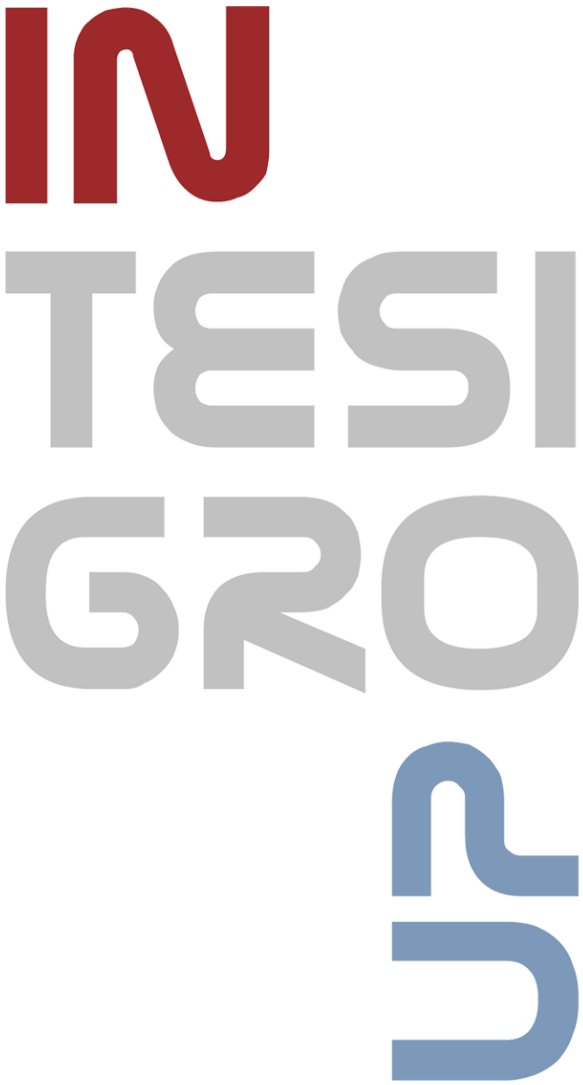
PkBox | Technical Overview

Ver. 1.0.7



Sommario

1. Introduzione

PkBox è un server di sicurezza potente e flessibile per la gestione delle operazioni di Firma Digitale (Massiva e Remota) a norma di legge, Crittografia (Simmetrica e Asimmetrica) e Autenticazione Forte a supporto delle applicazioni che debbano occuparsi di sicurezza logica dei dati.

L'uso di PkBox è utile in tutte le situazioni in cui è necessario gestire volumi elevati di transazioni con la massima flessibilità, affidabilità e scalabilità della soluzione realizzata.

Proprio al fine di garantire una soluzione ottimale alle problematiche di sicurezza dati, Intesi Group ha introdotto in PkBox, appartenente alla famiglia di prodotti PkSuite, una serie di funzionalità e di caratteristiche che ne fanno una soluzione estremamente scalabile e in grado di soddisfare ogni esigenza, in termini di numero di documenti da proteggere, trattamento di documenti di grandi dimensioni e gestione di grandi quantità di utenti (chiavi e certificati).

In questo documento ci si limita all'analisi delle caratteristiche funzionali di alto livello, mentre non vengono affrontati gli argomenti relativi alla programmazione delle applicazioni tramite le API rese disponibili dal prodotto, approfonditi in altri documenti. Vale comunque la pena citare il fatto che le funzionalità offerte dal sistema sono state implementate ad un livello di astrazione molto elevato, che nasconde la maggior parte delle complessità implementative delle funzionalità offerte. Tale approccio riduce ai minimi termini il tempo di apprendimento del sistema e non richiede una specifica competenza tecnica da parte degli sviluppatori delle funzionalità offerte da PkBox (uno sviluppatore che utilizza le interfacce PkBox non deve necessariamente essere un esperto di temi di sicurezza). La maggior parte delle caratteristiche operative delle funzionalità offerte dal sistema sono gestiti tramite parametri di configurazione.

