German Security Alliance

PKI ganz einfach: Bringen Sie Ihre PKI-basierten Prozesse auf das nächste Level!

Mit veralteten, komplexen PKI-Systemen lassen sich wachsende Sicherheitsanforderungen und zahlreiche Anwendungsfälle – wenn überhaupt – nur aufwendig umsetzen. Zudem zwingen gesetzliche Anforderungen den betroffenen Mittelstand zum Handeln. **Profitieren Sie jetzt vom Full-Service-Angebot aus einer Hand: Benutzerfreundliche Software, zertifizierte Infrastrukturservices und umfassende Beratung.**

Nie wieder abgelaufene Zertifikate – behalten Sie den Überblick

Unser benutzerfreundliches 360° Certificate Lifecycle Management (CLM) ermöglicht die einfache, schnelle und fehlerfreie Erstellung von Zertifikaten sowie volle Transparenz über den Status all Ihrer Zertifikate.

Erfüllen Sie wichtige regulatorische Anforderungen

Viele Unternehmen stehen vor steigenden, gesetzlich vorgeschriebenen Sicherheitsanforderungen: Vorgaben aus dem IT-Sicherheitsgesetz, der EU-DSGVO, NIS2, DORA sowie Branchenstandards und die DIN ISO 27001 verweisen in ihren Regelwerken zur IT-Sicherheit auf den Stand der Technik. Eine PKI leistet hierbei einen wichtigen Beitrag.

Public Certificates einfach mitverwalten

Öffentliche Zertifikate werden für die gesicherte Kommunikation mit externen Entitäten benötigt. Verwaltung, Beantragung, Import und Betrieb lassen sich mit dem CLM deutlich vereinfachen.

Microsoft PKI (AD CS) ersetzen oder mit unserem CLM optimal verwalten und mehr Anwendungsfälle umsetzen

Sie können Ihre Microsoft PKI (AD CS) ganz einfach und nahtlos auf 360° Managed PKI & CLM migrieren. Alternativ können Sie Ihre bestehenden AD CS weiter betreiben und nur unser CLM anbinden. Dadurch wird die Nutzung von AD CS auch für weitere nicht-Windows-Anwendungsfälle möglich, wie beispielsweise die Ausstellung von Linux-Server-Zertifikaten über ACME.

Nutzen Sie den Online-Support und die umfassende persönliche Beratung

Auf der 360° GSA-Webseite finden Sie zahlreiche nützliche Informationen zur PKI-Projektplanung und zum PKI-Betrieb. Ein umfangreiches Informationsangebot mit FAQs, einer Online-Dokumentation und anschaulichen Videos unterstützt Sie bei der Umsetzung erster Anwendungsszenarien. Das kompetente 360° GSA-Beratungsteam steht Ihnen außerdem jederzeit für spezielle Fragen oder die Planung eines Proof-of-Concepts zur Verfügung.

Foto: © DjelicS/ stockphoto.com

Mit unserer benutzerfreundlichen, intuitiven Oberfläche verwalten Sie bequem alle Zertifikate und vermeiden typische Fehlerquellen.

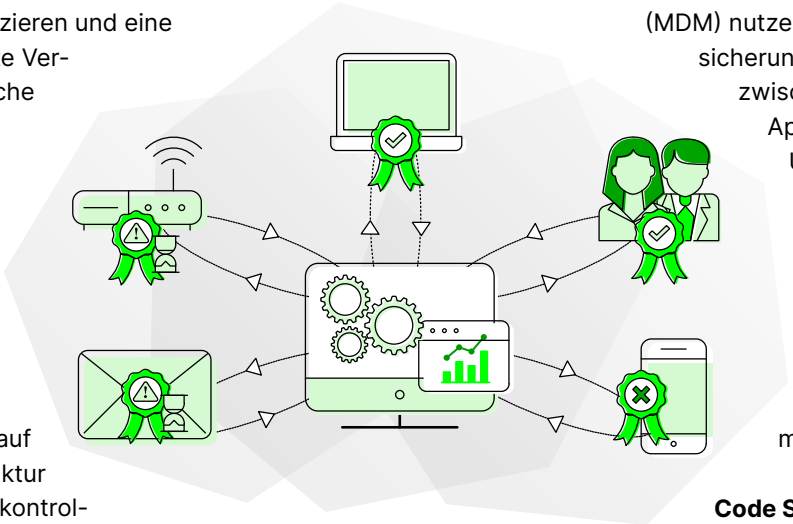
Mehr Anwendungsfälle, mehr Möglichkeiten:
Schützen Sie umfassend Ihre Unternehmensprozesse und erfüllen Sie gesetzliche Vorgaben

Identitäts- und Zugriffsmanagement
Authentifizierung und Autorisierung von Benutzern, wie Windows-Benutzern, Computern, Laptops, Firewalls, Routern, Switches und IoT-Geräten.

