Trittico Srl - Via Monte Cervino, 1 - 20021 Bollate (MI)
Tel 02 38306225 - Fax 02 38307440 - www.tritticosrl.com

TRITTICO Srl

New Crypto

Sistema di sicurezza per la protezione dei dati e delle comunicazioni e per la gestione delle chiavi crittografiche.

New Crypto è un sistema software che realizza operazioni di sicurezza, consentendo di proteggere le informazioni di un'azienda sia per l'archiviazione che per la loro trasmissione a distanza.

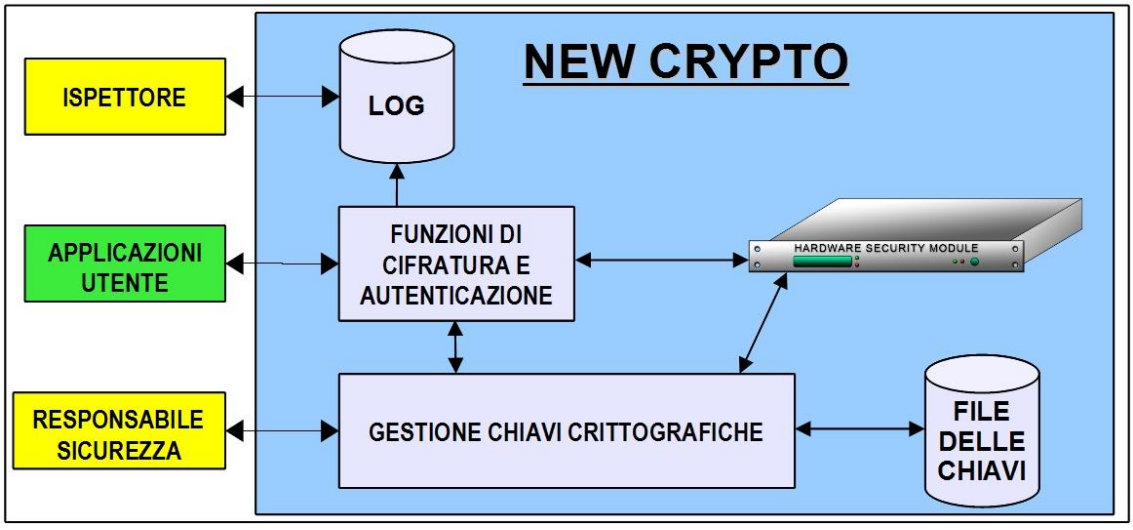
Il sistema New Crypto permette di:

- Proteggere ed archiviare ogni tipo di file e di documento digitale in modo che ne vengano preservate la riservatezza e l'integrità grazie all'utilizzo della crittografia e della firma digitale.

- Stabilire un canale sicuro per l'invio di file e documenti a distanza, proteggendo la comunicazione con l'utilizzo di protocolli e procedure collaudate, i quali garantiscono che i dati inviati rimangano protetti durante la trasmissione e possano poi essere letti e utilizzati solo da chi è in possesso della necessaria autorizzazione.

- Gestire in modo accurato ed efficiente le chiavi crittografiche coinvolte nei processi descritti, le quali rappresentano l'elemento alla base di ogni sistema che realizzi la sicurezza.

Architettura di New Crypto.



Trittico Srl - Via Monte Cervino, 1 - 20021 Bollate (MI)
Tel 02 38306225 - Fax 02 38307440 - www.tritticosrl.com

Il sistema è caratterizzato da un'applicazione software installata a livello centralizzato in ambiente mainframe, interfacciabile dai programmi applicativi per ottenere servizi di crittografia, decifratura, autenticazione e verifica degli autenticatori.

L'applicazione New Crypto comunica, tramite un modulo software, con un'apparecchiatura hardware HSM per effettuare operazioni crittografiche, utilizzando la Master Key protetta all'interno di tale dispositivo.

L'applicazione che si trova a livello centrale (ad es. nella sede dell'azienda) comunica con applicazioni software di New Crypto distribuite a livello periferico (ad es. nelle filiali) garantendo così la possibilità di scambio di dati, documenti, chiavi, ecc. in forma protetta tra le due entità collegate.
Permette inoltre lo scambio di dati con entità esterne all'azienda, previo lo scambio di chiavi con tali soggetti (quali ad esempio banche); anche queste chiavi rientreranno in modo semplice nella funzionalità di gestione chiavi del prodotto.

Dal punto di vista operativo, il Responsabile della Sicurezza ha il compito e l'autorità di gestire le chiavi crittografiche potendo generare, inserire, modificare, eliminare ed effettuare lo scambio (con i responsabili corrispondenti presenti in altre entità) di tali chiavi. Inoltre è presente la figura dell'Ispettore di LOG il quale ha la possibilità di visualizzare, ma non di modificare, il registro delle operazioni effettuate dagli utenti dell'applicazione.

La sicurezza del sistema New Crypto.

Per realizzare le funzionalità offerte da New Crypto vengono utilizzate le più recenti tecniche di cifratura ed autenticazione, ed algoritmi crittografici considerati universalmente sicuri.

Nel sistema sono integrate e coinvolte in ogni fase di lavoro le apparecchiature crittografiche HSM, Hardware Security Module, con le quali viene raggiunto un elevatissimo grado di sicurezza sia logica che fisica nella protezione delle chiavi di cifratura utilizzate e dei dati.

Grazie all'utilizzo di smart card e password personali, viene eseguita l'autenticazione forte degli utenti che accedono al sistema, rendendone certa l'identificazione. I dispositivi smart card vengono anche usati per effettuare il backup di dati sensibili.

Ogni operazione svolta viene registrata automaticamente in un LOG, memorizzato anch'esso in maniera protetta secondo precise modalità, che non ne permettono l'alterazione e lo rendono visibile solo a personale autorizzato, realizzando in questo modo un registro delle operazioni che ha inoltre un importante valore legale.