WHITEPAPER

PRODUCTION. WITH SECURITY.

PRODUCTION ASSURANCE THROUGH DIGITAL CERTIFICATE MANAGEMENT

m2trust . Marienstraße 27 . 70178 Stuttgart / Germany . m2trust.de/en

m2trust
it security.

"Whether digital factory, secure payment, smart mobility or smart home - digital certificate lifecycle management, is the core modern IT infrastructures."

Samuel Krüger, Founder & CEO

THE IMPORTANCE OF DIGITAL CERTIFICATES CONNECTED

Even if you're not always aware of it: In the connected world, digital certificates are used everywhere. When sending e-mails or communication between PC and printer (smart building), the exchange between applications and operating applications and operating systems, or in the field of industrial production (Industrie 4.0, IoT). Digital certificates ensure in all these fields of application, that information and data are exchanged securely and reliably.

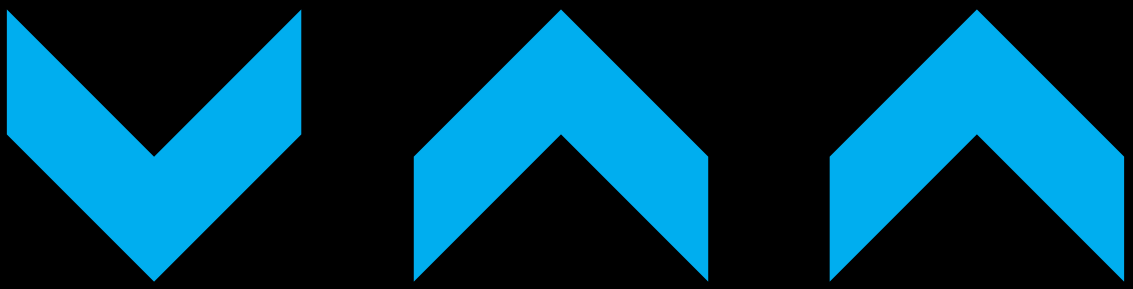
DIGITAL CERTIFICATES ARE AN INDISPENSABLE PART OF COMPANIES

Digital certificates are basically an "ID card" in electronic systems and applications. Originally, certificates were developed for the unique identification of employees. Soon after, however, they were also used in the machine environment in a more advanced form. Ultimately, they are a data record that establishes the identification of people, machines, servers or other network participants. Both the digital certificates themselves and the underlying infrastructure (public key infrastructure, or PKI for short) became increasingly complex and their administration more and more time-consuming.

WHAT IS DIGITAL CERTIFICATE MANAGEMENT?

The task of managing digital identification certificates not only became necessary in the course of this development. Rather, it also soon became clear that digital solutions were needed for the management of certificates.

THE CHALLENGES GROWING FOR COMPANIES



-66%

Shorter **RUNTIMES** of digital certificates force companies more and more often to updates of e.g. Chrome/ Firefox/ Safari These requires an annual renewal of SSL/ TSL certificates instead of previously every three years

+5%

More **DATA PROTECTION LAWS** since the year 2000 (from 20 to 100). The importance of information security continues to grow.

+30%

Companies lack **TECHNOLOGIES** to revoke certificates, even though lapses in IT security can give rise to potential lawsuits.

The increasing number of application fields for digital certificates and the growing requirements (data protection, maturity shortening, cybersecurity) pose significant challenges for companies. Ensuring IT security, smooth operation and cost efficiency while maintaining compliance is a seemingly unsolvable equation.

User-defined processes in particular usually rely on certificates to ensure that they run correctly. The certificates must be kept up to date in terms of content and their validity must be checked.

WHY DO COMPANIES NEED A DIGITAL CERTIFICATE MANAGEMENT?

Digital certificates therefore increase the operational reliability of highly complex technical systems on the one hand and security against unauthorized access from outside or by unauthorized persons on the other. One challenge in dealing with digital certificates is their ever shorter validity period and the number of systems in which they are used. Manual management of digital certificates is not a solution for several reasons. Firstly, this process is time-consuming and also dependent on the personnel situation, so that staff shortages or absences due to illness can disrupt or interrupt the functioning of an operation. For another, manual certificate management can in itself pose a cybersecurity risk. Sometimes manual checking and updating of certificates is simply not possible due to the complexity of the processes and the sheer volume of certificates, so that these must be automated as far as possible.

This means that without digital lifecycle certificate management, the smooth operation of technical systems and networks is often no longer feasible.

