datomo®

MOBILE IDENTITY MANAGEMENT

datomo® Mobile Identity Management

Remote Verwaltung von Schlüsseln, Zertifikaten und Content auf der datomo® Secure MIMcard®

Erstellen von Zertifikaten direkt auf mobilen Devices

Mit der raschen Verbreitung der mobilen Endgeräte im beruflichen Alltag steigt die Notwendigkeit, dass sich Mitarbeiter digital ausweisen, zertifikatsbasiert authentifizieren oder sich sicher in Unternehmenssysteme einloggen müssen. Unternehmen müssen einerseits interne Daten vor unberechtigten Zugriffen und Schadsoftware schützen, zugleich soll dem mobilen Mitarbeiter ein sicherer Zugriff auf alle unternehmensrelevanten Informationen, interne Zugänge oder Webdienste gewährt werden.

Die Zahl von Keys und Zertifikaten, mit denen sich jeder einzelne Mitarbeiter ausweisen muss, um Zugang zu sicherer Information und geschützter Kommunikation zu erhalten, steigt stetig an. Jeder, der mobile Devices beruflich nutzt, verfügt über eine mobile Identität in unterschiedlichster Ausprägung. Diese sogenannte mobile Identität gilt es zunächst auf das mobile Gerät zu bringen, zu sichern, zu verschlüsseln und sicher aufzubewahren und in einem nächsten Schritt auch effizient zu verwalten.

datomo® Mobile Identity Management

- Verwaltungsoberfläche für Zertifikate und Schlüssel, die auf den mobilen Endgeräten sicher abgelegt sind
- Erweiterung des **datomo® Mobile Device Management** um die Integration der bis auf die microSD-Karte durchgängigen Zertifikatsverwaltung
- Weltweit einzigartige Möglichkeit, Zertifikate direkt remote auf microSD-Karten in den mobilen Endgeräten zu erstellen und zu verwalten – ohne Eingreifen des Anwenders
- Schnittstelle zur **datomo® Secure MIMcard®**, einer manipulationssicheren microSD-Karte mit Verschlüsselungs- und Signaturfunktionen
- Optimale Plattform, um die **datomo® Secure MIMcard®** mit hochsicheren Zertifikaten und Content auf dem mobilen Endgerät zu beschreiben
- Ideale Oberfläche, um Zertifikate, die auf der **datomo® Secure MIMcard®** abgelegt sind, sicher remote zu verwalten *(Aktivierung / Deaktivierung / Wipe)*
- Zuverlässige Generierung und Speicherung aller Schlüssel und Zertifikate im manipulationssicheren Kryptospeicher der **datomo® Secure MIMcard®** auf dem mobilen Endgerät
- Hoch skalierbare Lösung durch Einbindung beliebig vieler Zertifizierungsstellen

VORTEILE

- **Mobile Device Management plus Mobile Identity Management**
- **datomo® Secure MIMcard® remote verwalten**
- **Automatisches Erstellen von Zertifikaten direkt auf mobilen Devices – ganz ohne Eingreifen des Anwenders**
- **Bring Your Own Device mit Zertifikaten**
- **Manipulationssicherer Zertifikatsspeicher**
- **Sichere Benutzer-authentifizierung**
- **Digitale Signaturen / E-Mail-Verschlüsselung**
- **Aufbau sicherer VPN- / SSL-Verbindungen**
- **Hochsichere Verwaltung von Identitäten**
- **Schutz verschlüsselter Daten vor unbefugtem Zugriff**

FORDERN Sie Ihren Tester an: www.datomo.de

PRETIOSO GmbH I Böhmsholzer Weg 40 I 21394 Südergellersen I Telefon: + 49 41 35 800 95 90 I info@pretioso.com I www.pretioso.com

datomo®
MOBILE IDENTITY MANAGEMENT

datomo® Secure MIMcard® als Basis für sicheres datomo® Mobile Identity Management

Die **datomo® Secure MIMcard®** ist der ideale Ort für persönliche Schlüssel und Zertifikate. Hier werden Schlüssel und Zertifikate erzeugt, verschlüsselt und sicher aufbewahrt, der Export durch den Anwender ist ausgeschlossen. Sie ist ein hochsicherer Hardware Token, eine microSD Karte mit Verschlüsselungs- und Signaturfunktionen, die Anwenderdaten und Geräte vor unberechtigten Zugriffen schützt. Sie basiert auf dem Sicherheitskonzept konventioneller Smartcards und bietet manipulationssichere Verschlüsselung. Sie ist auf allen gängigen mobilen Geräten wie Notebooks, PDAs und Smartphones mit Kartenslot einsetzbar.

