



## CONTROLLO ACCESSI LOGICI • ID-POCKET

### LOGICAL ACCESS CONTROL • ID-POCKET

L'introduzione sul mercato dei nuovi dispositivi di autenticazione ha portato alla diffusione di sistemi di firma digitale basati su card a microchip che, pur consentendo elevati standard di sicurezza per l'accesso ai certificati di firma, hanno tuttavia nel PIN il loro punto debole.

A tale scopo Italdata ha realizzato il sistema **ID-Pocket**, che utilizza la biometria come tecnologia sia per il controllo degli accessi ai sistemi informativi, che per l'apposizione della firma digitale e per la gestione delle transazioni "sicure". Il sistema è in grado di garantire la tutela ed il controllo dei dati personali nel rispetto della privacy, e di evitare all'operatore la memorizzazione di credenziali (username e password) necessarie per accedere a qualsiasi applicazione in rete, eludendo così il rischio di farsi estorcere le informazioni riservate.

*The entry onto the market of new authentication devices has driven the diffusion of digital signature solutions based on microchip cards. While these systems provide excellent signature certificate access security, they require the use of a PIN number, which represents their Achilles' heel.*

*As a response to this issue, Italdata has developed **ID-Pocket**, a device which uses biometric technology to control access to information systems, attach digital signatures and manage "secure" transactions. This solution protects and controls personal data in compliance with privacy regulations, without requiring users to memorise credentials (username and password) to access online applications, making it impossible for this confidential information to be obtained by fraudulent means or extortion.*



ID-Pocket

## CARATTERISTICHE E CAMPI DI APPLICAZIONE

ID-Pocket è un dispositivo che abilita e protegge l'accesso logico ai sistemi informativi (postazioni di lavoro e server) attraverso un processo di autenticazione biometrica, confrontando l'impronta digitale con la rappresentazione matematica (template) immagazzinato all'interno della smart card in possesso dell'utilizzatore, rendendone così più sicuro il suo riconoscimento. ID-Pocket può essere impiegato ovunque sia richiesta l'autenticazione certa dell'utente, espletando diverse funzionalità, quali:

- la gestione della postazione costantemente controllata dal dispositivo in tutte le fasi operative, dall'accesso alla disconnessione della stessa, passando per il blocco dell'utente in caso di estrazione della smart card o di time out per inattività
- l'accesso a reti condivise tramite autenticazione
- l'accesso a siti web protetti (es. home banking) tramite certificati digitali
- la firma digitale/cifratura di e-mail e di documenti elettronici.

## METODOLOGIA DI AUTENTICAZIONE

L'autenticazione biometrica avviene esclusivamente all'interno del dispositivo (matching on device): in questo modo le informazioni più delicate del processo non possono essere in alcun modo intercettate tramite sistemi di intrusione (sniffer) né replicate. Tale meccanismo, oltre a garantire un elevato livello di sicurezza, rispetta i vincoli legislativi relativi alla privacy: l'utente, infatti, porta con sé i propri dati biometrici, senza lasciare traccia all'interno del dispositivo.

Durante le fasi operative, di registrazione e/o di verifica biometrica, sul display vengono visualizzati opportuni messaggi che guidano l'utente nel corretto posizionamento del dito sul sensore di lettura. La durata media di un processo di identificazione è di circa 2/3 secondi.

### BENEFICI

- **Riservatezza dati utente**
- **Abilitazione selettiva utente**
- **Firma elettronica**
- **Matching on device**

## SYSTEM FEATURES AND FIELDS OF APPLICATION

The ID-Pocket device enables and protects logical access to information systems (workstations and servers) by means of biometric authentication, or the comparison of a live scanned digital fingerprint with the mathematical template stored in a smart card held by the user, making recognition much more secure.

The device can be used in all circumstances in which certain (biometrically guaranteed) user authentication is required to perform various functions:

- constant monitoring of work station management throughout all operating stages, from access to disconnection, including user blocking in the event of smart card removal or inactivity time out
- authenticated access to shared networks
- digital certificate based access to protected web sites (home banking)
- digital signing/encryption of e-mail and electronic documents.

## AUTHENTICATION METHOD

Biometric authentication takes place exclusively inside the device (matching on device), making it impossible for the sensitive information used in the process to be intercepted by "sniffer" intrusion systems or replicated. This mechanism, as well as delivering a high level of security, is in perfect compliance with current privacy legislation, because each user carries their own biometric data with them, without leaving any traces in the device. During registration and/or biometric verification, messages are displayed to guide users through the process of correctly positioning their finger on the scanner. Identification requires 2/3 minutes on average to perform.

### BENEFITS

- **User data confidentiality**
- **Selective user enabling**
- **Electronic signature**
- **Matching on device**



00128 Roma - Viale degli Eroi di Cefalonia 123  
Tel. +39 06 50797837 Fax +39 06 5087834  
e-mail: italdata@italdata-roma.com www.italdata-roma.com

