RIVISTA DI MECCANICA OGGI

mo

www.meccanica-plus.it

speciale anteprima MECSPE

TECNOLOGIE PER L'INNOVAZIONE - INDUSTRIE 4.0

AIGNEP

rexroth
A Bosch Company

COMAU

CONRAD

DANOBAT

E.O.I. TECNE

HERMLE
Italia S.r.l.

KUKA

meta

METAL WORK
PNEUMATIC

MITSUBISHI ELECTRIC
Changes for the Better

PNEUMAX

softing
Motors

SCHMALZ
WWW.SCHMALZ.COM

sps
ITALIA
smart production solutions
Parma, 26-28 maggio 2020

Synergon

VUOTOTECNICA
Your vacuum solutions catalogue

WAGO

WERMA

WIBU
SYSTEMS

FIERA MILANO
MEDIA

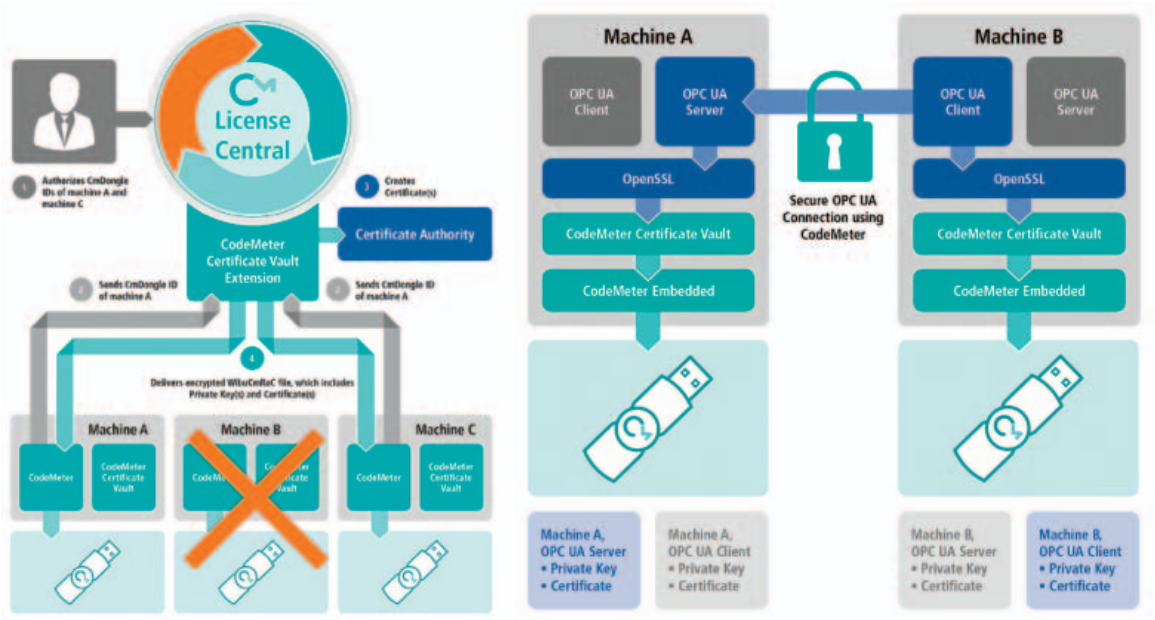
Wibu-Systems
Rueppurrer Strasse, 52-54
Karlsruhe - Germania
Tel. +39 035 0667070
team@wibu.com
www.wibu.it

L'headquarter di Wibu-Systems in Germania.

Nell'era dell'Industria 4.0, computer, macchine e milioni di altri dispositivi hanno iniziato a comunicare tra di loro. Uno dei prerequisiti essenziali, per rendere possibile questo dialogo digitale, è che ogni endpoint possa 'sapere' esattamente con chi sta colloquiando e 'fidarsi' della controparte. I certificati digitali garantiscono l'identità univoca e verificabile in modo affidabile; ad ogni dispositivo è associata una coppia di chiavi relative al proprio certificato: una chiave privata, che non deve mai essere divulgata, e una chiave pubblica. L'architettura deve anche prevedere un mezzo, per controllare la validità dei certificati assegnati, e il formato x.509 si è affermato come lo standard ideale per questo scopo, anche in ambito industriale. Dacché sempre più endpoint hanno iniziato ad entrare a far parte dell'Internet delle Cose industriale (IIoT), se da un lato, permane e cresce addirittura l'esigenza di conservare le chiavi in modo affidabile e sicuro, dall'altro, l'utilizzo dei certificati deve essere contestualizzato ai requisiti dell'attuale fase di digitalizzazione. CodeMeter Certificate Vault si pone esattamente questo obiettivo, realizzando una gestione dei certificati digitali in totale concerto con le procedure consolidate in fabbrica.