Mit der **datomo® Secure MIMcard®** können Anwender sicher auf Unternehmensressourcen zugreifen, digitale Dokumente signieren, sensible Daten verschlüsseln, Passworte und Schlüssel gesichert ablegen und ihre Smartphones und mobilen Geräte sicher und zuverlässig in die Unternehmens IT-Infrastruktur einbinden. Diese Karte erlaubt dem Anwender:

- zuverlässige Benutzerauthentifizierung
- digitales Signieren von Dokumenten und E-Mails
- E-Mail-Verschlüsselung
- Aufbau einer sicheren SSL-oder VPN-Verbindung vom mobilen Device aus
- Sicheres Ablegen von Content

Die **datomo® Secure MIMcard®** muss mit Zertifikaten und Content versehen und verwaltet werden, damit sie mobil effizient genutzt und optimalen Schutz bieten kann.

datomo® Mobile Identity Management als Verwaltungsplattform

Die ideale Verwaltungsoberfläche für die **datomo® Secure MIMcard®** und damit für alle privaten Schlüssel und Zertifikate, die auf dieser Karten abgelegt und gespeichert sind, bietet das **datomo® Mobile Identity Management** *(datomo® MIM)*.
datomo® MIM basiert auf dem erfolgreichen Konzept des **datomo® Mobile Device Management**. **datomo® Mobile Device Management** ermöglicht die plattformübergreifende Administration von mobilen Devices mit sämtlichen Anwendungen und Konfigurationen auf nur einer Oberfläche. Neu ist die zusätzlich bis auf die microSD-Karte durchgängig integrierte Zertifikatsverwaltung.
datomo® Mobile Identity Management ist die Erweiterung dieses datomo® Mobile Device Management-Konzeptes über die Verwaltung aller mobilen Geräte eines Unternehmens hinaus und erlaubt die Erzeugung von Zertifikaten und sichere remote Verwaltung von mobilen Identitäten auf der **datomo® Secure MIMcard®**. Hierzu können beliebig viele Zertifizierungsstellen in datomo® MIM eingebunden werden, wodurch eine nahezu grenzenlose Skalierung des Identity Managements möglich wird.

Wie funktioniert datomo Mobile Identity Management?

Mit dem **datomo® Mobile Identity Management** ist es möglich, die **datomo® Secure MIMcard®** mit Zertifikaten und Content zu beschreiben und zu verwalten. Persönliche Schlüssel und Zertifikate gelangen remote direkt auf die Secure MIMcard®. Das Unternehmen erhält einen vollständigen Überblick über die auf den einzelnen mobilen Endgeräten installierten Zertifikate.
Kernstück des **datomo® Mobile Identity Management** ist die sichere Zertifikatsverwaltung. Hier wird zunächst das Zertifikat vom Administrator über die Zertifizierungsstelle aus datomo® MIM heraus erstellt. Anschließend wird das mobile Gerät, das die **datomo® Secure MIMcard®** enthält und auf die das Zertifikat geschrieben werden soll, ausgewählt. Per Push wird das entsprechende Zertifikat an das Gerät und auf die Secure MIMcard® geschickt und in den Kryptospeicher auf diese Karte geschrieben. Es ist sichergestellt, dass das Zertifikat ausschließlich die **datomo® Secure MIMcard®** erreicht und nicht in einen Speicher des mobilen Endgerätes geschrieben wird. Per Remote Wipe kann im Verlustfall die SD-Karte vom Administrator gelöscht werden. Zudem kann ein Zertifikat für ungültig erklärt werden. Bei einer festgelegten Anzahl falscher PIN-Eingaben auf der **datomo® Secure MIMcard®** wird der Kryptospeicher der Karte ebenfalls unwiderruflich zerstört.

Wie wird ein Zertifikat erstellt?

- Administrator startet in der Zertifikatsverwaltung vom **datomo® Mobile Identity Management** den Prozess zur Zertifikatsgenerierung
- Base Agent erstellt CSR *(Zertifikatsanfrage)*
- Device erstellt Schlüsselpaar auf der **datomo® Secure MIMcard®**
- Schlüsselpaar signiert dieses CSR auf der **datomo® Secure MIMcard®**
- Base Agent sendet das CSR an den datomo® Server
- Server leitet CSR weiter an die CA *(Zertifizierungsstelle)*
- CA erstellt auf Basis des CSR das Zertifikat
- CA schickt das Zertifikat zurück an den datomo® Server
- Server sendet das Zertifikat an den Base Agent
- Base Agent schreibt das Zertifikat auf die **datomo® Secure MIMcard®**
- Zertifikatsverwaltung im **datomo® Mobile Identity Management** zeigt dem Administrator, dass das Zertifikat auf dem Device erfolgreich installiert ist
- Administrator kann Zertifikat für ungültig erklären oder bei Bedarf das Zertifikat per Remote Wipe löschen

Systemvoraussetzungen

- Lizenz datomo® Mobile Identity Management
- datomo® Secure MIMcard®