TELEKOM SECURITY

Digitale Identitäten schützen

Public Key Infrastuktur als Basis moderner IT-Sicherheit

Connecting your world.

Eines Tages in einem mittelständischen Unternehmen...

Lisa, talentierte IT-Spezialistin eines mittelständischen Unternehmens, engagiert sich leidenschaftlich für die Entwicklung innovativer Softwarelösungen. Das Unternehmen, in dem sie arbeitet, ist bekannt für seine maßgeschneiderten Anwendungen, die es Kunden ermöglichen, ihre Geschäftsprozesse zu optimieren und effizienter zu gestalten.

Als Lisa von einem Sicherheitsvorfall in der Branche erfährt, bei dem sensible Daten kompromittiert wurden, beginnt sie, sich Gedanken über zusätzliche Sicherheitsmaßnahmen zu machen. Vielleicht, so überlegt sie, sollte das Unternehmen auf eine Public Key Infrastruktur (PKI) setzten?

Wie sicher ist Ihre IT-Infrastruktur?

Die Cyber-Bedrohungslage ist besorgniserregend. Denn längst mischt die organisierte Kriminalität mit, wenn es um digitalen Datenklau geht. Und auch Cyber-Attacken staatlicher Akteure, die Spionage oder Sabotage betreiben, nehmen zu. Ob es sich um einen politischen oder einen rein kriminell motivierten Angriff handelt, ist oft nicht klar auszumachen. Klar ist aber: Unternehmen und öffentliche Einrichtungen müssen auf der Hut sein und sich bestmöglich vor den Angreifenden wappnen. Eine besondere Rolle spielt dabei der Schutz digitaler Identitäten.

Digitale Identitäten schützen

Unter digitalen Identitäten* versteht man verifizierte und durch Signatur integritätsgeschützte Daten, sogenannte Zertifikate, die Computersysteme verwenden, um in einer digitalen Welt Personen, Organisationen, Software-Anwendungen oder Geräte zu identifizieren. Das können etwa biometrische Daten, Standortdaten, IP-Adressen, Passwörter, Suchhistorien oder Aliasnamen sein. Ohne zuverlässige, fälschungssichere digitale Identitäten sind im Internetzeitalter keine verlässlichen Interaktionen möglich. Werden sie gekapert, können Angreifende sich mittels dieser als eine bestimmte Person, Organisation, Anwendung oder Maschine ausgeben und so vertrauliche Daten abgreifen oder weiteren großen Schaden anrichten.

* Mehr zum Thema digitale Identitäten können Sie in unserem **Whitepaper zu Identity Security** nachlesen. Darin wird die wachsende Bedeutung von Identity Security im Kontext von Identitätsdiebstahl und Datenmissbrauch, gesetzlichen Rahmenbedingungen und modernen Sicherheitsmodellen wie Secure Access Service Edge (SASE) und Zero Trust beleuchtet und verschiedene Sicherheitsbausteine für Identity Security vorgestellt.

Moderne Unternehmensnetze sind gefährdet

Durch Entwicklungen wie Cloudifizierung, mobiles Arbeiten und Industrie 4.0 bekommt der Schutz digitaler Identitäten eine immer größere Brisanz. Denn das Unternehmensnetz ist nicht mehr, wie früher, eine in sich geschlossene Systemlandschaft. Anwendungen und Daten liegen in Clouds verschiedener Anbieter, Mitarbeitende loggen sich aus dem Homeoffice via Internet ins Unternehmensnetz und Produktionsanlagen werden via Internet der Dinge überwacht. Der klassische Perimeterschutz, der die Grenzen des Netzwerks schützt und alles innerhalb des Netzwerks als vertrauenswürdig einstuft, reicht für diese Szenarien nicht mehr aus.

Verlässlich erprobte starke Verschlüsselungs- und Authentifizierungsmechanismen sind nötig, um sensible, persönliche Daten sowie Unternehmensdaten, die in eigenen Netzwerken und über das Internet verarbeitet werden, zu schützen.
Genau hier kommen Public Key Infrastrukturen (PKI) ins Spiel, die es ermöglichen, digitale Identitäten von Personen, Geräten und IT-Equipment mit digitalen Zertifikaten auszustatten. Durch kryptographische Verfahren wird so eine starke Authentifizierung, Autorisierung sowie Integritätsschutz und Verschlüsselung bei der Übertragung und Speicherung von Daten sichergestellt.

