

# 10 motivi principali per passare a payShield 10K

Il tuo payShield 9000 ti ha quasi certamente garantito un servizio prezioso e di lunga durata: ora però, per mantenersi al passo con l'innovazione nei sistemi di pagamento, sono necessari hardware di ultima generazione, gli ultimi standard di sicurezza e interventi che promuovano l'efficienza operativa. payShield 10K è la quinta generazione della nostra piattaforma HSM per i pagamenti dal 1988 ed è totalmente retrocompatibile a livello di interfaccia host per proteggere gli investimenti nelle tue applicazioni host. payShield 10K offre numerosi vantaggi. Per farti conoscere la soluzione HSM per i pagamenti di ultima generazione abbiamo compilato 10 motivi principali per effettuare subito la migrazione.



## Riduzione dei costi

### 1. Fattore di forma più snello

Lo spazio nei data center è costoso. Con payShield 10K abbiamo ridotto l'altezza dell'unità a 1U: ciò significa che puoi impilare il doppio delle unità nel rack di quanto ti permetteva payShield 9000, abbassando i costi per gli spazi. Ora l'unità è più lunga, così è più semplice arrivare ai connettori del pannello posteriore, ed è dotata di binari di scorrimento per facilitare e velocizzare il processo di installazione. Il pannello anteriore mantiene i meccanismi a destra e a sinistra già noti per bloccare l'HSM in sicurezza nel rack.

### 2. Ridotto consumo energetico

Per ogni watt di potenza necessario a un dispositivo aumentano i costi per l'energia e il raffreddamento del data center. Nella progettazione del nostro nuovo payShield 10K abbiamo sfruttato gli ultimi componenti ad alta efficienza energetica e le tecniche di gestione dell'energia per ridurre del 40% il consumo complessivo di corrente, perfino durante il funzionamento al doppio della prestazione di codifica. Questo aspetto contribuirà senza alcun dubbio ad abbattere i costi della bolletta dell'elettricità del tuo data center e aiuterà la tua azienda a raggiungere i suoi obiettivi di rispetto dell'ambiente.

### 3. Resilienza e disponibilità superiori

Il tempo di inattività programmato è sempre tempo di inattività. Essere obbligati a scollegare un HSM per eseguire interventi routinari di configurazione o per sostituire un alimentatore difettoso può influire negativamente sulla disponibilità dell'infrastruttura dei tuoi servizi finanziari. Abbiamo migliorato la struttura fisica di payShield 10K utilizzando come standard alimentatori e ventole hot swap doppi: questa scelta migliora di 14 volte l'MTBF (tempo medio tra i guasti), garantendo tempi previsti di attività molto elevati. Nel nostro obiettivo di garantirti l'operatività di payShield 10K 24 ore su 24, 7 giorni su 7, rientra il monitoraggio aggiuntivo in background dei processi del sistema HSM e del codice applicativo. Eventuali problemi rilevati vengono corretti automaticamente senza che sia necessario alcun intervento da parte tua.

## Ottimizzazione delle operazioni

### 4. Aggiornamenti del firmware più rapidi

Per caricare il firmware di solito è necessario scollegare per qualche minuto l'HSM. Il processo del flusso di lavoro per l'aggiornamento del firmware in payShield 10K è stato ridotto di oltre 10 volte, pur mantenendo tutti i controlli di sicurezza necessari per l'autenticità e l'integrità del codice. Sono stati inoltre migliorati gli aspetti di affidabilità e di facilità di utilizzo di modo che, in caso di interruzioni di corrente o di connettività, il processo di caricamento riprenda in modo automatico riducendo al minimo la possibilità che l'HSM diventi inattivo.

### 5. Indicatori visivi più chiari

Il pannello anteriore di payShield 10K è semplice e ordinato e, nel caso di una manomissione, mostra un triangolo rosso di avviso. È facile capire quando tutto funziona correttamente, perché il quadratino a sinistra nel pannello anteriore è illuminato di bianco, mentre diventa rosso se viene riscontrato un problema durante i consueti controlli in background sullo stato del dispositivo. Per aiutare a individuare quale HSM di un rack può avere bisogno di un intervento o di attenzione programmata, i team delle operazioni ora possono indirizzare il personale locale all'HSM in questione, illuminando le luci di manutenzione sul pannello anteriore e posteriore dal payShield Manager. Inoltre, la luce anteriore illumina il numero di serie dell'unità, facilitandone la lettura, se necessario. Queste sono solo alcune delle funzionalità che abbiamo integrato, anche su suggerimento di clienti, per consentire un risparmio di tempo.

