

## Key Management System

Quando si dispone di una rete di dispositivi di comunicazione cifrati, si rende necessario il compito della generazione e della distribuzione delle chiavi di cifratura ai vari elementi del network sicuro. Per ragioni di sicurezza le chiavi dovrebbero essere modificate almeno una volta al mese. E' possibile aggiornare manualmente i dispositivi, ma è piuttosto scomodo soprattutto quando i dispositivi da aggiornare sono numerosi o dislocati sul territorio o all'estero.

CasparTech presenta la miglior soluzione per la gestione centralizzata di reti di cellulari cifrati: CRYPTTECH® KMS. Fornito su un moderno e comodo notebook con controllo di accesso tramite smartcard, Cryptech KMS permette una facile e veloce distribuzione delle chiavi di cifratura ai dispositivi Cryptech. Gli aggiornamenti periodici possono essere eseguiti sia mediante cavo USB e connessione diretta con il notebook, sia attraverso l'invio automatico di SMS cifrati che in pochi minuti permettono l'aggiornamento di decine di dispositivi dislocati sul territorio.

Come in tutte le soluzioni Cryptech, viene privilegiata la sicurezza. L'intero repository centralizzato delle chiavi è mantenuto cifrato e gli aggiornamenti vengono inviati anch'essi cifrati ai dispositivi con algoritmi simmetrici. Il dati sul notebook risiedono cifrati e protetti dalla smartcard che deve essere custodita in un luogo sicuro esclusivamente dal responsabile della procedura. A richiesta l'utilizzatore può utilizzare un algoritmo proprietario per cifrare il repository delle chiavi e quelle inviate agli utenti locali o remoti.

Un generatore hardware di numeri casuali, con certificazione di sicurezza EAL5+, può essere integrato su richiesta nel sistema. Le chiavi vengono generate in maniera casuale e soltanto l'amministratore del sistema è in grado di visualizzarle. Gli utenti non possono avere visibilità sul contenuto delle chiavi di cifratura se non attraverso un valore hash, riducendo così il rischio di compromissione delle chiavi stesse.

Per fornire un totale controllo e protezione dei dispositivi, nel KMS è stata implementata la funzione di cancellazione dei dispositivi da remoto. In questo modo, in caso di furto o smarrimento dei telefoni, si può inviare un comando tramite sms cifrato che cancellerà tutti i dati nella memoria del dispositivo. In caso di sostituzione della sim, un sms con il nuovo numero e i dati per la localizzazione del telefono vengono inviati automaticamente all gestore del KMS.

Chiave	Inizio validità chiave	Fine validità chiave	Stato chiave
1 thvDuGH0H+uqbl_eVv@kMLLuv=	15/11/2006 23.00	14/12/2006 23.00	Chiave creata
2 J4Cluy4chlVR90pPmvr1186D4=	15/11/2006 23.00	14/12/2006 23.00	Chiave creata
3 K4iwnTzbx@WHbxvFvFNabc=	15/11/2006 23.00	14/12/2006 23.00	Chiave creata
4 UEZG0fzrD6PwSAvzTY~Z/Gipw=	15/11/2006 23.00	14/12/2006 23.00	Chiave creata
5 MID668rZcDq9zPULEx7F/v/c=	15/11/2006 23.00	14/12/2006 23.00	Chiave creata
6 b+QzBLSYAuz/8le/Sbc05Nag=	15/11/2006 23.00	14/12/2006 23.00	Chiave creata
7 DHAP5DUw4UvYLMN9Q4qH87J0=	15/11/2006 23.00	14/12/2006 23.00	Chiave creata

Codice IMEI	Nome dispositivo	Nome utente	Ultimo aggiornamento
1 3548172602600501	imate JAM	John	16/11/2006 11.03
2 35627260607260500	imate SP5	Jack	-
3 35638408403840400	Qtek		
4 35465072607260201	imate		
5 354726072602607	imate JAM	Albert	16/11/2006 11.03

16/11/2006h: 9.44 -> Inizio sessione utente Admin  
Aggiunto dispositivo -> imei n.ro: 35634584003458400  
Aggiunto dispositivo -> imei n.ro: 35465000803458400  
Aggiunto dispositivo -> imei n.ro: 354813458400587  
Aggiunta relazione, imei n.ro: 35481303663458400, gruppo: Sales  
Aggiunta relazione, imei n.ro: 35481303458400501, gruppo: Developers  
Aggiunta relazione, imei n.ro: 35628834584008500, gruppo: Executive  
Aggiunta relazione, imei n.ro: 35628834584008500, gruppo: Sales  
Aggiunta relazione, imei n.ro: 35638434584008400, gruppo: Executive



Il Kit CRYPTTECH KMS comprende:

- 1 notebook preconfigurato con il sistema CRYPTTECH KMS
- 1 smartcard per la protezione del sistema
- 1 cavo per la connessione USB dei dispositivi
- 1 modem per l'invio e la ricezione di SMS cifrati
- 1 manuale d'uso del sistema di generazione e distribuzione chiavi CRYPTTECH KMS

CRYPTTECH KMS funzioni standard:

- Protezione del sistema mediante smartcard di cifratura
- Ulteriore protezione del repository centralizzato delle chiavi mediante cifratura AES 256
- Gestione grafica dei gruppi e delle chiavi
- Possibilità di distribuzione delle chiavi attraverso cavo USB o invio di SMS cifrati tramite AES256
- Inserimento e visualizzazione delle chiavi di cifratura in formato HEX, ASCII, BASE64
- Cifratura End-to-End (dal KMS ai dispositivi che ricevono l'aggiornamento delle chiavi)
- Storico degli aggiornamenti per una tracciabilità delle chiavi nel tempo
- Sistema di backup sicuro delle chiavi
- Possibilità di gestire più reti di dispositivi, ognuna composta da più gruppi di appartenenza
- Possibilità di cancellazione remota delle chiavi e della memoria dei dispositivi

CRYPTTECH KMS funzioni opzionali:

- Generatore hardware crittografico di numeri casuali con certificazione EAL5+
- Personalizzazione con algoritmi proprietari su richiesta del cliente
- Possibilità di implementare un proprio algoritmo di cifratura



Un notebook di ultima generazione contiene il sistema di creazione e distribuzione chiavi avanzato. Il sistema, l'archivio chiavi e gli aggiornamenti inviati ai dispositivi sono protetti attraverso l'uso di smartcard e cifratura.

**CASPERTTECH**  
TRUST IN COMMUNICATIONS

Casper Technology s.r.l. - [www.caspertech.com](http://www.caspertech.com) - [info@caspertech.com](mailto:info@caspertech.com)  
Operation and Sales: via Cardinal G.Massaia 83 - 10147 Torino - Italia  
Tel +390112303634 - Fax +390112303632