



FINMATICA INFORMATION SECURITY

E' la divisione di Finmatica specializzata nella progettazione e sviluppo di prodotti e soluzioni per la tutela del Patrimonio Informativo Aziendale dal punto di vista delle tecnologie, degli standard e delle normative.

La suite di prodotti Finmatica Information Security include soluzioni per la protezione delle informazioni, delle comunicazioni e delle risorse informatiche aziendali, che garantiscono:

- la confidenzialità delle comunicazioni e dei messaggi
- l'integrità delle informazioni
- la non ripudiabilità dei documenti
- l'autenticazione forte degli utenti per l'accesso alle risorse

Information Security

Concierge

L'infrastruttura per la messa in sicurezza del patrimonio informativo

Concierge è la soluzione che Finmatica propone per la realizzazione di una infrastruttura a chiave pubblica leggera. Uno dei principali problemi in cui solitamente si imbattono le organizzazioni nell'abilitazione di tali tipi di strumenti di sicurezza informatica è la gestione delle chiavi private, che implica notevoli investimenti in risorse umane e finanziarie. Concierge riduce drasticamente il peso di attività quali configurazione e manutenzione delle postazioni di lavoro, rendendole immediatamente operative ed eliminando la necessità di investimenti in dispositivi da distribuire ai singoli utenti, mantenendo il massimo livello di sicurezza delle chiavi private.

Concierge consente la generazione delle chiavi e la distribuzione dei certificati digitali in modo rapido ed efficace. Le tecniche di distribuzione e l'utilizzo di protocolli standard garantiscono l'integrazione immediata e trasparente dei certificati digitali con le più comuni e diffuse applicazioni basate su una infrastruttura a chiave pubblica (PKI), come ad esempio S/MIME per la messa in sicurezza delle comunicazioni via e-mail.

La facilità e la robustezza dell'uso dei certificati digitali è sicuramente un fattore abilitante per l'adozione dell'infrastruttura stessa. Concierge aiuta le organizzazioni che vogliono introdurre l'utilizzo di una PKI al loro interno, riducendo l'impatto sul lavoro quotidiano grazie alla sua integrazione con il sistema operativo.

L'ergonomia della soluzione permette agli utenti di Concierge di firmare e cifrare documenti, e di utilizzare tutte le funzionalità proprie di una infrastruttura a chiave pubblica senza che questi posseggano conoscenze tecniche specifiche. In tal senso Concierge può essere considerato alla stregua di un normale dispositivo crittografico, quali smartcard e token, ma di utilizzo estremamente più semplice.

▲ Concierge risulta utile in tutti quei contesti in cui sia necessario:

- evitare di memorizzare la propria chiave privata su un supporto fisico. La chiave privata sarà custodita su un server protetto e sarà disponibile in qualsiasi momento e in qualsiasi luogo si trovi il proprietario (caratteristica particolarmente utile per i cosiddetti utenti roaming)
- distribuire certificati digitali in modo rapido ed efficace all'interno di una comunità chiusa di utenti
- abilitare l'utilizzo di nuovi strumenti software per la sicurezza in contesti lavorativi in cui le conoscenze informatiche sono molto ridotte
- eliminare la proliferazione di password necessarie per la cifratura e l'autenticazione a chiave simmetrica garantendo livelli di sicurezza comparabili
- utilizzare una PKI perfettamente interoperabile tra ambienti eterogenei quali Microsoft, Linux, AIX, ecc.

▲ Il modulo Concierge Key Server fornisce le funzionalità tipiche di una Certification Authority:

- generazione di certificati digitali secondo la raccomandazione ISO X.509
- revoca di un certificato digitale Concierge
- interfaccia Web-based per la registrazione di nuovi utenti (Web enrollment)
- produzione e distribuzione della Certificate Revocation List (CRL) via LDAP
- accesso al database dei profili utente attraverso interfaccia LDAP
- funzioni remote per l'accesso ai certificati via protocollo SOAP

▲ Il modulo Concierge Virtual Token mette a disposizione dell'utente, in modo semplice e immediato, tutte le funzionalità tipiche di un crittosistema:

- accesso trasparente ai certificati digitali e alla chiave privata distribuita attraverso Concierge Server mediante due implementazioni conformi rispettivamente allo standard CSP di Microsoft e allo standard PKCS#11 per le comunità di utenti di sistemi open
- funzioni crittografiche di base per firma e cifratura
- funzioni di amministrazione delle policy per la sicurezza mediante pannello di controllo
- funzionalità di base per le modalità di lavoro off-line con caching delle chiavi



Via Sorbanella, 30 - 25125 - Brescia - Italia
Tel +39 030 35161 - Fax +39 030 3516700
finmatica@finmatica.com
www.finmatica.com