



InfoCert

Descrizione della problematica o del bisogno nell'azienda o pubblica amministrazione utente

As the Internet of Things (IoT) continues to connect objects and relay information to people, new possibilities for business and personal life arise. In light of the reams of sensitive data that the IoT generates, the need for security has never been greater. This is the environment in which Machine ID PKI solution developed by InfoCert finds its place. In designing a Machine Trust Framework, InfoCert leveraged its about 20 years' experience managing PKI infrastructure as a Trust Service Provider. The context of human and machine identity can share the same PKI paradigm, giving strength to regulated and de facto standards in a single technological and process solution. More in details, interconnected devices and people are provided with digital certificates issued by a PKI that aims at securing the identities and the actions carried on by the network components (devices and people). Such trusted IoT system enables real time control of all the logistics and predictive maintenance to promptly intercept and resolve potential malfunctions, having as result an overall increase of the productive line efficiency level.

Descrizione della soluzione tecnologica (tecnologie usate, architettura, ecc.)

InfoCert MID PKI, dedicated to the IoT environment, supports two deployment models:

- on premises virtual appliance fully equipped, or as
- cloud solution ready to run for quick deployment

and it is based on the following technological and organizational enabling structure:

- Certification Authority (CA) to issue different kinds of electronic certificates based on different trust levels
- Registration Authority (RA) to record and verify information used by the CA
- Simple Certificate Enrollment Protocol (SCEP) to provide a solid basis for the provisioning of certificates and Enrollment over Secure Transport (EST) to support SCEP by ensuring enrollment and re-enrollment
- Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) for ensuring a common scheme for maintaining the security of the network, and having full control on the revoked certificates issued by the CA

The solution permits a flexible configuration by being set up with one or more levels of intermediate CAs, according to the type of business, geographical area and certificates to be issued. The latter represents the most innovative feature, given that certificates are issued for both machines (or devices) and for the personnel who interact with them. MID PKI manages the whole certificate life cycle. The enrollment of devices' certificates complies with the standard automatic enrollment protocols, while the enrollment of people certificates complies with the RBAC model and all the secured communications (M2M, M2H or H2M) rely on TLS protocol. The compliance with those standards guarantees full market interoperability and immediate use of the solution.

Descrizione del progetto di implementazione - complessità, tempi, aspetti organizzativi, costi, ecc.

The implementation of the MID PKI solution requires full involvement of the client (who adopts the solution) and InfoCert. On client side it is necessary to involve people with expertise in the following business areas: ICT, automated industrial solution and cyber security. Project management best practices enable the realization of a POC solution in about 3 months at a total cost of about 100.000 €.



Descrizione dei principali benefici raggiunti dall'azienda o pubblica amministrazione utente

A common IoT solution system enables companies to gain a set of benefits that are typical of a Smart Factory: full control of the automated productive line, timely interception and resolution of potential malfunctions, and reduction of overall production time processes. On top of these benefits, InfoCert MID PKI guarantees an additional advantage in bringing beyond state of the art security and traceability of machine identity and communication together with the certain attribution of responsibilities of involved people. This is the real innovative added value perceived by clients and it is made possible thanks to the trusted interconnected network and on the processes described above.

Descrizione degli elementi distintivi e di reale innovatività/originalità della soluzione, anche con riferimento a soluzioni «concorrenti»

InfoCert MID PKI leads to the following main benefits:

- guaranteeing a trusted IoT system represented by a secure network made by interconnected machines and people
- issuing digital certificates for devices and humans allows to certainly assign responsibilities to actions undertaken by people and machines that interact in a production process
- providing source for Big Data collection and analysis based on real time trusted information
- ensuring high flexibility and market interoperability due to adaptability to different operating systems and compliance with common standards/protocols