94 % **der Angriffe auf Unternehmen stehen in einem Zusammenhang mit gefälschten Identitäten[1].**

[1] 2024 Email Security Risk Report (egress.com)

Was ist eine Public Key Infrastruktur?

Eine Public Key Infrastruktur (PKI) ist ein Team Player und ergänzt als solcher klassische Sicherheitsmaßnahmen wie Firewalls, Intrusion Prevention und Detection Systeme. Eine PKI interagiert außerdem mit anderen Systemen, um eine umfassende Sicherheitsarchitektur im Sinne von Zero Trust zu schaffen. Sie spielt zudem eine entscheidende Rolle bei der Integration verschiedener IT-Anwendungen zur Unterstützung von Geschäftsprozessen, indem sie eine sichere Kommunikation, Datenübertragung und Speicherung von Daten zwischen diesen Anwendungen ermöglicht.

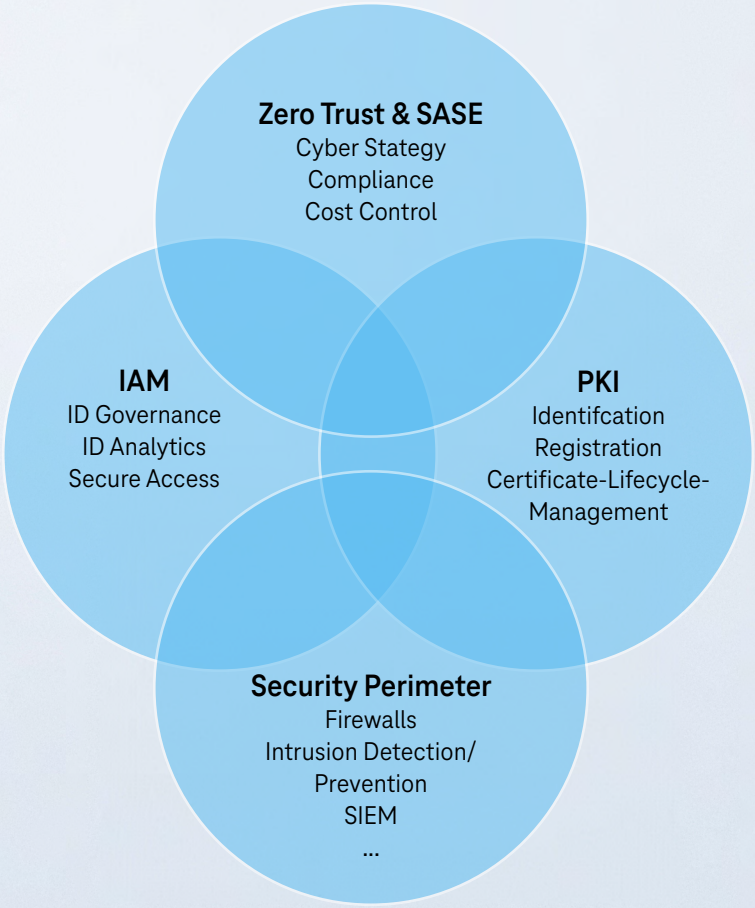
Zum Schutz von Daten vor Ausspähung oder Manipulation während der Übertragung und Speicherung sowie zur sicheren Authentifizierung von Personen, Anwendungen und Geräten werden moderne kryptographische Verfahren eingesetzt. Basis dieser Verfahren sind digitale Schlüssel, die eindeutig einer Person oder einem Gerät zugeordnet werden können. Die sichere Zuordnung solcher Schlüssel, sowie weiterer Informationen, erfolgt auf Basis eines digitalen Zertifikates. Die Ausgabe und Sperrung eines digitalen Zertifikates folgt festgelegten Prozessen und Regeln und wird durch eine Public Key Infrastruktur umgesetzt.

Public Key Infrastrukturen ermöglichen somit im Zusammenwirken mit einem IAM (Identity Access Management) die Absicherung von Zugriffen auf und in Netzwerke und Cloud-Umgebungen sowie die sichere Kommunikation innerhalb und außerhalb davon.

Public Key Infrastrukturen werden in unterschiedlichen Ausprägungen eingesetzt und können je nach Einsatzszenario einschlägige Standards wie WebTrust, ETSI oder eIDAS berücksichtigen. Durch regelmäßige Auditierungen bzw. Zertifizierungen der Betriebs- und der Zertifikatsverwaltungsprozesse wird sichergestellt, dass die PKI relevanten regulatorischen Anforderungen und Branchenstandards entspricht.

