, devices and applications. OATH participants work collectively to facilitate standards work and build a reference architecture for open authentication while evangelizing the benefits of strong interoperable authentication in a networked world.

oath
initiative for open authentication

Iteon
6, rue Camille-Desmoulins
92300 Levallois-Perret - France

Phone: +33.1.5676.6026
Fax: +33.1.7071.9219

Email: info@iteon.net

www.iteon.net