Microsec aiuta le banche a trarre vantaggio dalla direttiva PSD2 con gli HSM nShield di Entrust

Tra i potenziali vantaggi dell'open banking, un approccio che prevede la condivisione sicura di informazioni finanziarie in seguito all'approvazione da parte dell'utente, spiccano una migliore esperienza per i clienti e nuovi flussi di entrate per le organizzazioni. Forte dell'esperienza in campo tecnico e industriale acquisita negli anni, Microsec ha sviluppato una soluzione basata sugli hardware security module (HSM) nShield® di Entrust per garantire la conformità e la competitività delle banche e dei servizi finanziari. L'azienda leader nel mercato IT ungherese gestisce l'autorità di certificazione (CA) e-Szignó, una delle prime in Europa a fornire certificati qualificati conformi alla direttiva (UE) 2015/2366 relativa ai servizi di pagamento (PSD2).

Le principali attività di Microsec includono:

- Manutenzione e sviluppo del registro delle imprese e del sistema informativo sulle aziende dell'Ungheria
- Offerta di una gamma completa di servizi di infrastruttura a chiave pubblica (PKI) e soluzioni aziendali, tra cui formazione e consulenza professionale in Ungheria, Europa centrale e orientale
- Fornitura di servizi fiduciari qualificati in conformità al Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS)

LA SFIDA COMMERCIALE

La direttiva PSD2 dell'Unione europea disciplina i servizi di pagamento e i relativi prestatori, mirando a dare ai consumatori maggiore autonomia per l'accesso e il controllo dei propri dati finanziari e imponendo alle banche una responsabilità maggiore di proteggere tali informazioni. Consente inoltre a terze parti di creare servizi finanziari nuovi e innovativi tramite API aperte applicate direttamente ai conti bancari dei clienti.

La direttiva PSD2 ha introdotto due importanti cambiamenti nel settore dei pagamenti. Da un lato, impone requisiti di sicurezza più rigorosi per le transazioni online tramite l'autenticazione sicura degli utenti e, dall'altro, obbliga le banche e altre istituzioni finanziarie a concedere ai prestatori di servizi di pagamento terzi l'accesso ai conti dei clienti che hanno prestato il proprio consenso.

Prima dell'introduzione della direttiva, i prestatori di servizi finanziari utilizzavano le informazioni di identificazione dei clienti per effettuare le transazioni per loro conto. Questo rappresentava un rischio molto serio per la sicurezza.

Microsec

La direttiva PSD2 stabilisce che i prestatori di servizi di pagamento sono tenuti a interagire con le banche utilizzando le proprie identità, anziché quelle dei loro clienti. In risposta a questo requisito, le banche devono quindi pubblicare API aperte per rendere le informazioni relative ai conti dei clienti accessibili ai prestatori di servizi finanziari terzi. A tal fine, gli istituti bancari devono implementare nuove infrastrutture che prevedano l'uso di certificati digitali per identificare e autenticare sia il prestatore di servizi di pagamento terzo sia la banca stessa.

CERTIFICATI DIGITALI QUALIFICATI

Gli standard tecnici introdotti dalla direttiva PSD2 impongono l'uso di certificati digitali qualificati, che attestano in modo sicuro l'identità del prestatore di servizi di pagamento (PSP) e la relativa chiave pubblica. I certificati qualificati consentono ai PSP, inclusi i fornitori terzi (Third Party Provider, TPP) e i prestatori di servizi di pagamento per la manutenzione degli account (Account Servicing Payment Service Provider, ASPSP), tra cui ad esempio le banche, di operare in conformità alla direttiva PSD2. Questi certificati garantiscono l'autenticità, la riservatezza e l'integrità delle comunicazioni, oltre a fornire prove legalmente vincolanti sulle transazioni e sui relativi contenuti.

I certificati digitali qualificati previsti dalla direttiva PSD2 devono essere creati in conformità con il Regolamento eIDAS, che richiede ai prestatori di servizi fiduciari (Trust Service Provider, TSP) di utilizzare sistemi affidabili e HSM dotati di certificazione per proteggere l'infrastruttura di emissione dei certificati. Gli HSM nShield hanno ottenuto la certificazione ai sensi dei Common Criteria EAL4+ AVA_VAN.5 e ALC_FLR.2 secondo il profilo di protezione EN 419 221-5 incluso nello schema NSCIB olandese, grazie a cui le soluzioni dei TSP che emettono marcature temporali, certificati e firme digitali possono soddisfare i requisiti di conformità del Regolamento eIDAS.

