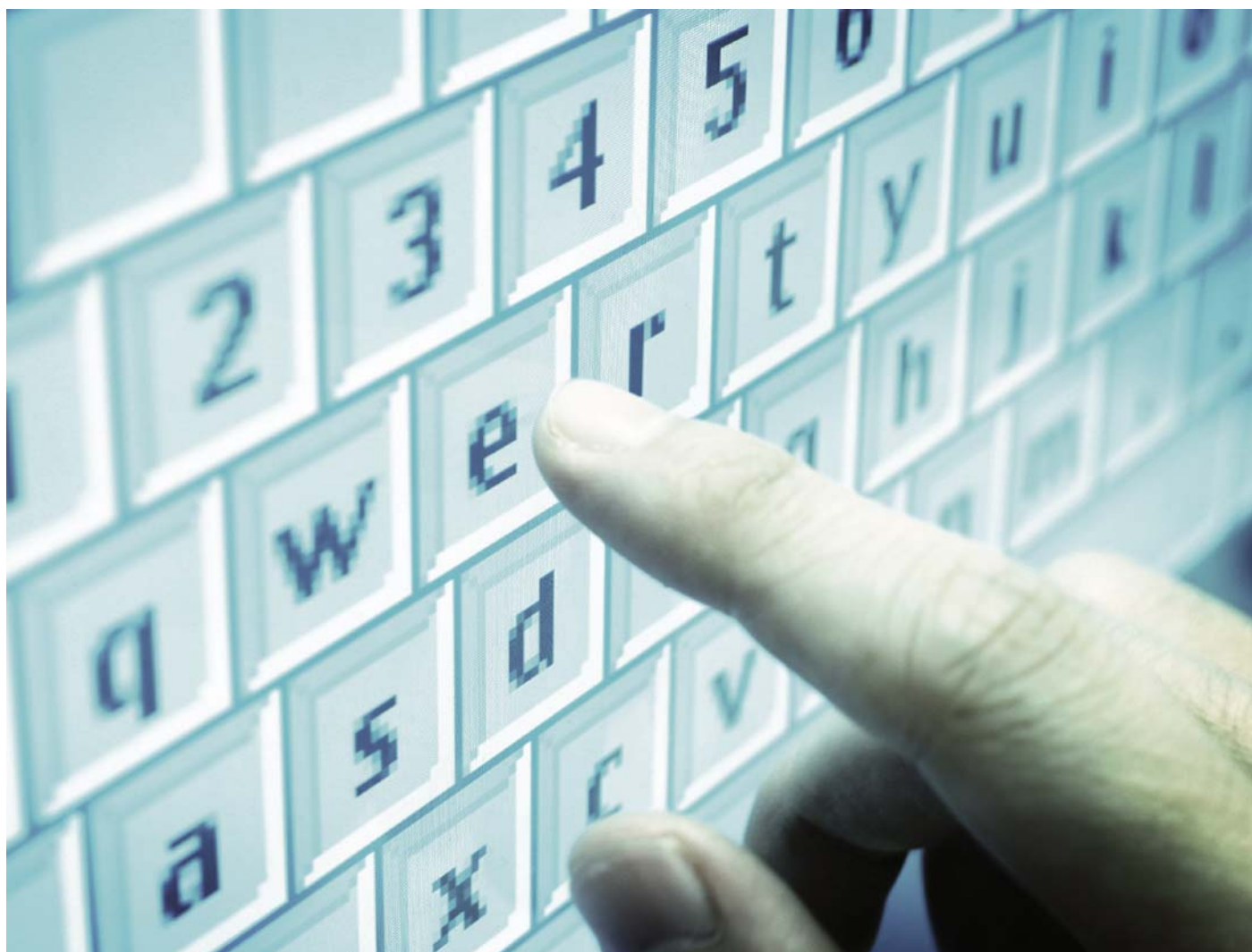


## CryptoAccelerator

### La firma digitale

La soluzione semplice, veloce e sicura per garantire l'autenticità, l'integrità e la non ripudiabilità dei documenti



## Le nuove esigenze aziendali

Durante gli ultimi anni l'informatizzazione dei processi, lo scambio documentale di file e l'invio via web di dati sensibili sono diventati parte integrante e imprescindibile delle attività aziendali.

Questo ha consentito una più **efficace gestione dei flussi documentali** e un netto **risparmio di tempo e di denaro** per le aziende, ma ha anche reso necessaria **l'introduzione di nuove normative** per la fatturazione elettronica, la conservazione sostitutiva a norma, la firma di disposizioni bancarie e in ambito CBI, etc...

Pertanto è diventato essenziale avere uno strumento sicuro per le operazioni di **firma digitale, le richieste di apposizione/verifica della marca temporale, la verifica dei certificati** al fine di garantire l'autenticità, l'integrità e la non ripudiabilità dei documenti.

Ad oggi, le principali soluzioni adottate utilizzano **dispositivi crittografici, che necessitano componenti software** da integrare con le proprie applicazioni con conseguenti difficoltà dovute all'installazione, alla compatibilità alla scalabilità.

**CryptoAccelerator** supera queste difficoltà affermandosi come la soluzione più semplice, più completa e meno invasiva.

# CryptoAccelerator

CryptoAccelerator è in grado di firmare in modalità **"massiva", centralizzata e semplificata** grandi volumi di documenti tramite qualsiasi dispositivo sicuro normalmente utilizzato e connesso al server (smart card, token, HSM) e di apporre firme multiple sullo stesso documento.

La soluzione offre un provider completo per i servizi di firma digitale che combina tecnologia hardware e software integrandosi così in maniera non invasiva all'infrastruttura aziendale esistente ed eliminando di conseguenza i colli di bottiglia nei processi di sicurezza.