Netzwerksicherheit (VPN)
In VPNs (Virtual Private Networks) werden PKIs verwendet, um die Identität der kommunizierenden Parteien zu authentifizieren und eine sichere, verschlüsselte Verbindung über öffentliche Netzwerke hinweg zu etablieren.

Network Access Control (NAC)
Mit diesem Sicherheitsmechanismus werden Zertifikate genutzt, um den Zugriff von Endgeräten auf die Netzwerkinfrastruktur von Unternehmen zu kontrollieren. Dabei muss zunächst eine erfolgreiche Authentifizierung mit einem gültigen Zertifikat erfolgen.

Sichere E-Mail-Kommunikation
Zertifikate ermöglichen es, E-Mails digital zu signieren, um die Integrität der Nachricht sowie deren Authentizität zu garantieren sowie die Inhalte zu verschlüsseln.



SSL/TLS Webserver-Zertifikate
SSL/TLS-Zertifikate sind unerlässlich für die Sicherung von Webanwendungen und -diensten. Hierbei kommen Zertifikate einer öffentlichen Zertifizierungsstelle (Public CA) zum Einsatz.

Verwaltung und Absicherung mobiler Geräte
Mobile-Device-Management-Plattformen (MDM) nutzen eine PKI zur Absicherung der Kommunikation zwischen mobilen Geräten, Apps, Benutzern und Unternehmensdiensten.

Digitale Signaturen für Dokumente
Dokumentensignaturzertifikate werden verwendet, um Authentizität und Integrität von Dokumenten sicherzustellen.

Code Signing
Digitale Zertifikate tragen im Rahmen des Code Signing wesentlich zur Sicherheit, Integrität und zum Vertrauen in Softwareprodukte und Firmware bei.

Unsere beiden Angebotspakete:

Professional Package (CLM)

Sie möchten die Verwaltung und Überwachung Ihrer Zertifikate optimieren und benötigen keine Zertifikate von einer MTG Corporate PKI? Besonders interessant ist die Möglichkeit der Anbindung von ausgewählten Public CAs sowie der Microsoft CA.

- Alle CLM Funktionalitäten:
  Übersichtliches Dashboard, Organisation in Bereiche (Realms), Policies, Kontrollen & Freigaben, Zertifikate, Rollen & Rechte, Dokumentation
- Reporting & Monitoring
- Rollen- & Rechtemanagement
- Policy Enforcement & Konfigurations GUI
- Public CA Anbindung
- Microsoft PKI Anbindung (AD CS) an das CLM

Ultimate Package (CLM & PKI)

Sie benötigen zusätzlich Zertifikate aus einer privaten PKI oder suchen einen Ersatz für Ihre Microsoft PKI? Das Ultimate Package umfasst alle Funktionen des Professional Packages und bietet zusätzlich die Funktionalität einer privaten CA.

- Alle Funktionen des Professional Pakets
- Unternehmens PKI
- Eigene Root CA und Sub CA
- HSM Anbindung & Support
- OCSP & CRL Responder
- Audit-Log
- Microsoft PKI Migration mit speziell entwickeltem AD CS Autoenrollment Connector

Mit System schneller ins Ziel:
PKI-Projekte endlich einfach umsetzen

1 Analysieren

In einem ersten Kennenlerngespräch klären wir Ihren aktuellen Bedarf: Möchten Sie Ihre Microsoft PKI (AD CS) ersetzen oder mit unserem CLM erweitern? Haben Sie noch keine PKI und wollen eine einführen? Wie viele Zertifikate benötigen Sie und für welchen Zweck? Gibt es regulatorische Anforderungen (z.B. NIS2, DORA)? Benötigen Sie zusätzlichen Service und Support? Wir stellen Ihnen mögliche Anwendungsfälle sowie unsere Softwarelösungen vor.

2 Planen

Sie legen die Anwendungsfälle fest, mit denen Sie starten möchten. Falls noch nicht geschehen, registrieren Sie sich für die kostenlose Online-Demo. Anschließend planen wir den Kick-off-Termin für Ihr PKI-Projekt. In diesem kostenlosen Beratungstermin stehen Ihnen unsere PKI-Experten für die ersten Schritte zur Seite. Sie entscheiden, wie viel Unterstützung Sie darüber hinaus benötigen. Für Ihre Planungssicherheit bieten wir Festpreispakete für Onboarding, Umsetzung der Use-Cases und spätere Supportservices im operativen Betrieb an.