Digitale Zertifikate

Digitale Zertifikate ermöglichen eine vertrauenswürdige, fälschungssichere und eindeutige Zuordnung von kryptographischen Schlüsseln zu Personen, Maschinen, Geräten oder Dingen mit einer digitalen ID bzw. Identität. Ein professionelles Certificate Lifecycle Management sorgt für klar definierte Prozesse zur Ausstellung, Erneuerung, Sperrung sowie des Ablaufs (End of Life) digitaler Zertifikate.



PKI als Team Player

Die Entscheidung steht...

Lisa weiß, dass Firewalls eine wichtige Komponente der IT-Sicherheit sind, da sie den Datenverkehr überwachen und unerwünschte Zugriffe blockieren können. Aber sie erkennt auch, dass eine Public Key Infrastruktur (PKI) ein wichtiger zu ergänzender Sicherheits-Baustein ist, der die Vertraulichkeit und Integrität von Daten gewährleistet. Die Implementierung einer PKI würde dazu beitragen, die Sicherheit neuer IT-Anwendungen erheblich zu verbessern und das Risiko von Datenlecks zu minimieren. Lisa kann ihre Vorgesetzten und ihr Team von den Vorteilen einer PKI überzeugen. Aber wie geht es weiter?

Kein Kinderspiel: Die Implementierung

Aufbau, Betrieb und technische Integration einer PKI in bestehende, oft komplexe IT-Infrastrukturen, ist nicht trivial. Meist müssen unterschiedlichste prozessuale und betriebliche Anforderungen sowie unter bestimmten Umständen auch regulatorische Vorgaben berücksichtigt und erfüllt werden. Was ist zu beachten? Wir fassen die wichtigsten Aspekte zusammen.

Welche Rolle spielt Automatisierung?

Automatisierte Workflows spielen eine entscheidende Rolle bei der Umsetzung einer skalierbaren Verwaltung und Nutzung digitaler Identitäten innerhalb und außerhalb eigener Netzwerkbereiche. Automatisierung erleichtert die effiziente Bereitstellung und Sperrung von Identitätsnachweisen (digitale Zertifikate) und Identitätsträgermedien (Token), vereinfacht Zugriffsanforderungs- und Genehmigungsprozesse und unterstützt Self-Service-Funktionen für Benutzer. Automatisierte Prüfungen helfen zudem dabei, die Einhaltung von Sicherheitsrichtlinien wirksam durchzusetzen.

Sollte man in jedem Fall auf Hochsicherheitsbetrieb setzen?

Der Betrieb einer PKI muss nicht für jeden Anwendungsfall immer den höchsten Sicherheitskriterien genügen. Vielmehr sollte er je nach Unternehmensanforderungen, Betriebsmodell (Inhouse, Outsourcing oder Nutzung eines Services) und regulatorischen Vorgaben differenzierbar sein und unterschiedliche Sicherheits- bzw. Trust-Level, wie sie z. B. im Rahmen von eIDAS von „niedrig“ über „substanziell“ bis „hoch“ definiert sind, jeweils angemessen umsetzen können.

Welche Vorgaben müssen beachtet werden?

Eine Public Key Infrastruktur (PKI) bildet einen wichtigen Vertrauensanker in der Sicherheitskonzeption von Unternehmen. Bei Design und Umsetzung bzw. Auswahl einer PKI spielen daher nicht nur eigene und kundenbezogene Anforderungen eine wichtige Rolle. Hinzu kommen gesetzliche Anforderungen, Branchenvorschriften sowie bewährte Sicherheitsnormen und -richtlinien.

Durch die konsequente Durchsetzung dieser Richtlinien – z. B. dem Prinzip des geringsten Wissens, der geringsten Berechtigungen und der Aufgabentrennung – können Risiken in Bezug auf Datenschutzverletzungen und Compliance-Verstöße reduziert werden. Das schafft Vertrauen in die Sicherheit und Integrität digitaler Identitäten und der damit verbundenen Systeme, Prozesse und Daten.