DIGITAL CERTIFICATE MANAGEMENT FROM m2trust

m2trust's solution is a flexible, multitenant and CA*-independent platform for event- and rule-based management of digital certificates throughout their lifecycle. m2trust's certificate platform ensures that all certificates used in a company can be kept in view at a central location. The dashboard provides an overview of certificate processes, algorithms used, certificate types as well as compliance or technically problematic certificate content.

The m2trust Core consists of a dynamic rule set that aggregates events, policies and actions. The management of devices and directory services enables automated, centralized processing of device data and events from different data sources such as SQL, REST or LDAP. The software solution from m2trust automatically detects that a certificate will expire the day after tomorrow and can even replace it itself. This not only relieves the burden on PKI administrators, but also ensures efficient and smooth operation.

* Certificate Authority

SECURE AND COMPLIANT - EVERY TIME

- Close security gaps before the occur
- Operationalize regulatory requirements easily
- Reporting and analysis for compliance and security audits
- Crypto agility (more frequent replacement of cryptographic methods requires renewal of digital certificates to continuously secure systems)

SAVES TIME AND MONEY

- Consolidate systems and interfaces
- ø 1.5 person hours/day efficiency gain
- ø 24% savings in process costs through automated & event-based coordination

INCREASES COMPETITIVENESS

- Provide new device classes with certificates and thus realize new, smart use cases in the company
- Increase collaboration speed in the company by reducing IT security barriers
- Gained resources can be used more effectively.

SEAMLESS PRODUCTION: DIGITAL CERTIFICATES IN MECHANICAL ENGINEERING

When it comes to the field of industrial production, it is not only certificates that must always be kept up to date in terms of content. The hierarchy of trusted CAs must also be checked and harmonized again and again. This creates the additional challenge that such processes must run automatically for the most part, otherwise they cannot be processed.

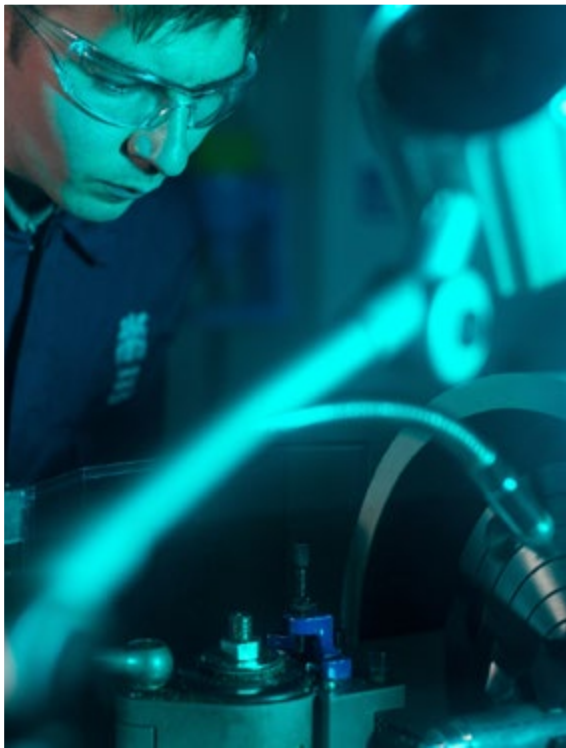
The area in which machine identity management is to be used must also be permanently monitored and analyzed. This is one of the major difficulties, because different data sources have to be integrated, data aggregated and enriched.

Another challenge is that admins are very familiar with their applications, but usually do not have in-depth knowledge of certificates, cryptography and keys. In contrast, the PKI administrator often has little or no competence about the applications and system landscapes.

DIGITAL CERTIFICATES FOR MACHINE IDENTITY MANAGEMENT

Often, system landscapes have grown and classic management solutions mainly work in a user-centric way. Over time, specially developed scripts or solutions have become established for the individual use cases. Alternatively, niche products are used that only cover individual areas. This results in many different solutions that have to be maintained, operated, serviced and further developed. The users must also be technically familiar with them. Even then, only sub-areas of the individual systems are covered, rather than the entire certificate landscape.

A central solution such as m2trust for machine identity management can connect all devices and thus replace the fragmented IT landscape that was previously used to automate or integrate certificates in individual areas. Harmonizing certificates in a uniform PKI model also creates the possibility of replacing a large number of different services, systems, proprietary developments or scripts and mapping them using a centralized certificate platform, as is common in the machine building sector.



THE ADVANTAGES OF DIGITAL CERTIFICATE MANAGEMENT BY EXAMPLE OF A PRODUCTION LINE

For manufacturing companies in the mechanical engineering sector, one of the key challenges is that production lines must not stop. Take, for example, a robot arm that gets stuck. The search for the exact cause is not always easy. Is it a defective module, an interrupted drive circuit, a discharged DC link voltage, an error in the controller, an expired program or was a required update not installed?

