Server Strong Authentication Protiva

Una piattaforma di autenticazione flessibile

AZIENDA > PRODOTTO

Nomi utente e password non sono più sufficientemente sicuri per proteggere le risorse dati dai furti di dati informatici. Dal momento che il cybercrimine e le minacce on-line continuano a diventare sempre più sofisticati, l'unico modo per proteggere i dati della propria società è creare nuovi livelli di autenticazione che vi permettano di sapere in ogni momento chi accede alla vostra rete. Il server Strong Authentication (SA) Protiva di Gemalto offre questa maggiore protezione e si presenta come una piattaforma di autenticazione facile da implementare e da utilizzare.

Al fine di soddisfare le esigenze di ogni singola azienda, il server SA Protiva supporta un ampio portfolio di dispositivi per un'adeguata autenticazione contro i rischi. Questo portfolio spazia dalla tecnologia One Time Password (OTP) al supporto di una soluzione PKI (Public Key Infrastructure) completa basata su smart card. Questa gamma di dispositivi offre agli amministratori IT la flessibilità necessaria per proporre diversi dispositivi di autenticazione in base alle esigenze del cliente, gestiti da un unico server di autenticazione. Questa soluzione fornisce anche un semplice percorso di migrazione da

- **Facile da implementare**
- **Usa l'infrastruttura esistente**
- **Licenza per utenti finali flessibile e riutilizzabile**
- **Portfolio scalabile di dispositivi di autenticazione (OTP – PKI)**

OTP a PKI senza bisogno di cambiare i dispositivi o il server di autenticazione. L'implementazione PKI ottenuta mediante un plugin al Forefront Identity Manager di Microsoft permette di gestire tutto da un'unica interfaccia.

Un semplicissimo wizard guida all'installazione di un server SA Protiva specificando il percorso di installazione, le informazioni amministrative, i data server e le selezioni LDAP. Una volta implementato, un'interfaccia web-based consentirà di gestire gli account e l'hardware dell'utente finale in modo assolutamente semplice.

Il server SA Protiva consiste nei seguenti componenti:

- Moduli di autenticazione che provvedono alla convalida dell'utente finale utilizzando One-Time Password
- Un'interfaccia Customer-Care riservata agli amministratori per la gestione di dispositivi degli utenti finali Gemalto, politiche di autenticazione, ruoli, utenti, chiavi e altre funzioni
- Un'interfaccia per l'utente utilizzatore che permette la registrazione e la gestione delle proprie password e le informazioni sul proprio account.

gemalto
security to be free

Server Strong Authentication Protiva

Una piattaforma di autenticazione flessibile

Uso dell'infrastruttura di rete pre-esistente

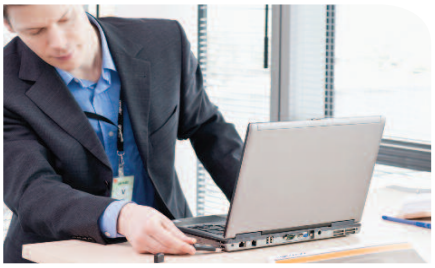
Il server SA Protiva funziona con svariati sistemi operativi e configurazioni server. I moduli del server SA supportano i protocolli standard del settore garantendo quindi un'integrazione senza problemi in architetture pre-esistenti tra cui RADIUS (Remote Authentication Dial-In Server), AAA (Authentication, Authorization and Accounting) e server per applicazioni Web.

Al fine di fornire il livello più avanzato di protezione dell'identità degli utenti, il server SA Protiva ha integrato un modulo di sicurezza software oppure un modulo di sicurezza hardware esterno (HSM) è collegato ad un server di autenticazione per memorizzare e utilizzare chiavi crittografiche. Utilizzando framework e protocolli standard quali HTTP/HTTPS e RADIUS i moduli di autenticazione interagiscono con i server dati pre-esistenti in modo da conservare e aggiornare le informazioni di autenticazione dell'utente. Sono supportate svariate opzioni di server dati tra cui MySQL, Firebird e directory LDAP quali Microsoft Windows Active Directory.

