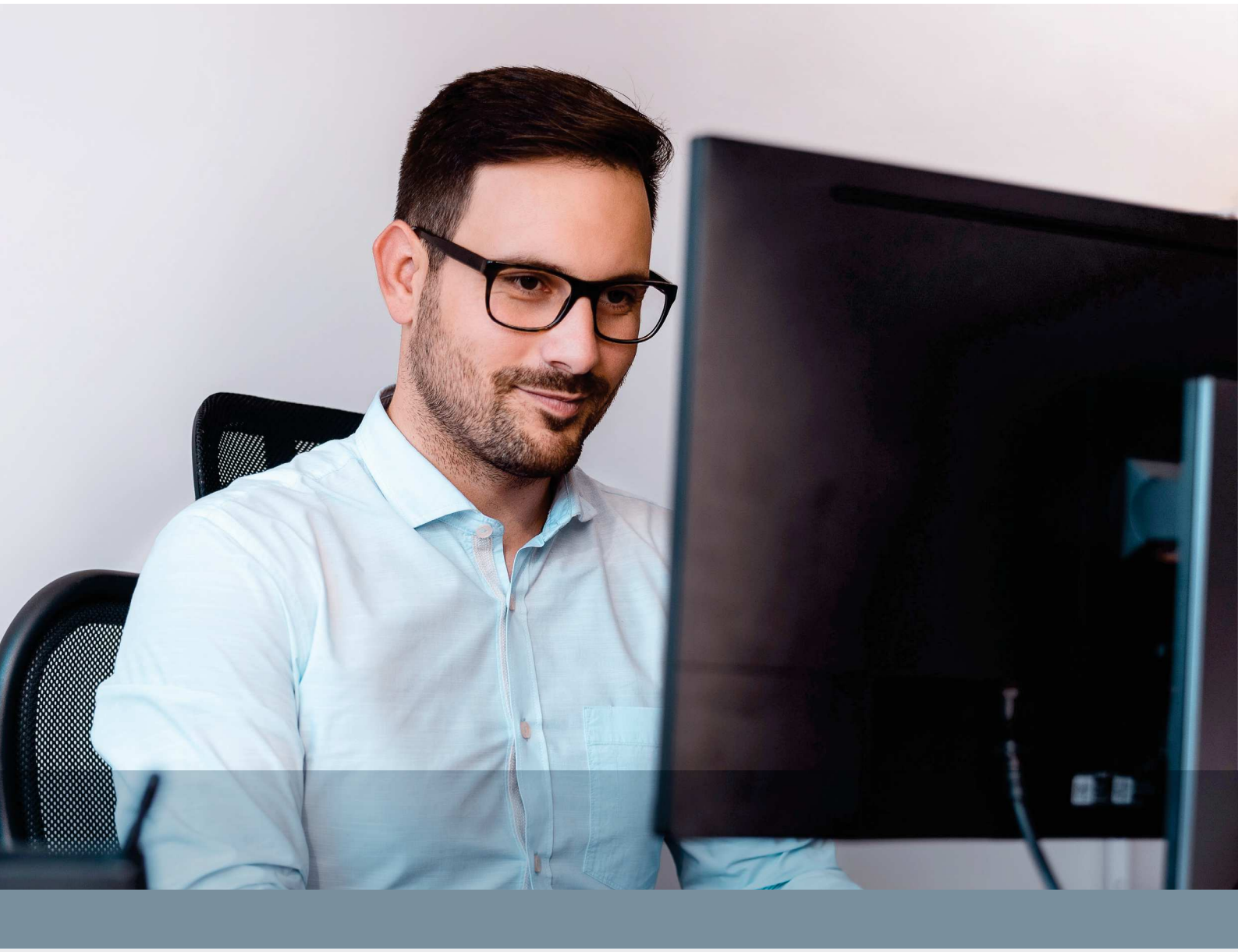
digicert + QuoVadis



Sichere digitale Kommunikation mit S/MIME Zertifikaten

Verschlüsseln, Signieren, Authentisieren!