The list of possible causes is long. Even a cyber incident cannot be ruled out from the outset today. A common cause of errors can also be an expired certificate or a compromised CA. However, such causes are often not recognized right away. Long downtimes and the associated high financial losses are the result.

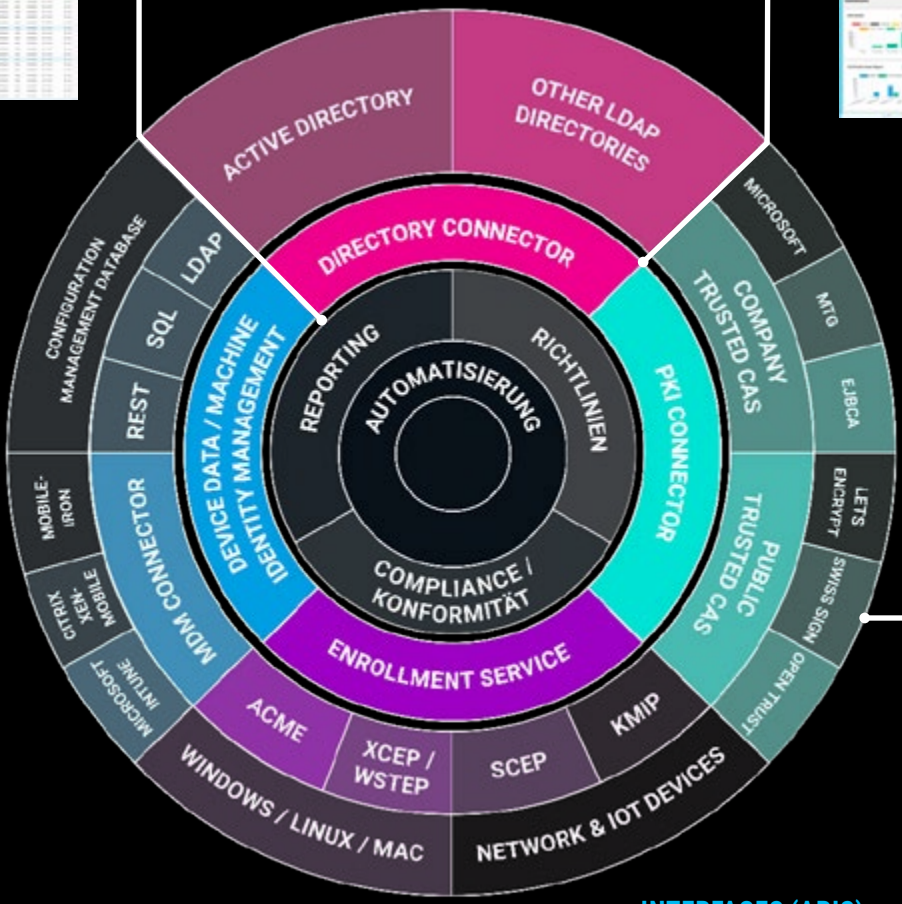
Digital certificate lifecycle management can not only detect expired certificates at an early stage and automatically renew them if possible. Rather, by harmonizing certificates from different CAs and centralizing the management and control of all internal and public trusted certificates, it ensures less downtime, smooth processes and efficient production. This has a positive effect on production management as a whole: with centralized digital certificate management, as offered by m2trust's platform, automated IT security increases, error-proneness is reduced, IT compliance can be maintained, and process as well as follow-up costs such as support are significantly reduced.

FLEXIBLE ARCHITECTURE

The m2trust Core consists of a **DYNAMIC RULEWORK** that combines **EVENTS, DIRECTIONS & ACTIONS.** The management of devices and directory services enables automated, centralized processing of device data and events from various data sources such as SQL, REST or LDAP.

CORE MODULE
Admin Section
Intelligent Automation Engine
Reporting & Analyse
Compliance & Data Security

CERTIFICATE-MANAGEMENT
MDM Connector
PKI Connector
DIRECTORY Connector
ENROLLMENT Services



INTERFACES (APIS)
MS Intune, XenMobile, MobileIron (MDM)
Microsoft, MTG, Entrust, Swiss Sign uvm.
(CA) Active Directory, LDAP directories
Windows, Linux, Mac – ACME, XCEP
Network / IoT Devices – SCEP, KMIP

m2trust

Marienstraße 27 . 70178 Stuttgart / Germany

T. +49 (0) 711 96 000 100

info@m2trust.de . m2trust.de/en