CryptoAccelerator è il nuovo punto di riferimento al quale delegare il colloquio con i servizi di Authority:

- **Certification**
- **Time Stamping**
- **Validation (CRL)**

## Come funziona

### Architettura

L'architettura della piattaforma è assolutamente modulare e integrabile. Essa dispone di una serie di interfacce che la rendono una soluzione ideale per l'interoperabilità con qualsiasi applicativo sia esso interno od esterno all'azienda ed in diversi ambienti.

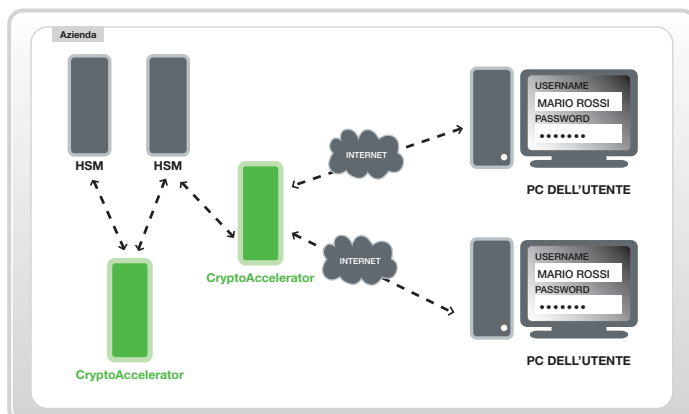
CryptoAccelerator utilizza linguaggi **C++ e Java** per lo sviluppo e **web services** lato front-end per la comunicazione fra client e server che consentono l'utilizzo del protocollo **HTTP o HTTPS** e semplificano la pubblicazione del servizio in ambito internet.

Oltre al server è disponibile un'applicazione client per la firma di uno o più documenti (treno di firme) e relative API in formato libreria per poter integrare in maniera veloce applicazioni esistenti.

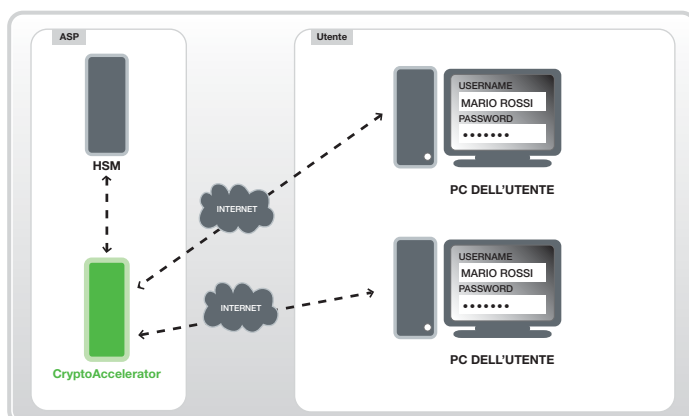
### Compatibilità

CryptoAccelerator è compatibile con qualsiasi apparato che segua gli standard **PKCS#11**.

Tale standard è utilizzato dalla maggior parte dei sistemi sicuri: Smart Card/Token delle CA più diffuse e dai dispositivi HSM (Hardware Security Module)



CryptoAccelerator in house



CryptoAccelerator in ASP

## Interfaccia di gestione

CryptoAccelerator dispone di una **semplice ed intuitiva interfaccia grafica web-based** per la configurazione e la manutenzione anche da remoto e da qualunque PC (Windows, Unix, Linux, ecc).

## Controllo liste di revoca (CRL)

La piattaforma, ad intervalli regolari prefissati ed in maniera del tutto trasparente ed automatica, effettua una copia locale delle CRL di diversi certificatori. Tale gestione centralizzata garantisce una riduzione dei tempi in questa fase evitando l'accesso online alle CRL.

# Sicurezza

Il Server di CryptoAccelerator utilizza una banca dati "locale" dove mantiene le informazioni relative alle utenze, questo gli consente di **gestire diversi utenti contemporaneamente**, quindi più chiavi e certificati allo stesso tempo indirizzando correttamente le richieste.

La banca dati "locale" è basata su database relazionale (RDBMS) tra i più utilizzati al mondo (Oracle, Postgres, MS SQL, etc...) e con **standard di sicurezza tra i più elevati**.

Al fine di garantire la sicurezza dei certificati il server identifica una serie di amministratori che hanno il privilegio di definire gli utenti ed associare i certificati. Ogni utenza è anche protetta da password, obbligatoria per accedere a tutti i servizi web esposti.

L'accesso è reso sicuro mediante preliminare fase di autenticazione (utente/password) e rilascio di un ID univoco di sessione utilizzato nelle fasi successive. L'utente titolare è comunque in grado di controllare (attivare, disattivare, sospendere, ecc) i propri certificati tramite un'interfaccia web.

Per maggiori informazioni [www.aliaslab.net](http://www.aliaslab.net)

## Vantaggi

- Basso costo di integrazione
- Rapido ritorno sugli investimenti (ROI)
- Aumento delle performance dei server
- Semplice espandibilità delle funzionalità

### Aliaslab s.p.a.

Uffici  
via Cremona 27/6 - 46100 Mantova - Italy  
Ph + 39 0376 285101 F + 39 0376 263856  
Sede legale  
Galleria Passerella, 2 - 20122 Milano - Italy  
[www.aliaslab.net](http://www.aliaslab.net)

### Elaide s.r.l. Aliaslab Group

Galleria Spagna, 1 - 35127 Padova - Italy  
Ph + 39 049 4102390 F + 39 049 2108800  
[info@elaide.com](mailto:info@elaide.com)  
[www.elaide.com](http://www.elaide.com)