Identity Security
Reglementierungen und Vorgaben (Auszug)

Branchenvorschriften: CA Browser Forum BR, Kritis, Smart-Meter (BSI), gematik (Telematik)
Sicherheitsstandards: VDE, IETF
Normen: ISO, IEC
Gesetzliche Anforderungen: DSGVO, NIS-2, CRA, eIDAS

Die Umsetzung nimmt Formen an...

Lisa und Ihr Team haben entschieden, sich für die Implementierung einen zertifizierten Dienstleister mit ins Boot zu holen. Dieser erfüllt ihre unternehmensspezifischen Anforderungen optimal und ist auch in der Lage, diese bei Bedarf mit höchsten Sicherheitsanforderungen zu kombinieren. So spart das Unternehmen knappe Personalressourcen und muss das Rad nicht neu erfinden.

Lisa begleitet die Implementierung. Der Organisationsaufwand hält sich für sie in Grenzen, denn der Dienstleister übernimmt die Generalunternehmerschaft. Gegen Ende des Projektes werden dann aber doch noch mal alle eingebunden. Denn der Dienstleister führt bedarfsgerechte Schulungen für sämtliche Mitarbeitende durch.

Ihre individuelle Public Key Infrastruktur

Profitieren Sie von unserer Erfahrung und Fachkompetenz

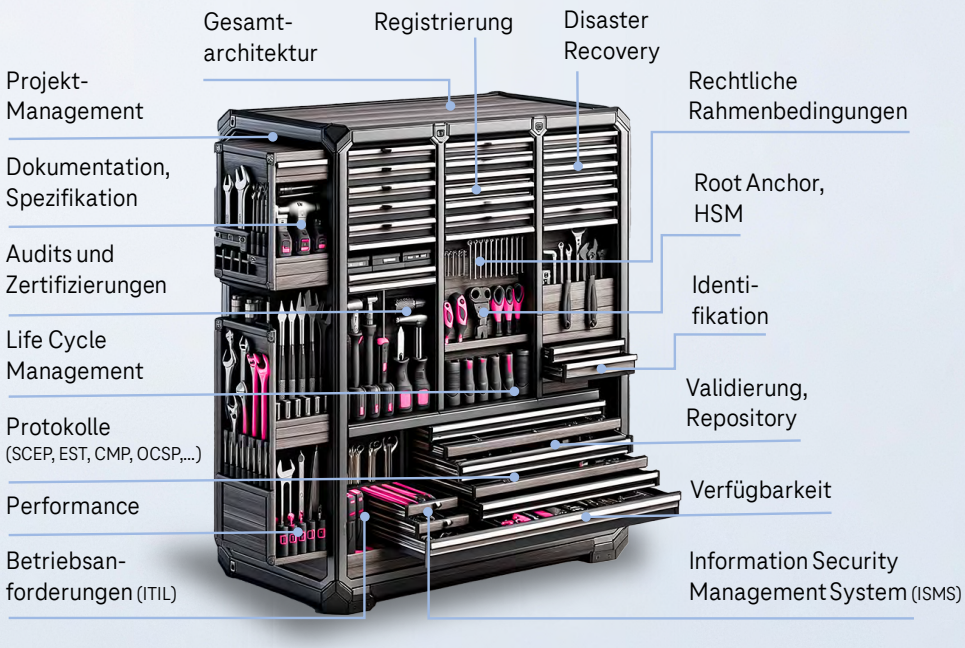
Wir bieten Ihnen umfangreiche Beratungsleistungen und entwickeln gemeinsam mit Ihnen auf Grundlage einer Anforderungsanalyse ein an Ihren Bedürfnissen ausgerichtetes PKI-Lösungsdesign. Auch bei der Umsetzung stehen wir Ihnen gern zur Seite und übernehmen auf Wunsch das komplette Projektmanagement und die Generalunternehmerschaft. Wir kümmern uns um Inbetriebnahme, Audit-Management und Zertifizierung und schulen Ihre Mitarbeitenden. Dabei greifen wir auf eine langjährige Erfahrung in Sachen PKI und deren Integration, ein umfangreiches Kompetenznetzwerk und unsere erprobte PKI-Toolbox zurück.

Effizienter und sicherer Betrieb

Als Alternative zum Betrieb in Ihrem Hause bieten wir auf Wunsch auch den Betrieb in unseren georedundanten Rechenzentren an, in denen ausschließlich geschultes und sicherheitsüberprüftes Personal eingesetzt wird und die über eine zusätzlich integrierte Hochsicherheitsumgebung verfügen.

