CRYPTOTEAM

PROPONE

OpenXPKI

Piattaforma di gestione dei certificati digitali per una maggior sicurezza dei dati aziendali

E-mail

Private E-mail

Accesso ai dati Sicuro

(Forti) Password Automatiche

Identità

Digital Identity

Firma

Firma Elettronica

Chiave di cifratura fino a 4096 bit

www.cryptoteam.it

*Il quadro normativo richiede un costante adeguamento tecnologico degli strumenti aziendali. La piattaforma **OpenXPKI** è predisposta al recepimento del Regolamento Europeo GDPR 679/2016.*

OpenXPKI

	**Crittografia Asimmetrica** Il sistema è basato su Certificati Digitali che contengono le chiavi di cifratura. La chiave di cifratura è dimensionabile fino a 4096 bit. Ogni titolare ha la garanzia di avere uno strumento automatico di protezione dei propri dati e di controllo: potrà verificare la provenienza e l'integrità di un qualsiasi documento informatico aziendale.
	**Proprietà delle Chiavi** Le chiave generate per accedere ai dati sono di uso esclusivo dell'azienda acquirente OpenXPKI, unico reale proprietario. Per ovvi motivi di sicurezza e di riservatezza non sono previste copie in possesso di terzi soggetti.
	**Informazioni Contenute** Il Certificato Digitale contiene le seguenti informazioni: versione del certificato, numero di serie certificato, specifiche tecniche es. tipo di chiave a 2048 bit oppure 4096 bit e tipo di algoritmo, nome del titolare, numero identificativo, firma digitale, usi consentiti, eventuali estensioni, numero della chiave pubblica, periodo di validità, nome ufficio CA emittente.
	**OpenXPKI** Progetto decennale consolidato, costituisce l'infrastruttura di gestione del ciclo di vita dei certificati digitali: verifica la richiesta tramite interfaccia grafica utente, convalida l'emissione al richiedente o l'eventuale rifiuto, rilascia il certificato digitale, controlla le informazioni sul certificato, gestisce le revoche e le sospensioni, verifica e gestisce automaticamente i rinnovi, infine gestisce i flussi di lavoro.
	**Private Email** In base al ruolo ed ai compiti assegnati, viene emesso il certificato digitale, con il quale l'utente potrà scambiare in sicurezza le informazioni confidenziali, commerciali e amministrative, più eventuali documenti allegati; le informazioni scambiate risulteranno leggibili solo agli utenti autorizzati.
	**Autenticazione per Accesso Sicuro** Questo sistema di accesso ai dati consente di superare la gestione delle password tradizionali, difficili da gestire e vulnerabili. Il certificato digitale garantisce rapidamente un'autenticazione verso le applicazioni aziendali in modalità cosiddetta a fattore forte.
	**Identità Digitale** La procedura di identificazione e di registrazione degli utenti viene gestita internamente dall'azienda acquirente del sistema OpenXPKI, in quanto dispone delle conoscenze necessarie per una corretta identificazione: persona, ruolo e compiti. L'incaricato responsabile emetterà il certificato digitale seguendo la policy di sicurezza aziendale o un proprio criterio procedurale personalizzato.
	**Firma Elettronica** Ha lo scopo di garantire i contenuti dei documenti, ovvero non essere falsificati. Qualsiasi messaggio mail o documento allegato può contenere informazioni di valore hackerabili, come ad esempio il codice IBAN. La firma elettronica garantisce integrità e autenticità di tutti i documenti scambiati in rete, oltre a quelli residenti nei back-up aziendale.
	**Assistenza** Sempre disponibile da remoto H24 - 7/7.
	**Norma GDPR 679/2016** OpenXPKI soluzione predisposta al recepimento del "GDPR" (General Data Protection Regulation - 679/16), cioè norme che impongono la protezione dati, secondo precise indicazioni. Particolare attenzione è stata posta verso la modalità di trattamento e di conservazione dei dati residenti, fino all'eventuale trasferimento presso terzi.

10 Buoni Motivi

OpenXPKI Utilizza Standard Internazionali

L'infrastruttura fornisce tutti i componenti necessari per gestire chiavi e certificati basati sullo standard principale di crittografia X509v3 più S/MIME (Secure/Multipurpose Internet Mail Extensions).

CryptoTeam Integra le piattaforme

Mette in condizione il cliente di generare le chiavi di cifratura autonomamente.
OpenXPKI può essere affiancato e configurato per sfruttare le caratteristiche di sicurezza della piattaforma Cloud in-house per la condivisione e il trasferimento dei dati aziendali.

Programmazione Senza Dipendenze

Codici sorgenti liberi e disponibili agevolano un rapporto di collaborazione equilibrato tra fornitore e cliente. OpenXPKI consente una gestione autonoma e personalizzata orientata al controllo dei propri dati aziendali: possesso, protezione, integrità e autenticità.

Maggiore Fiducia

La sicurezza insita nella soluzione OpenXPKI porta come vantaggio l'incremento della fiducia da parte di: clienti, fornitori, collaboratori, utenti, aziende, pubbliche amministrazioni, ecc..

Aumento delle Attività

OpenXPKI facilita le relazioni di scambio tra i corrispondenti, abbattendo i costi di gestione. Favorisce in sicurezza l'operatività.

Autenticazione Forte

L'utente attraverso il proprio certificato accede automaticamente alle applicazioni aziendali con un livello di sicurezza cosiddetto a fattore forte.

Integrità dei Documenti

Con la firma elettronica l'utente è in grado di verificare se un documento è stato compromesso, e individuare una eventuale contraffazione dei nuovi documenti generati.

Certificati Pubblici

OpenXPKI può emettere certificati riconosciuti da Autorità di Certificazione pubbliche (previo accordo separato), quali ad esempio SwissSign, Comodo, VeriSign.

Internet of Things (IoT)

La piattaforma consente di stare al passo con i nuovi prodotti tecnologici, dispositivi che comunicano dati ad altri dispositivi. I certificati digitali gestiti con OpenXPKI sono in grado di garantire la sicurezza dei dati trasferiti da un oggetto all'altro.

Protezione dei Certificati Digitali aziendali

Per una ancora maggiore sicurezza e conservazione dei Certificati Digitali aziendali, sono disponibili prodotti hardware specifici, come ad esempio: HSM (Hardware Security Module), Smartcard,Token USB, progettati per la sicurezza fisica delle chiavi di cifratura.

Perchè Scegliere CryptoTeam

L'adeguamento al quadro normativo sulla Privacy richiede multicompetenze, quali ad esempio: Resp. IT - Resp. di Rete - Resp. di Sicurezza - Resp. Privacy. Grazie alle competenze acquisite, CryptoTeam collabora con le aziende IT partner del cliente, per un comune raggiungimento degli obiettivi e massima soddisfazione.

CRYPTOTEAM

Rev. 2017.12.22