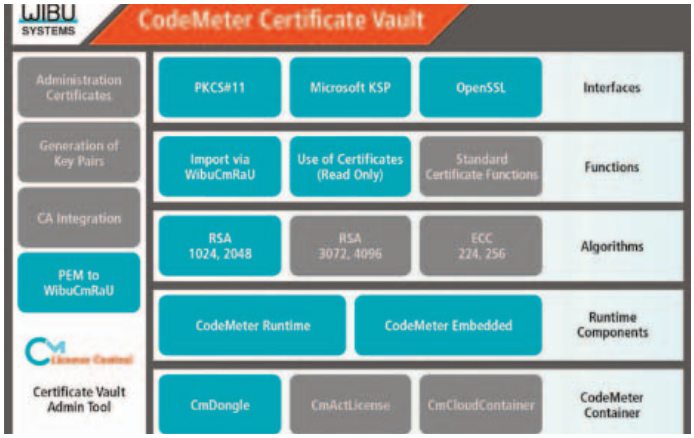
Come CodeMerter cambia le regole in gioco

CodeMeter Certificate Vault è stato sviluppato da Wibu-Systems partendo dalla pluri-decennale esperienza raggiunta con la sua tecnologia CodeMeter, una serie di soluzioni scalabili ed interoperabili, per la protezione del ciclo di vita di software, firmware e dati sensibili e per una gestione versatile delle licenze, che apra la strada a nuovi modelli di business per la vendita dei beni digitali. Applicato al settore industriale, CodeMeter consente ai produttori di dispositivi intelligenti



CodeMeter Certificate Vault di Wibu-Systems concorre alla realizzazione di una gestione dei certificati digitali in totale concerto con le procedure consolidate in fabbrica.

Publiredazionale



CodeMeter Certificate Vault è una scelta ideale per le comunicazioni M2M ma anche per crittografare e-mail o certificati VPN in reti aziendali.

di fare leva sul software, per monetizzare gli investimenti effettuati, mediante l'attivazione e la disattivazione in tempo reale di funzionalità dei macchinari; i singoli clienti vedono così recepite le loro individuali e mutevoli necessità e i produttori possono ottimizzare costi di produzione e logistica.

Che si tratti di CodeMeter in generale o del modulo Certificate Vault, le CmDongle, l'hardware di protezione proprietario dell'azienda, agiscono come elemento sicuro, in quanto il chip smart card a bordo dell'unità, indipendentemente dal fatto che si tratti di una chiave USB, di una scheda di memoria (con interfaccia SD, microSD, CF, CFast) o di un ASIC, fornisce sia le funzioni di archiviazione sicura delle chiavi sia un processore crittografico.

CodeMeter Certificate Vault memorizza i certificati nel chip smart card protetto e si affida alle normali API di CodeMeter, per interfacciare questo nuovo modulo dell'universo CodeMeter con le applicazioni e gli ecosistemi consolidati del cliente. CodeMeter Certificate Vault funziona come un token provider conforme allo standard PKCS#11, si integra come Key Storage Provider (KSP) nella Cryptographic API Next Generation (CNG) di Microsoft e può anche essere utilizzato con l'API OpenSSL, ad esempio, per conservare le chiavi per i certificati TLS o le installazioni OPC UA, ed operare con le stesse. CodeMeter License Central, la soluzione di Wibu-Systems su cloud per la creazione, la gestione e la distribuzione di licenze e diritti utente, trasferisce i certificati e le chiavi crittografiche in modo sicuro sulle CmDongle. Ciò rende possibile la creazione e l'assegnazione dei certificati con il minimo sforzo, all'interno di un processo completamente automatizzato e scalabile. Inoltre, l'architettura così concepita impedisce azioni quali la lettura, la rimozione, la duplicazione o la compromissione di chiavi e certificati.

Come viene gestito il processo

L'intero processo viene gestito centralmente e può includere un'autorità di certificazione designata, come la CA del reparto IT interno all'azienda. Essa produce i certificati, le coppie di chiavi e le password, conferma inoltre che la chiave pubblica appartenente a un certificato sia valida e la associa alla macchina o al dispositivo in questione. Il processo di trasmissione e assegnazione agli utenti può avvenire automaticamente.

La procedura sembra andare contro la prassi standard per la gestione dei certificati, in quanto le chiavi private non dovrebbero mai lasciare l'elemento hardware sicuro dell'utente, ma, con chiavi e certificati creati in un ambiente condiviso e tuttavia strettamente protetto, lo strumento di amministrazione CodeMeter Certificate Vault combinato a CodeMeter License Central può trasformarli in speciali file di aggiornamento (WibuCmRaU), protetti con metodi crittografici all'avanguardia e accessibili solo dalla CmDongle assegnata. È questa tipologia di file di aggiornamento che rende sicuro il trasferimento delle chiavi e dei certificati, utilizzando un processo sequenziale di richiesta (CmRaC) e di risposta (CmRaU).

È pertanto la tecnologia CodeMeter stessa a garantire che i certificati e le loro coppie di chiavi siano messi e mantenuti in sicurezza durante il loro intero ciclo di vita. Con CodeMeter, non solo il flusso di lavoro viene alleggerito, ma vengono rese disponibili altre speciali funzionalità tipiche di questa tecnologia, come la gestione di certificati a tempo, la cui scadenza viene legata all'orologio virtuale e a prova di manomissione di cui sono equipaggiate le CmDongle.

Sebbene lo scopo precipuo di CodeMeter Certificate Vault sia volto a semplificare la gestione dei certificati in ambito M2M, le interfacce standard su cui si fonda sono a disposizione lato utente e possono essere utilizzate da ogni applicazione compatibile per accedere ai certificati e alle chiavi sulle CmDongle e beneficiarne, ad esempio, per crittografare e-mail o certificati VPN in reti aziendali. Sono parimenti possibili funzioni aggiuntive, come i PIN opzionali per l'autenticazione a due fattori. E da ultimo, i certificati possono anche essere rinnovati o cancellati, senza coinvolgere in alcun modo l'utente