Seit 1994 betreiben wir das bundesweit erste Trust Center „Made in Germany“. Viele Millionen Zertifikate wurden seitdem produziert und sind bei unseren Kunden im täglichen Einsatz. Als Zertifizierungsstelle und Vertrauensinstanz für den elektronischen Datenaustausch sind wir Ihr Partner für sichere und moderne IT-gestützte Geschäftsprozesse mit einem verlässlichen 24/7-Service und Support.

Unsere PKI-Toolbox



Magenta Security Enterprise.ID

Mit Magenta Security Enterprise.ID erhalten Sie Ihre individuelle Public Key Infrastruktur als Dienstleistung. Dabei können private Zertifizierungsstellen (Root CA, Sub CA) speziell für Ihr Unternehmen genutzt werden. Die Lösung kann sehr flexibel mittels Micosoft AutoEnrollment und Active Directory in Ihre Systemlandschaft eingebunden werden.

Magenta Security Business.ID

Mit Magenta Security Business.ID stellt die Telekom Ihnen eine Public Key Infrastructure (PKI) als Dienstleistung bereit. Dabei werden anerkannte, öffentliche Zertifizierungsstellen (Root CA, Sub CA) der Telekom genutzt. Sie erhalten einen eigenen Mandanten und haben damit direkt nach der Beauftragung Zugriff auf Ihren eignen Mandanten.

Praxisbeispiel: Elektronische Signaturen für Kanzlei

Herausforderung:

Unser Kunde, eine renommierte Kanzlei, wollte papierbasierte Prozesse digitalisieren. Ein Ziel der angestrebten Digitalisierung war es, Mitarbeitenden flexible Arbeitskonzepte und das Arbeiten im Homeoffice zu ermöglichen. Beim Umgang mit juristischen Akten und Dokumenten gelten jedoch besonders hohe Ansprüche an Datensicherheit.

Lösung:

Mit der Implementierung einer Public Key Infrastruktur – hier bestand die Wahl zwischen Magenta Security Business.ID und Enterprise.ID – ist die Kanzlei in der Lage, elektronische Signaturen zu nutzen. Sie gewährleisten die Authentizität zweifelsfrei identifizierbarer Sender bzw. Empfänger und können durch spezielle, berufsbezogene Attribute auch bestimmte Rollen und Funktionen (z. B. Rechtsanwalt oder Notar) sicher abbilden. So kann die Kanzlei rechtssichere digitale Kommunikation und Dokumentation konform zu gesetzlichen Vorgaben wie der Verordnung für elektronische Identifizierung und Vertrauensdienste (eIDAS) oder dem Vertrauensdienstegesetz (VDG) gewährleisten.

Kundennutzen:

Prozesse beschleunigt:
Digitale Unterschriften senken die Durchlaufzeiten von Dokumenten von mehreren Tagen auf wenige Minuten

Warte- Arbeits- und Reisezeit gespart:
Terminvereinbarungen, Dienstreisen und Aufenthalte im Zusammenhang mit der Unterzeichnung von amtlichen Dokumenten entfallen

Medienbrüche abgeschafft:
Durchgängig digitale Prozesse von der Erstellung eines Dokumentes über die Signatur bis hin zur Archivierung

Ressourcen geschont:
Geringerer Energie- und Papierverbrauch senkt den CO_2-Abdruck

Kunden- und Mitarbeiterzufriedenheit erhöht:
Mitarbeitende können agil und ortsunabhängig arbeiten; Kunden profitieren von den beschleunigten Prozessen

Einzelne PKI-Lösungsbausteine

Software Trust: Manipulation verhindern

Schädliche Software kann schnell in die Unternehmenslieferkette eingeschleust werden. Die Folgen von Angriffen auf die Software-Integrität sind hoch. Es drohen Produktionsausfall, Umsatzeinbruch und Image-Verlust.

Wir bieten Ihnen Software-Integrität als gemanagten Service, der einen hohen Automatisierungsgrad ermöglicht.