Il prestatore di servizi fiduciari qualificati (Qualified Trust Service Provider, QTSP) emittente deve controllare tutti i dati inclusi in un certificato qualificato ed eseguire una verifica dell'identità del PSP di persona (o con un processo equiparabile). I certificati qualificati devono essere convalidati in base agli elenchi di fiducia dell'Unione europea, che contengono la lista dei QTSP di ogni Stato membro.

L'OPPORTUNITÀ COMMERCIALE

L'introduzione dell'utilizzo dei certificati digitali qualificati ha rappresentato un'opportunità commerciale con il potenziale di generare un nuovo flusso di entrate per Microsec. L'azienda offriva già i propri strumenti di autenticazione dei clienti, conformi alla direttiva PSD2, a numerose banche. Con l'entrata in vigore delle misure che impongono la pubblicazione di API aperte per rendere gli account degli utenti accessibili ai TPP, Microsec ha intuito di poter aiutare gli istituti di credito e i prestatori di servizi di pagamento terzi a proteggere le comunicazioni e soddisfare i requisiti previsti per l'identificazione.

LA SFIDA TECNICA

Con l'espansione verso questa nuova linea d'impresa, Microsec ha dovuto adattare e scalare l'infrastruttura a chiave pubblica (PKI) esistente per soddisfare la domanda crescente di assistenza alle banche e ai TPP. L'azienda ha dovuto creare nuovi profili specifici in base alla direttiva PSD2, sviluppare un software della CA per supportarli e specificare le procedure e le prassi per emettere e gestire il nuovo tipo di certificati. Ha inoltre dovuto completare la valutazione di conformità del nuovo servizio fiduciario di emissione di certificati qualificati per l'autenticazione dei siti Web.

INFRASTRUTTURA A CHIAVE PUBBLICA

Le applicazioni aziendali di nuova generazione si affidano sempre di più alla tecnologia PKI per garantire un livello elevato di sicurezza. L'evoluzione dei modelli di business, infatti, sta portando a una dipendenza maggiore dalle interazioni elettroniche, che richiedono l'autenticazione online e il rispetto di normative più severe in materia di sicurezza dei dati.

Microsec

La direttiva PSD2 impone ai prestatori di servizi di pagamento di utilizzare certificati qualificati secondo la definizione indicata nel Regolamento eIDAS, ovvero certificati a chiave pubblica basati su PKI che rispettano lo standard X.509. Sebbene il Regolamento eIDAS non indichi una tecnologia specifica, al momento la PKI è l'unica in grado di fornire il livello richiesto di sicurezza e usabilità.

HARDWARE SECURITY MODULE (HSM)

Gli HSM sono dispositivi hardware affidabili e a prova di manomissione che mettono in sicurezza l'elaborazione crittografica generando, proteggendo e gestendo le chiavi usate per la cifratura e decifratura dei dati e creando firme e certificati digitali. Gli HSM sono testati, convalidati e certificati conformemente ai più elevati standard di sicurezza, come FIPS 140-2 e Common Criteria e consentono alle organizzazioni di:

- Soddisfare e superare gli standard normativi consolidati ed emergenti relativi alla cybersicurezza, tra cui il Regolamento eIDAS, la direttiva PSD2, il GDPR, lo standard PCI DSS, la legge HIPAA, ecc.
- Raggiungere livelli più elevati di sicurezza e affidabilità dei dati
- Mantenere livelli superiori di servizio e flessibilità

Il Regolamento eIDAS impone ai TSP di utilizzare sistemi affidabili, mentre gli standard tecnici applicabili richiedono nello specifico l'impiego di HSM certificati per proteggere le chiavi private coinvolte nell'emissione dei certificati digitali.

LA SOLUZIONE

Microsec ha concentrato i suoi sforzi sullo sviluppo di software per le autorità di certificazione, includendo i nuovi attributi nei certificati digitali richiesti per le transazioni di TPP e ASPSP.

Grazie alla protezione delle chiavi private utilizzate nel processo, resa possibile dagli HSM nShield di Entrust, Microsec ha potuto soddisfare i requisiti per l'emissione di certificati qualificati conformi al Regolamento eIDAS, ottenendo il riconoscimento come QTSP in tutti gli Stati membri dell'Unione europea.

L'azienda disponeva già di diversi HSM nShield di Entrust dislocati in due data center geograficamente distanti, per cui poteva contare sulla capacità e sulla flessibilità necessarie per soddisfare l'aumento previsto della domanda.