### 6. Conferma più semplice della cancellazione delle chiavi

A volte è necessario spostare un HSM da un ambiente produttivo a un luogo meno sicuro. Le restrizioni dei vari audit di sicurezza impongono che quando l'unità si trova nella nuova ubicazione non debba contenere le chiavi cruciali come le LMK live. payShield 10K presenta sul pannello posteriore un'apposita spia di conferma di cancellazione delle chiavi: ciò garantisce che nessuna chiave né alcun dato sensibile siano conservati nell'unità, che quindi si può disattivare in sicurezza. Questo criterio ottimizzato fornisce una conferma di cancellazione delle chiavi anche dopo lo spegnimento dell'unità.

payShield 10K è la quinta generazione della piattaforma HSM per i pagamenti di Thales. La sua retrocompatibilità con payShield 9000 è garanzia che gli investimenti realizzati dai nostri clienti sono al sicuro.

## Tieniti pronto

### 7. Maggiore resistenza contro le manomissioni

payShield 10K presenta diversi livelli di rilevamento delle manomissioni che, quando sono attivati, cancellano le chiavi e i dati sensibili in caso di attacco. Per complicare ulteriormente a qualsiasi malintenzionato la riuscita di un attacco, viene utilizzato anche un coperchio completamente bloccato (impossibile da aprire senza danneggiare notevolmente il dispositivo). Eventuali tentativi di accesso al modulo interno di sicurezza provocano la disattivazione irreversibile del dispositivo.

### 8. Supporto di codifica più ampio

Per essere compatibile con i nuovi metodi di pagamento, payShield 10K è in grado di sfruttare l'elaborazione tramite crittografia su curve ellittiche (ECC) basata su hardware a elevata velocità oltre agli algoritmi legacy 3DES, AES ed RSA. Molti dei casi d'uso emergenti che emettono credenziali per i pagamenti utilizzano la ECC invece dell'RSA, soprattutto quando lo strumento per il pagamento è un dispositivo mobile, IoT o connesso. payShield 10K è già ottimizzato per supportare una gamma più ampia di algoritmi e di meccanismi di crittografia, man mano che le sempre più numerose specifiche di sicurezza per i pagamenti li rendono ufficiali.

### 9. Prestazione massima migliore

I pagamenti tramite carta e quelli online digitali aumentano anno dopo anno, e richiedono controlli e miglioramenti costanti della banda larga di elaborazione. payShield 10K offre prestazioni RSA e 3DES notevolmente maggiori rispetto ai predecessori, il che può ridurre il numero di dispositivi payShield utilizzati e abbattere i costi. Questo motore crittografico più veloce garantisce inoltre prestazioni più omogenee e prevedibili su tutti i comandi di host, perfino in situazioni di grande carico e quando sono in uso le comunicazioni sicure basate su TLS.

### 10. Architettura di servizio di livello superiore

Mentre il mondo dei pagamenti si rivolge sempre di più verso nuovi modelli di utilizzo che implicano un insieme di cloud pubblici e privati, payShield 10K è stato appositamente progettato per offrire gestione e controllo sicuri da remoto e al tempo stesso un'autentica esperienza "senza alcun contatto". Grazie a questo aspetto, può supportare numerosi tipi di offerte di servizi di pagamento e offrire più funzionalità per eseguire le funzioni in modo sicuro in una gamma più vasta di ambienti operativi.

## Che cos'è payShield

payShield è in costante evoluzione per aiutarti a proteggere le tue transazioni commerciali. Per maggiori informazioni visita: [www.thalessecurity.com/products/payment-hsms](http://www.thalessecurity.com/products/payment-hsms).

## Chi è Thales

Le persone a cui ti affidi per tutelare la tua privacy si affidano a Thales per proteggere i propri dati. Le organizzazioni si ritrovano ad affrontare sempre più spesso momenti decisivi in materia di sicurezza dei dati. Qualunque sia l'obiettivo del momento, dal creare una strategia di crittografia al passare al cloud o garantire il rispetto degli obblighi di compliance, puoi contare su Thales per proteggere la tua trasformazione digitale.

Tecnologia decisiva per momenti decisivi.



# THALES

## Americas

Arboretum Plaza II, 9442 Capital of Texas Highway North,  
Suite 100, Austin, TX 78759 USA  
Tel: +1 888 343 5773 or +1 512 257 3900  
Fax: +1 954 888 6211 | E-mail: sales@thalessec.com

## Asia Pacific – Thales Transport & Security (HK) Ltd

Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East  
Wanchai, Hong Kong | Tel: +852 2815 8633  
Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

## Europe, Middle East, Africa

350 Longwater Ave, Green Park,  
Reading, Berkshire, UK RG2 6GF  
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550  
E-mail: emea.sales@thales-esecurity.com

> [cpl.thalesgroup.com/it](http://cpl.thalesgroup.com/it) <

