

## SecureAccess

SecureAccess sostituisce Microsoft G.I.N.A. consentendo all'utente l'autenticazione tramite smartcard nel dominio o sul PC locale.

SecureAccess semplifica e protegge la normale procedura per effettuare il logon al PC, utilizzando una smartcard e l'impronta digitale. La smartcard può contenere più di un set di credenziali accessibili solamente tramite l'utilizzo della propria impronta digitale o del PIN. L'utilizzo dell'impronta o del PIN dipende dalla precedente inizializzazione della smartcard.

L'accesso può avvenire tramite le credenziali (nome utente e password) che sono memorizzate nella smartcard oppure tramite i certificati validi per lo Smartcard Logon.

Generalmente una corretta policy della password prevede l'utilizzo di una password complessa con scadenza mensile, SecureAccess aggiunge un altro fattore di sicurezza : la *One-Time Password*. Secondo le comuni policy della password, ogni volta che l'utente effettua un accesso sul dominio o sul PC locale, viene generata una password casuale formata da quattordici caratteri scelti tra lettere maiuscole e minuscole, numeri e caratteri speciali.

SecureAccess inoltre aggiunge una protezione all'utente che utilizza la smartcard. Quando l'utente abbandonerà la postazione, gli basterà rimuovere la carta dal lettore e SecureAccess bloccherà automaticamente il PC oppure provocherà la disconnessione di quell'utente.. Nel primo caso, solamente il possessore della smartcard, dopo verifica dell'impronta digitale, può sbloccare il PC. SecureAccess controlla analogamente lo stato dello screen saver.

SecureAccess utilizza Siemens CardOS API per comunicare con le smartcard Siemens; in particolare, SecureAccess utilizza l'interfaccia PKCS#11.

SecureAccess, per l'autenticazione biometrica, utilizza la tecnica proprietaria di Precise Biometrics *Precise Match On Card*: il dato biometrico (template) risiede nella smartcard che effettua il confronto. Utilizzando poi i lettori della serie Precise 200, anche la creazione del template avviene all'interno del lettore e quindi nessun dato biometrico esce dall'accoppiata lettore-smartcard massimizzando così sicurezza e privacy: infatti il dato biometrico è sempre e solo sotto il diretto controllo del suo proprietario, che possiede la smartcard; nessun dato biometrico viene registrato né nel client né nel server.