Il codice sorgente delle applicazioni che usano le funzionalità di PkBox risulta indipendente dalla particolare configurazione impostata a livello del server. In questo modo le variazioni alla configurazione del server non richiedono modifiche al codice applicativo già sviluppato, garantendo un'alta riusabilità degli sviluppi effettuati.

Sfruttando la capacità di PkBox di gestire contemporaneamente differenti configurazioni (denominate Environment), più applicazioni potranno essere configurate per eseguire operazioni crittografiche con modalità operative differenti, senza alcuna impostazione preliminare adottata in fase di sviluppo e senza alcun intervento sul codice sorgente.

Questo aspetto è di grande importanza nell'economia delle consuete operazioni di sviluppo e d'integrazione, in quanto la stessa applicazione potrà essere proposta in differenti configurazioni e in grado di gestire tipologie di operazioni crittografiche differenti senza dover modificare il codice sorgente applicativo.

Per eventuali approfondimenti delle interfacce API offerte dai prodotti PkSuite si rimanda alla specifica documentazione tecnica disponibile sul sito www.pksuite.it.

2. Funzionalità PkBox

Sulla base della configurazione del prodotto, PkBox offre differenti funzionalità. Il prodotto è disponibile in tre differenti versioni funzionali: Advanced, Enterprise e EMV.

Si rimanda alla scheda tecnica PkBox per un'indicazione di dettaglio in merito alla disponibilità delle specifiche funzionalità per ogni configurazione di prodotto.

Le funzionalità offerte da PkBox sono:

- Firma Digitale / Verifica Firma Digitale
- Firma Elettronica / Verifica Firma Elettronica
- Richiesta apposizione Marche Temporali / Verifica Marche Temporali
- Autenticazione Forte
- Crittografia Asimmetrica
- Crittografia Simmetrica
- Comandi EMV
- Utilità

Le funzionalità offerte da PkBox sono fruibili tramite interfacce di programmazione quali:

- servizi Web Services
- API remote Java
- API remote .Net

3. Firma Digitale

La firma digitale rappresenta un sistema di autenticazione digitale tale da garantire il non ripudio e l'integrità dei dati a cui è stata apposta la firma. Il processo di firma digitale è basato sulla crittografia a chiavi asimmetriche pubbliche e provate (o Public Key Infrastructure - PKI).

La firma digitale qualificata ha un'eccezione giuridica, in quanto individua in maniera certa ed affidabile il soggetto che ha firmato un documento, e viene quindi equiparata alla firma autografa che viene apposta ai documenti cartacei tradizionali.

PkBox implementa le funzionalità di firma digitale e la relativa verifica della firma, comprensiva dei processi di verifica dei certificati (percorso di certificazione delle Certification Authority che hanno emesso il certificato, validità temporale, verifica dei profili e verifica della validità del certificato).

PkBox supporta inoltre il calcolo e la verifica di firme singole, multiple parallele e controfirme.

I formati di firma digitale supportati sono:

- RSA pkcs#7
- ISO 3200 PDF signature
- XMLDSIG
- ETSI CAdES (CAdES-BES, CAdES-T)
- ETSI PAdES (PAdES-Basic, PAdES-BES, PAdES-T)
- ETSI XAdES (XAdES-BES, XAdES-T, XAdES-C, XAdES-X-1, , XAdES-X-2, XAdES-X-L, XAdES-A).

L'algoritmo di firma digitale supportato è:

- RSA (512, 1024, 2048, 4096).

Gli algoritmi di calcolo hash supportati sono:

- MD2 e MD5
- SHA-1, SHA-256 e SHA-512
- RIPEMD-128 e RIPEMD-160

4. Marche temporali

La marca temporale è un'evidenza informatica che consente di rendere opponibile a terzi il riferimento temporale. La marca temporale di un documento informatico è una firma digitale (aggiuntiva rispetto a quella del sottoscrittore), emessa da una terza parte fidata (tipicamente le Certification Authority/Time Stamp Authority) cui è associata l'impronta del documento (o l'impronta della firma digitale del documento, se presente) e l'informazione relativa a una data e a un'ora certa.

