PRODUCT SHEET

Secure M2M communication

Machine certificates

Advantages at a glance

01
Secure
outstanding security thanks to the use of the latest signature algorithms

02
Clearly organized
central management of the entire certificate stock

03
Automated
automated provision and distribution of certificates

04
Reliable
many years of experience as an IT security provider

Certificates are essential in state-of-the-art, connected Industry 4.0 environments and in the Internet of Things (IoT)

They provide each machine with a strong identity which the machine can use in the digital world to identify itself to other devices, persons and systems. This ensures that only authorized systems can access your network and that communication between devices is secure.

No company is an island when it comes to its business processes. D-Trust's machine certificates with their two different trust levels enable secure machine-to-machine communication (M2M). Your devices can now authenticate themselves and communicate with each other using encryption, not just within your own infrastructure but also with your partners. This means that D-Trust, Bundesdruckerei-Group's qualified trust service provider, offers secure connectivity for processes and devices that is tailored to your security needs, thus creating the basis for trust in the connected industry.

Part of the Bundesdruckerei Group
bdr.

In the modern Industry 4.0 environments as well as the Internet of Things, certificates play a decisive role.

Machine certificates in practice

Secure authentication
D-Trust's solutions for secure authentication of devices and processes in connected environments provide outstanding security combined with simple integration and use. Thanks to the Advanced Device ID as the machine certificate, devices in IoT environments are given their own identity, ensuring that each device authenticates itself before encrypted communication begins.

Advanced Device ID
By assigning any particular device name, this type of certificate can be used in many different ways as a machine certificate.Organization Validation (OV) clearly proves the identity of your device to communication partners. In addition to Advanced Device ID, Basic Device ID can be used for closed user groups and infrastructures. D-Trust's Device IDs support both device authentication as well as the establishment of IPsec-based communication and document signing. Other certificate types are distinguished on the basis of functionality (Advanced Signature ID, Basic Authentication ID, Basic Encryption ID).

Applications

IoT
IT security is an essential aspect for success in the IoT. IoT infrastructures must be secure in order to protect data and devices against outside attacks. Machine certificates can be used, for instance, to ensure that a smart meter is authenticated via a public network and can communicate in encrypted form with the supplier's infrastructure.

Industry 4.0
The business processes of a modern company take place in a connected, interactive environment. This means that production environments must be protected and secure communication between devices must be warranted. Advanced Device ID, for instance, can ensure that remote production environments are accessed via a public network through a secure channel.

Autonomous driving
In this case, the vehicle responds to special algorithms that are generated by data from visual information sources and the communication between the vehicle and nearby devices. Thanks to secure device authentication and encrypted communication between the vehicle and device, machine certificates can help to reduce risks in this field.

Possible procurement channels for certificates

Machine certificates can only be procured via D-Trust's Certificate Service Manager (CSM), a managed PKI platform. The CSM provides an interface for integration into legacy systems or infrastructures.

Functions of machine certificates at a glance

Functions	Advanced Device ID	Basic Device ID	Advanced Signature ID	Basic Authentication ID	Basic Encryption ID
Public trust	✓		✓		
Closed infrastructures and user groups		✓		✓	✓
Client authentication	✓	✓		✓	✓
Digital signature	✓	✓	✓		
Data encryption	✓	✓			✓