Security World, il quadro di gestione delle chiavi nShield, garantisce inoltre un controllo completo, back-up semplici, scalabilità e flessibilità, tutti criteri richiesti dai prestatori di servizi per mantenere un'infrastruttura qualificata e affidabile.

Microsec ha poi introdotto le procedure e i protocolli necessari, tra cui:

- Il controllo di tutte le informazioni personali e aziendali necessarie quando una banca, un prestatore di servizi di pagamento o una società di tecnofinanza richiede un certificato
- La consultazione del registro pubblico dell'autorità competente a livello nazionale per verificare che il prestatore di servizi di pagamento disponga dell'autorizzazione necessaria
- L'identificazione del numero univoco di autorizzazione dell'entità richiedente, che rappresenta un riferimento o identificatore univoco a livello globale all'interno del certificato
- La verifica dei ruoli che l'entità è autorizzata a ricoprire

I RISULTATI

Microsec è in grado di emettere certificati qualificati secondo il Regolamento eIDAS per l'autenticazione dei siti Web (QWAC) e i sigilli elettronici (QSealC) ai sensi dello standard ETSI TS 119 495, che indica i criteri per il formato e la gestione dei dati specifici previsti dalla direttiva PSD2. Offerto all'interno dello Spazio economico europeo (SEE), il servizio ha già consentito a Microsec di emettere certificati conformi alla direttiva PSD2 a richiedenti di 10 Stati membri dell'Unione europea.

Microsec

Obiettivi commerciali

- Creazione di un servizio per aiutare le banche e i TPP a operare all'interno del quadro normativo introdotto dalla direttiva PSD2

Obiettivi tecnici

- Creazione di un nuovo servizio sfruttando l'infrastruttura esistente, attraverso lo sviluppo del software e dei processi necessari per l'emissione di certificati specifici secondo la direttiva PSD2

Le soluzioni

- HSM nShield Solo di Entrust
- Software e processi personalizzati per la CA
- nShield Security World di Entrust

I risultati

- Adattamento rapido dell'infrastruttura esistente per offrire un nuovo servizio che sfrutta le normative introdotte a livello comunitario, portando a un aumento del fatturato complessivo
- Soluzione HSM comprovata e affidabile
- Conformità ai requisiti normativi

Al momento, i servizi fiduciari, lo sviluppo di software e la consulenza rappresentano due terzi del fatturato di Microsec. Con l'aggiunta del nuovo servizio per i PSP, l'azienda prevede un aumento della quota di fatturato internazionale nei prossimi anni.

Dal 2007 Microsec è membro a pieno titolo dell'European Telecommunications Standards Institute (ETSI), un'organizzazione riconosciuta a livello mondiale che si occupa di introdurre standard per le tecnologie IT applicabili in tutto il mondo, pietre miliari dei processi economici futuri. Microsec partecipa attivamente al Technical Committee for Electronic Signatures and Infrastructures (TC ESI) di ETSI e ha contribuito allo sviluppo della specifica TS 119 495 relativa ai certificati conformi alla direttiva PSD2.

Gli standard elevati per i prodotti e i servizi di Microsec sono supportati dal sistema di garanzia della qualità dell'azienda basato sui criteri ISO 9001:2008 e da un sistema di gestione della sicurezza delle informazioni approvato da Lloyd's in linea con la normativa ISO/IEC 27001:2013.

Per ulteriori informazioni sui prodotti e servizi di Microsec, visita www.microsec.com.

INFORMAZIONI SU ENTRUST

Entrust permette al mondo di continuare ad avanzare in sicurezza attraverso sistemi di identificazione, pagamento e protezione dei dati ad alta affidabilità. Oggi più che mai, le persone si aspettano esperienze sicure e ottimizzate, che si tratti di attraversare le frontiere tra Stati, effettuare un acquisto, accedere ai servizi elettronici della pubblica amministrazione o collegarsi a una rete aziendale. Entrust offre un'ineguagliabile gamma di soluzioni di sicurezza digitale ed emissione di credenziali, il vero fondamento di tutte queste interazioni. Con oltre 2.500 colleghi, una rete di partner globali e clienti in più di 150 Paesi, non sorprende che le organizzazioni più fidate al mondo scelgano noi.

Scopri di più su
entrust.com/HSM

ENTRUST

Per contattarci:
HSMinfo@entrust.com