Sicher

- Minimiert Schwachstellen im Entwicklungszyklus und in der Lieferkette von Software
- Schutz vor Code-Manipulation, Schlüsseldiebstahl und Malware
- Zentrale Steuerung verhindert unsichere Praktiken im Zusammenhang mit der Erstellung, Verteilung und Nutzung von Softwarecode durch Zugriffskontrollen für Schlüssel und Signaturen

Compliance-konform

- Entspricht den Standards und Anforderungen des Software Supply Chain Integrity Frameworks
- Ermöglicht die Durchsetzung unternehmensinterner und gesetzlicher Vorgaben und sorgt für mehr Agilität

IoT Trust: IoT-Sicherheit automatisiert durchsetzen

Bei IoT handelt es sich schnell um tausende Geräte, die gesichert werden müssen. Das bedeutet auch, tausende digitaler Identitäten zu managen, inklusive Ausstellung, Erneuerung und Genehmigung von Zertifikaten. Manuelle Prozesse bedeuten in diesem Kontext einen sehr großen Aufwand und die Gefahr von menschlichem Versagen.

Wesentliches Merkmal dieses auf Maschinenzertifikate ausgerichteten PKI-Services ist der hohe Automatisierungsgrad in den für die Zertifikatserstellung erforderlichen Prozessen. Applikationen, Maschinen, Things, Netzelemente, VoiP Telefone, Drucker etc. werden damit in die Lage versetzt, über standardisierte Protokolle und ohne manuellen Eingriff Zertifikate effizient aus dem Trust Center der Telekom Security zu beziehen.

Wir bieten einen PKI-Service für die Sicherheit im IoT M2M Umfeld und unterstützen mit unserem modularen Aufbau eine Vielzahl von Automatisierungsschnittstellen.

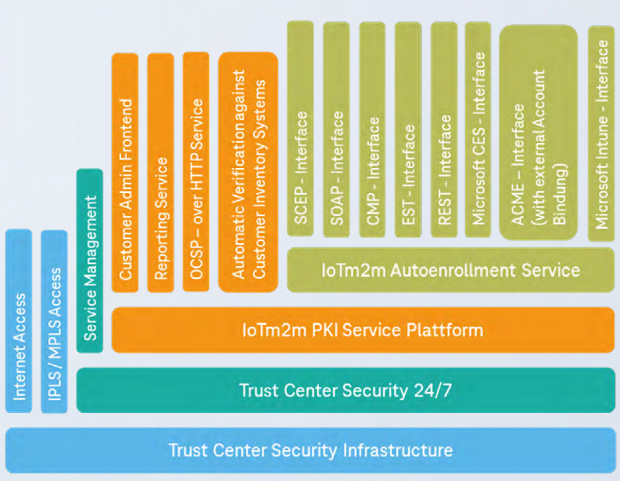
Einfach

- Einfache Skalierung zur Ausstellung und Unterstützung von Millionen von Zertifikaten und Geräten
- Eigenständiger und automatisierter Zertifikatsbezug durch ein Gerät oder eine Applikation
- Implementierungsabhängig ist ein orts- und zeitunabhängiger Zertifikatsbezug ohne manuellen Eingriff mit einem vollständig nachgelagerten Zertifikats-Lifecycle Prozess möglich

Sicher

- Bindung der Identität an jedes einzelne Gerät als Grundlage für eine sichere Kommunikation

IoTm2m.ID PKI-Service



Trust Lifecycle Manager: PKI managen

Bei der Realisierung einer Public Key Infrastruktur (PKI) müssen unterschiedliche technische, prozessuale und betriebliche Anforderungen beachtet werden. Auch regulatorische Vorschriften und Compliance-Vorgaben können sehr hohe Anforderungen an die Realisierung und den Betrieb der PKI stellen. Aufbau, Betrieb und Integration einer PKI erfordern daher eine hohe Fachkompetenz.

Wir bieten Ihnen erprobtes Zertifikats-Lifecycle-Management, das einen hohen Automatisierungsgrad ermöglicht.

Zertifikats-Lifecycle-Management

- Vereinfachung des IT-Betriebs mit Zertifikatserkennung, -verwaltung und -benachrichtigung sowie einem hohen Grad an Automatisierung und Integration

PKI-Dienste

- Optimierte Nutzung von digitalen Identitäten mit einem Plus an Sicherheit durch die Bereitstellung von Zertifikaten für Personen, Geräte, Server sowie andere IT-Ressourcen

Geschafft!