3 Durchstarten

Sie haben zwei Monate Zeit, um Ihre Online-Demo und alle Funktionen ausführlich zu testen. Bei Bedarf können Sie unsere PKI-Experten für eine detaillierte Analyse und die Umsetzung hinzuziehen, beispielsweise zur Vorbereitung eines Proof-of-Concepts. Für maximale Sicherheit bei der Planung und Umsetzung bieten wir Ihnen Festpreispakete, die alle Phasen Ihres Projekts abdecken, vom Onboarding bis zum operativen Betrieb.

Jetzt kostenlos testen
und alle Funktionen im Detail ansehen

Ihre persönliche Online-Demo steht nach wenigen Anmeldeschritten für Sie bereit. Testen Sie alle wichtigen Funktionen ausgiebig und erstellen Sie beispielsweise Policies, richten Rollen und Rechte ein oder kreieren mit wenigen Klicks Ihre eigenen Testzertifikate.

Foto: © rawpixel / freepik.com

Alle Features im Überblick:

360° Managed PKI & Certificate Lifecycle Manager		Professional CLM	Ultimate CLM & PKI
Features	**Kurzbeschreibung**	**x**	**x**
Identity Management	Keycloak mit sicheren Login-Optionen	**x**	**x**
Manueller Import von Zertifikaten	Import aller Unternehmenszertifikate in das CLM	**x**	**x**
Reporting & Monitoring	Alarmfunktionen, Benachrichtigungen, Daten in übersichtlicher GUI	**x**	**x**
Rollen & Rechtemanagement	Organisation der Zugriffsrechte sowie Rollen- & Rechtekonfiguration	**x**	**x**
Policy Enforcement & Konfigurations GUI	Vollständige & fehlerfreie Erstellung von Zertifikaten	**x**	**x**
Public CA Anbindung	CLM Zugriff auf Public CA Zertifikate	**x**	**x**
Private CA Anbindung	CLM Zugriff auf Microsoft AD CS	**x**	**x**
Certificate Discovery	Systematisches Scannen nach Zertifikaten	**x**	**x**
Automation Paket ACME	Automatisierungs-Support Linux-basierter Server	**x**	**x**
Automation Paket SCEP, EST, CMP	Automatisierungs-Support von Netzwerk Geräten	**x**	**x**
Automation Paket REST & CLI Client	Automatisierungs-Support Drittsysteme	**x**	**x**
CLM Autoentrollment Connector	Verbindung zum Microsoft Active Directory (AD CS migrieren)		**x**
HSM Support	Schlüsselaufbewahrung in Hardware Security Modulen		**x**
Dedizierte Root-CA und Sub-CA	Dedizierte Trusted Chain		**x**
OCSP & CRL Responder	Prüfen Sie in Echtzeit den Zertifikatsstatus		**x**
Audit-Log	Garantierte Rückverfolgbarkeit aller CA-Aktivitäten		**x**
Add-Ons			
Multi - Root-CAs	Gestalten Sie Ihre PKI mit mehreren Root-CAs		**x**
Multi - Sub-CAs	Gestalten Sie Ihre PKI mit mehreren Sub-CAs		**x**
Offline Root-CA	Root-CA für spezifische Sicherheitsanforderungen		**x**

360° German Security Alliance:

Neue Partnerschaft für die erfolgreiche Umsetzung von PKI-Projekten

Der Zusammenschluss von **MTG** (Software), **DARZ** (Infrastrukturservices) und **XELANED** (Beratung) bündelt das spezifische PKI-Know-how dreier starker Partner aus Deutschland. Ziel ist es, den wachsenden Bedarf des Mittelstands nach benutzerfreundlichen und verlässlich planbaren PKI-Lösungen bestmöglich zu erfüllen.

Infrastruktur-Dienstleister DARZ:

- ☑ Deutsche Standorte: Darmstadt, Frankfurt
- ☑ ISO 27001
- ☑ BSI C5 – für sicheres Cloud-Computing
- ☑ BSI TR-03145
- ☑ DIN EN50600 CAT III
- ☑ HSM-Zertifizierung: FIPS 140-2 Level 3, Common Criteria EAL4+ (EN 419 221-5)
- ☑ Hochverfügbarkeit: > SLA 99,98 %

360 German Security Alliance

Analysieren, planen, durchstarten – unsere Experten begleiten Sie bei jedem Schritt auf dem Weg zu Ihrer Unternehmens-PKI.

MTG DARZ XELANED

Ihr Kontakt:
DARZ GmbH
360° GSA Managed Services
Julius-Reiber-Straße 11
64293 Darmstadt
Telefon: +49 6151 8762-777
E-Mail: mpki@360-gsa.de
Website: www.360-gsa.de