

## **Consulenza e Implementazione di Soluzioni PKI** *Public Key Infrastructure*

**La soluzione che garantisce un flusso di comunicazione sicuro in ambito Internet, Intranet ed Extranet**

### **Area: Infrastrutture IT**

**Tipologia servizi:** Architetture di sicurezza

### **Scenario**

La sempre più strategica necessità di identificazione certa dell'utente che esegue una qualsiasi operazione in rete, sia essa una transazione commerciale o l'accesso a informazioni riservate, così come l'esigenza fondamentale di proteggere le informazioni stesse in transito su internet, hanno messo in evidenza le lacune dei tradizionali meccanismi di autenticazione e protezione. Internet infatti è nata e si è sviluppata senza tenere presente alcuna esigenza di sicurezza; d'altro canto le sue caratteristiche di facilità di accesso e disponibilità hanno portato allo sviluppo di una serie di servizi per i quali la sicurezza è un requisito fondamentale.

I meccanismi di autenticazione ed encryption legati a soluzioni di Public Key Infrastructure, rappresentano attualmente la soluzione tecnologica più idonea per risolvere i problemi di sicurezza legati alle comunicazioni in ambito Internet, Extranet ed Intranet.

### **Soluzione : Public Key Infrastructure**

Implementare una PKI significa predisporre una serie di servizi di infrastruttura volti all'emissione, rinnovo, revoca e pubblicazione di certificati digitali da distribuire ai propri utenti. I certificati possono essere emessi dall'azienda stessa per i propri dipendenti oppure acquistati da terze parti (ad esempio Verisign o Infocamere).

I certificati digitali provano inequivocabilmente l'identità dell'utente o del computer al quale sono stati rilasciati. Utilizzando una tecnologia a chiavi asimmetriche, rappresentano la soluzione tecnologicamente più avanzata sul mercato per firmare digitalmente o criptare documenti e posta elettronica oppure per accedere a siti web sicuri o a reti remote. Il certificato digitale costituisce la base dell'architettura PKI ed è uno standard industriale definito nelle specifiche X.509 v.3 rilasciate da ITU-T.

Le funzionalità della PKI vengono a loro volta standardizzate nella RFC 2459 definita di IETF. Questi standard garantiscono che le soluzioni che li rispettano siano interoperabili fra di loro.

Tramite una PKI ben implementata sarà possibile rendere sicuri e sfruttabili da chiunque una grande quantità di servizi:

- firma digitale
- logon sicuro (anche tramite smart card) alla LAN, a siti web o a sistemi VPN
- e-mail sicura
- transazioni protette su https

Utilizzando la tecnologia fornita da PKI, ad esempio, due utenti possono scambiarsi e-mail protetta, essendo certi allo stesso tempo che nessuno possa intercettare il contenuto del messaggio e che quest'ultimo provenga dal reale interlocutore. In ambito web, ancora, possiamo garantire la privatezza di una transazione, ma anche l'identità sia dell'utente che esegue la transazione stessa sia dell'organizzazione presso cui la transazione viene eseguita. PKI fornisce quindi in maniera trasparente i servizi di autenticazione, integrità e confidenzialità, integrandosi con l'infrastruttura di rete preesistente.

### **Implementazione**

Implementare una soluzione PKI richiede un'accurata analisi degli scopi da raggiungere e un'attenta valutazione delle soluzioni già presenti con cui integrarsi. Una buona soluzione PKI dovrà essere trasparente garantendo però allo stesso tempo elevati standard di sicurezza.

### **La nostra offerta**

Alya, grazie all'esperienza accumulata nell'analisi e nell'implementazione di sistemi informativi a tutti i livelli, è in grado di aiutare l'azienda nella progettazione, pianificazione e nell'implementazione della propria soluzione PKI.

La nostra consulenza si estende dallo studio e implementazione di soluzioni basate su servizi Certification Authority di Windows 2000 fino all'assistenza nel deployment di soluzioni Verisign, considerando anche la possibilità di implementazioni miste.

Particolare attenzione viene posta nell'integrazione della soluzione PKI con le altre infrastrutture presenti e nello sviluppo di soluzioni aperte alle evoluzioni che il mercato e la tecnologia richiedono.

### **alya Tecnologie Integrate**

System integrator per l'azienda digitale.

Dal 1994, la nostra missione è fare delle tecnologie ICT una priorità strategica per il vantaggio competitivo dell'Azienda.

Integriamo competenze, prodotti e metodologie per realizzare architetture e soluzioni di business funzionali, scalabili e sostenibili lavorando in partnership con il committente per ottenere, assieme, il massimo del risultato.

Alya ha partecipato al Rapid Deployment Program di Microsoft Windows Server 2003.

Microsoft Certified Partner.