Lo scopo di una marca temporale è quello di garantire in maniera certa l'"esistenza" di un documento (firmato digitalmente o meno) a una certa data.

PkBox supporta l'accesso ai servizi di marcatura temporale delle Time Stamp Autority tramite i protocolli e i formati indicati nella specifica RFC 3161.

Il prodotto gestisce l'apposizione ed il riconoscimento di marche temporali a documenti firmati in conformità con la specifica RFC 3161, a documenti generici in conformità con la specifica RFC 5544 ed in modalità detached tramite TimeStampToken o TimeStampResp.

L'algoritmo di firma digitale delle marche temporali supportato è:

- RSA (512, 1024, 2048, 4096).

Gli algoritmi di calcolo hash supportati sono:

- MD2 e MD5
- SHA-1, SHA-256 e SHA-512
- RIPEMD-128 e RIPEMD-160

5. Autenticazione forte

L'autenticazione è un processo tramite il quale un sistema verifica l'identità di un altro soggetto, software o utente, che richiede l'accesso a risorse o servizi. Durante l'accesso ai servizi messi a disposizione sul Web è importante per l'utente utilizzare metodi semplici e sicuri per definire la propria identità, per l'erogatore dei servizi riconoscere in maniera certa ed affidabile l'identità di chi richiede l'accesso.

Per i servizi più critici o con un elevato valore delle informazioni trattate, come ad esempio i servizi finanziari o i servizi che trattano dati personali sensibili, è strettamente importante che l'identità virtuale sia associata in maniera univoca a quella "fisica" degli utenti.

In molti casi il processo di autenticazione può essere ripetuto diverse volte al giorno: questo comporta che, oltre ai requisiti di sicurezza necessari a riconoscere l'utente in maniera affidabile, il processo deve richiedere meccanismi semplici per garantire un elevata usabilità da parte degli utenti.

Un buon processo di autenticazione dovrebbe infine offrire meccanismi flessibili per garantisce il riconoscimento degli utenti e l'accessibilità ai servizi erogati tramite diversi dispositivi (PC, smartphone, tablet, …).

Un meccanismo di autenticazione forte punta a elevare il livello di affidabilità del processo di riconoscimento delle entità che richiedono accesso, basandosi sull'utilizzo di più fattori di autenticazione distinti.

Tipicamente i fattori di autenticazione utilizzati sono:

- la conoscenza di un segreto: una password o un PIN
- il possesso (o la dimostrazione di un possesso): un dispositivo di sicurezza (smartcard o token), una carta di credito o un telefono cellulare
- una caratteristica biometrica: un'impronta digitale o in generale una caratteristica unica del corpo umano.

I sistemi di autenticazione a più fattori tipicamente fanno uso di due elementi distinti fra quelli elencati. L'autenticazione a due fattori è maggiormente sicura rispetto ad un meccanismo a singolo fattore (come la conoscenza di una sola password) in quanto la "perdita" di uno dei parametri di autenticazione non è sufficiente per un tentativo di accesso fraudolento.

I più comuni meccanismi di autenticazione a due fattori si basano su "la conoscenza di un segreto" (tipicamente una password) e su "il possesso". L'utilizzo del Bancomat è un esempio di autenticazione a due fattori: la carta Bancomat tessera è l'oggetto che rappresenta "il possesso" il PIN rappresenta "la conoscenza del segreto".

PkBox supporta i seguenti meccanismi di autenticazione forte:

- tramite utilizzo di certificati digitali
- tramite utilizzo di token OTP (token fisici, virtuali o via SMS)
- tramite schede PIN

Nel caso di autenticazione tramite certificati digitali, PkBox implementa un meccanismo di challenge / response firmati tramite utilizzo di certificati digitali X.509. Con tale meccanismo è possibile identificare in maniera forte sia gli utenti nei confronti di chi eroga il servizio, sia in servizi nei confronti degli utenti che ne richiedono l'accesso. In questo caso il primo fattore di autenticazione è il dispositivo di firma che contiene le chiavi e il relativo certificato digitale, il secondo fattore è rappresentato dal PIN di accesso al dispositivo.