Lisa ist zufrieden. Die Implementierung der PKI ist abgeschlossen und ein wichtiger Schritt hin zu einer robusten und zuverlässigen IT-Sicherheitsinfrastruktur, die den wachsenden Anforderungen an Datenschutz und neuen vielfältigen Bedrohungen gerecht wird, ist getan. Die PKI verbessert die Sicherheit von IT-Anwendungen erheblich und minimiert das Risiko von Datenlecks oder unbefugtem Zugriff. Dies bedeutet nicht nur eine Investition in die Sicherheit des Unternehmens, sondern ist auch ein Meilenstein für den Schutz der Daten von Kunden und Mitarbeitenden.

Die PKI ermöglicht es dem Unternehmen, digitale Zertifikate auszustellen, verschlüsselte Verbindungen zu authentifizieren und die Identität von Usern zu überprüfen. Im Zusammenhang mit der Benutzeranmeldung wurde beispielsweise das traditionelle Passwortverfahren erfolgreich durch digitale Zertifikate ersetzt. Damit wird die in der Vergangenheit häufig zu beobachtende Weitergabe von Passwörtern unter den Mitarbeitenden weitgehend unterbunden. Die Mitarbeitenden, die im Zuge der Einführung der PKI zusätzlich für das Thema Sicherheit in einer digitalen Welt sensibilisiert wurden, arbeiten heute wesentlich sicherer und gleichzeitig effizient zusammen.

Auch organisatorisch ergeben sich Synergien, beispielsweise im Kontext von Offboarding-Prozessen. Verlässt ein Mitarbeiter das Unternehmen, kann er durch die zentrale Sperrung eines digitalen Zertifikats automatisch für alle Anwendungen und Systeme, die in die PKI-Architektur eingebunden sind, gesperrt werden.

Last but not least können durch die Kombination der PKI mit anderen Sicherheitstechnologien im Sinne von Zero Trust heute nur autorisierte Personen auf sensible Informationen zugreifen, so dass die Daten vor unbefugtem Zugriff geschützt sind. Durch die Integration verschiedener Sicherheitstechnologien und IT-Anwendungen kann das Unternehmen seine Systeme und Daten verlässlich schützen und sich in innovativer Weise auf das eigene Kerngeschäft konzentrieren.

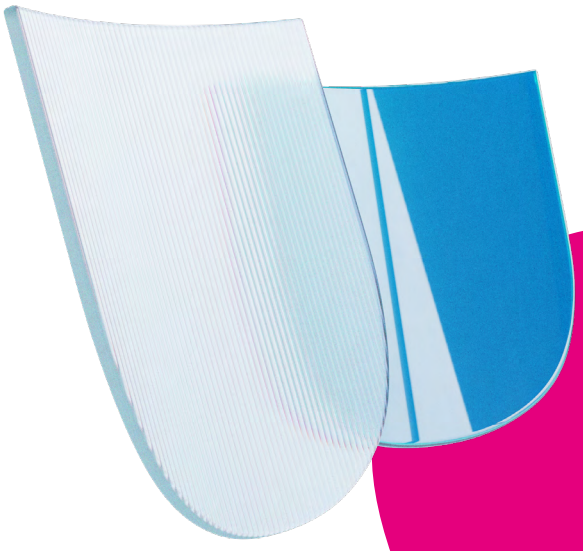
All dies trägt dazu bei, die Wahrnehmung des Unternehmens als vertrauenswürdiger Partner in der digitalen Welt zu stärken und das Geschäft erfolgreich auszubauen.

Legen Sie den Grundstein für Ihre Cybersicherheit!

Sie planen die Einführung einer Public Key Infrastruktur in Ihrem Unternehmen oder wollen eine bestehende Public Key Infrastruktur aktualisieren, um diese zukunftssicher zu machen?

Unsere PKI-Produkte, Services und individuellen Lösungen basieren auf neuesten Technologien und werden stetig weiterentwickelt. Sie haben die Wahl, ob Sie eine PKI von uns inhouse konzipieren und integrieren lassen, oder ob Sie auf unsere Kompetenz als zertifizierten Vertrauensdienstanbieter setzen und Ihre PKI in unseren hochsicheren Rechenzentren betreiben lassen.

Wir unterstützen Sie gern beim Aufbau Ihrer Public Key Infrastrktur!



Deutsche Telekom Security GmbH | 07/2024

Kontakt
security.dialog@telekom.de
security.telekom.de

Herausgeber
Deutsche Telekom Security GmbH
Office Port 1
Friedrich-Ebert-Allee 71–77
53113 Bonn

Connecting your world.