Fornitura, gestione e permessi agli utenti finali

Il portale di assistenza clienti del server SA Protiva prevede tre opzioni di fornitura e gestione dei dispositivi smart card e delle credenziali di autenticazione degli utenti finali: batch client provisioning, Customer Care Interface e live provisioning. Il batch client provisioning permette agli amministratori di creare simultaneamente diverse registrazioni di dispositivi e di attivare più utenti. Ciò è particolarmente utile in caso di configurazione di un nuovo sistema poiché in un'unica fase è possibile abilitare un gran numero di registrazioni di dispositivi.

Il portale di customer care basato sul web supporta funzioni amministrative per la gestione degli utenti e dei loro



privilegi di accesso, dei dispositivi smart card e delle transazioni di sistema tra cui la creazione o l'aggiornamento della registrazione di un dispositivo, il collegamento di una registrazione ad un utente e l'attivazione del dispositivo. Il portale di customer care supporta anche il Live Provisioning, un modo rapido e conveniente di personalizzare un nuovo dispositivo Gemalto o di riutilizzare un dispositivo pre-esistente.

Il server SA Protiva permette inoltre agli utenti finali di gestire operazioni di routine per mezzo di un portale self-service. Questo portale è incorporato nell'applicazione web del server SA e può essere personalizzato in modo da supportare l'accesso dell'utente finale alle appropriate funzioni del server SA.

Integrazioni per il server SA Protiva

SO:
- Windows Server 2003
- Windows Server 2008
- Red Hat Linux

Metodi di autenticazione:
Il server SA si avvale dei seguenti metodi di autenticazione principale:
- OATH HOTP (Event based, Time based)
- SMS OTP
- Mobile Time based OTP
- EMV CAP

Server web:
- Apache Tomcat

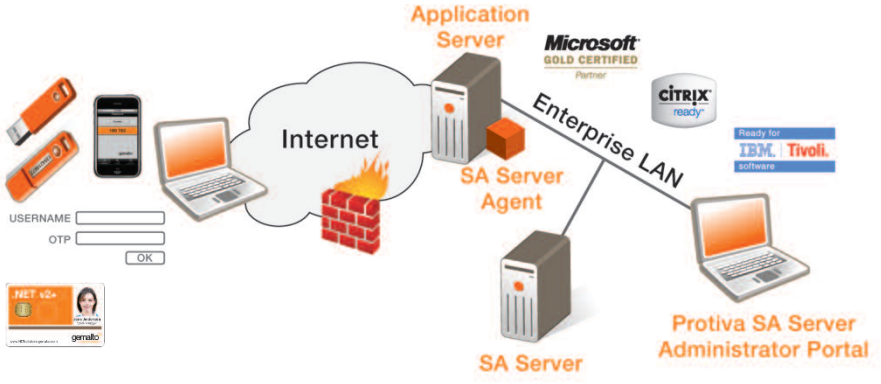
L'architettura scelta consente di impostare le configurazioni "High Availability" e "Fail-Over" a seconda dei sistemi operativi, dei database e dei meccanismi di monitoraggio.

Database:
Il server SA memorizza i dati relativo all'OTP e se necessario anche i dati utente (modalità DB) in:
- Firebird
- MySQL
- MS SQL
- Oracle
- IBM DB2 (Windows o AIX)
- Mediante uno sviluppo specifico può essere supportato qualsiasi altro database SQL

Repository utente:
Il server SA può essere collegato ai seguenti LDAP quando gli account utente vengono gestiti esternamente (modalità mista):
- Microsoft Active Directory
- Novell eDirectory
- Sun One
- Open LDAP
- Mediante uno sviluppo specifico può essere supportato qualsiasi altro LDAP

Interfaccia dei servizi di autenticazione:
I servizi di autenticazione vengono integrati utilizzando le seguenti interfacce:
- Richieste HTTP o HTTPS,
- Richiesta XML inviata a Web API,
- Richieste RADIUS mediante il server SA Agenti RADIUS per
- Microsoft IAS o NPS (Windows Server 2008)
- Juniper Steel Belted RADIUS,
- FreeRADIUS

Architettura del server SA



gemalto
security to be free