Nel caso di autenticazione tramite token OTP o schede PIN, PKBox implementa un meccanismo di verifica di password dinamiche. Nel caso dell'autenticazione OTP, PkBox implementa internamente il calcolo e la verifica dei valori OTP tramite algoritmi standard quali OATH Time Based (TOTP) e Event Based (HOTP). Inoltre, PkBox integra sistemi di validazione OTP di vendor esterni già disponibili sul mercato, offrendo un'interfaccia di integrazione applicativa omogenea e trasparente indipendente dal vendor OTP. In questo caso il primo fattore di autenticazione è il dispositivo OTP o la scheda PIN, il secondo fattore è rappresentato da una password associata all'utente o al token OTP stesso.

I provider di autenticazione OTP sono:

- Time4ID SMS e Mobile Token OTP (algoritmi TOTP e HOTP)
- Time4ID OATH (algoritmi TOTP e HOTP)
- Vasco Vacman controller
- Vasco IdentiKey Server
- RSA SecureID Authentication Engine
- RSA SecureID ACE Server
- Radius

6. Crittografia asimmetrica

La crittografia asimmetrica, detta anche crittografia a chiave pubblica e privata, è un processo crittografico in cui ad ogni entità è associata una coppia di chiavi:

- la chiave pubblica è utilizzata per cifrare un documento "destinato" all'entità che possiede la relativa chiave privata
- la chiave privata è utilizzata per decifrare un documento cifrato con la chiave pubblica.

La caratteristica fondamentale degli algoritmi a chiave asimmetrica è che un documento o un messaggio cifrato con la chiave pubblica può essere decifrato soltanto con la chiave privata corrispondente: la chiave pubblica serve solo per cifrare, quella privata serve solo per decifrare. Un soggetto che ha necessità di inviare un documento/messaggio cifrato ad un destinatario deve pertanto essere in possesso della chiave pubblica del destinatario. Il ricevente utilizza la propria chiave privata per decifrare il documento/messaggio cifrato.

Tale meccanismo richiede la distribuzione della sola chiave pubblica (un'informazione che non è necessario mantenere in forma protetta) fra i vari soggetti che intendono scambiare documenti in forma protetta (cifrata), evitando così il problema dello scambio di informazioni segrete tipico dei meccanismi a chiave simmetrica (che usano una sola chiave pubblica sia per cifrare sia per decifrare). Ogni utente possiede la propria coppia di chiavi: la chiave privata viene mantenuta segreta e memorizzata in un luogo/forma sicuro, la chiave pubblica viene condivisa con i vari soggetti in maniera libera: tramite messaggi di posta elettronica, pubblicata in elenchi o directory accessibili alla comunità di utenti che ne fanno uso.

Il meccanismo di crittografia asimmetrica consente inoltre di proteggere (cifrare) un singolo documento per N destinatari differenti utilizzando la chiave pubblica di ogni destinatario. In tal modo è possibile condividere un singolo documento in forma protetta evitando di crearne una copia cifrata per ogni destinatario.

Il processo di cifratura di un documento prevede la generazione di una chiave simmetrica con cui viene cifrato il documento, la chiave simmetrica viene cifrata N volte tramite la chiave pubblica di ognuno dei destinatari del documento. Tale approccio offre due vantaggi molto interessanti:

- utilizzare un algoritmo di crittografia a chiave simmetrica per cifrare il documento garantisce maggiori prestazioni rispetto ad un algoritmo a chiave asimmetrica
- utilizzare un algoritmo di crittografia a chiave asimmetrica per proteggere la chiave simmetrica garantisce i meccanismi di semplicità e di sicurezza descritti precedentemente.

PkBox supporta i seguenti formati di documenti cifrati:

- CMS Enveloped Data – RFC 3852
- PGP Encrypted Data – RFC 2440 (formato PGP)

L'algoritmo di cifratura asimmetrica supportato è:

- RSA (512, 1024, 2048, 4096).

Gli algoritmi di cifratura simmetrica supportati sono:

- DES e triplo DES
- RC2 e RC5
- AES 128, AES 192 e AES 256.

7. Crittografia simmetrica

La crittografia simmetrica, detta anche crittografia a chiavi segrete, è un processo crittografico in cui ogni entità condivide lo stesso valore di chiave per scambiarsi documenti o dati in maniera cifrata.

La sicurezza di un sistema crittografico a chiave simmetrica è riposta principalmente sulle seguenti caratteristiche:

- la segretezza delle chiavi utilizzate dagli interlocutori che le utilizzano
- la bontà dell'algoritmo di generazione ed utilizzo delle chiavi
- la lunghezza delle chiavi utilizzate.

La crittografia simmetrica utilizza dei meccanismi più semplici e degli algoritmi più veloci rispetto alla crittografia asimmetrica, e per questo motivo viene "preferita" per le operazioni di cifratura che richiedono prestazioni elevate, ma richiede che sia condivisa a priori una chiave fra i vari interlocutori. Appare quindi evidente come le modalità di scambio delle chiavi rappresentino il punto critico della sicurezza del sistema.

I meccanismi di scambio di chiavi simmetriche possono essere differenti. In alcuni ambiti le chiavi vengono scambiate manualmente in diversi spezzoni (chiamati anche componenti), ogni spezzone di chiave è conosciuto ad un entità differente (un Key Manager). E' anche possibile scambiare in maniera semplice e sicura una chiave simmetrica utilizzando la crittografia asimmetrica: la chiave pubblica verrebbe scambiata in forma non protetta, la chiave simmetrica verrebbe scambiata in forma cifrata tramite il meccanismo delle chiavi pubbliche e private.

PkBox supporta i seguenti formati di cifratura:

- ECB
- CBC
- CBC con padding (pkcs#5 o pkcs#7)

Gli algoritmi cifratura simmetrica supportati sono:

- DES e triplo DES
- RC2 e RC5
- AES 128, AES 192 e AES 256.

8. Comandi EMV

PkBox offre uno specifico gruppo di servizi crittografici di sicurezza per gestire gli strumenti di pagamento elettronico. I servizi crittografici di tipo Europay Mastercard Visa (qui di seguito denominati EMV) offerti da PkBox sono utili per gestire i processi di emissione, e di autorizzazione degli strumenti di pagamento elettronico quali carte di debito (ad esempio Carte Bancomat) o carte di credito.

Le funzionalità crittografiche EMV sono state classificate secondo le diverse categorie di operazioni svolte. Ogni categoria di funzioni è organizzata in uno specifico servizio.

La suddivisione delle funzionalità in servizi, permette di innalzare il livello di sicurezza offerto dalla soluzione PkBox EMV. Vengono infatti separati in maniera netta i comandi crittografici fruibili dai servizi applicativi abilitati all'accesso alle singole installazioni. Grazie alla suddivisione in moduli distinti si impedisce, ad esempio, agli applicativi che gestiscono i processi autorizzativi di usufruire dei comandi necessari ai processi di Issuing.

I servizi di sicurezza offerti da PkBox EMV sono suddivisi nelle seguenti categorie:

Issuing

Nel modulo Issuing sono compresi tutti i comandi crittografici necessari ai processi di emissione carte e generazione dei PIN (ad esempio PVV, CVV, CVV2, calcolo offset, ...).

EMV

Il modulo EMV rende disponibili i comandi crittografici relativi ai servizi EMV di "Data preparation" (la personalizzazione carte), autenticazione e derivazione chiavi.

Authorization

Il modulo Authorization prevede i comandi crittografici relativi alla gestione e validazione dei messaggi autorizzativi (calcolo e verifica MAC, verifica e transcodifica PinBlock, validazione IN/PVV, cambio PIN, verifica CVV/CVV2, gestione crittogrammi 3D secure e EMV).

Petrol

Il modulo Petrol include il set di comandi relativi alla gestione e validazione dei messaggi autorizzativi relativi alle fuel card (gestione dei circuiti Shell, DVK, Routex, Uta e Lomo).