Schützen Sie Ihre gesamte E-Mail-Kommunikation mit dem sichersten digitalen Verschlüsselungsverfahren, dem S/MIME Zertifikat von Digicert QuoVadis.

digicert® + QuoVadis

WAS SIND DIGITALE ZERTIFIKATE?

„Eine E-Mail, die nicht verschlüsselt ist, ist wie eine Postkarte. Jeder kann sie lesen.“
In der elektronischen Welt erlangt der Begriff „Vertrauenswürdigkeit“ eine neue Dimension. Benutzer müssen immer mehr in der Lage sein, den Kommunikationspartner eindeutig zu identifizieren sowie gegenseitig die Identitäten zu prüfen und damit das Vertrauen in elektronische Transaktionen zu untermauern. Nutzen Sie für Urlaubspost Postkarten und für Ihre E-Mail-kommunikation stattdessen lieber S/MIME!

Digitale Zertifikate und die daraus erstellbaren Digitalen Signaturen sind der Schlüssel zur Sicherstellung von Online-Sicherheit und Vertrauen.
Ein elektronisches Zertifikat ist die nicht veränderbare Form einer „**elektronischen Identitätskarte**“, welche dem Benutzer/Besitzer erlaubt, sich online zu identifizieren, Daten und Dokumente zu verschlüsseln und diese digital zu signieren.

QuoVadis übernimmt für die eindeutige Identifikation im Bereich der digitalen Kommunikation für Sie quasi die Rolle eines Notars.

Das Digicert QuoVadis Secure E-Mail Zertifikat kann zum Signieren, Verschlüsseln und Authentisieren Ihrer E-Mails verwendet werden.

WARUM VERSCHLÜSSELUNG DER DIGITALEN KOMMUNIKATION?

Schutz vor **Wirtschaftsspionage**, **Cybercrime**, **E-Mail-Phishing**, besonders in der E-Mail-Kommunikation oder bei Online Transaktionen (z. B. von Webbrowser zu Webseite) sowie bei der Speicherung vertraulicher Daten auf mobilen Geräten.

Unsere digitalen Zertifikate bescheinigen die Korrektheit der Informationen und die Nachvollziehbarkeit der Herkunft. Damit erzeugte elektronische Signaturen beweisen, dass eine Nachricht nicht manipuliert wurde, gewährleisten die Vertraulichkeit und können rechtliche Verbindlichkeit erwirken.

Rechtssicherheit. Zahlreiche Normen und Gesetze, wie die DSGVO, stellen hohe Anforderungen an die IT-Sicherheit. z. B.:

- **Datenschutz** und die Nachweisbarkeit von Vorgängen bei der Verarbeitung personenbezogener Daten.
- Einhaltung der **Revisionssicherheit** für elektronische Dokumente (gesetzliche Anforderungen an aufbewahrungspflichtige Dokumente).
- **Sicherheitsstandards** wie ISO 27001/02 oder IT-Grundschutz (BSI-Standard 100-2). Nicht selten weisen Daten und Anwendungen ein geringeres Sicherheitsniveau auf, als in den für das Unternehmen relevanten Standards oder Vorschriften gefordert.

WARUM S/MIME (SECURE-E-MAIL) ZERTIFIKATE?

Secure E-Mail: Ihre Geschäftskommunikation basiert zu großen Teilen auf E-Mail Verkehr? Dann wird es Zeit, dieses wichtige Kommunikationsinstrument zu schützen. Für Sie und für Ihre Kunden. Das Digicert QuoVadis Secure E-Mail Zertifikat wird auf Personen ausgestellt und kann zum Signieren, Verschlüsseln und Authentisieren Ihrer E-Mails verwendet werden. S/MIME oder Secure/Multipurpose Internet Extensions stellen den Industriestandard für die Verschlüsselung und das Signieren von nachrichtenbasierten Daten dar.

Das Prinzip von S/MIME basiert auf der **asymmetrischen Verschlüsselung**. Bei der asymmetrischen Verschlüsselung wird für jeden, der verschlüsselt kommunizieren möchte, ein Schlüsselpaar erstellt. Dieses besteht jeweils aus einem **privaten (geheimen)** und einem **öffentlichen Schlüssel**. Diese werden so generiert, dass eine Datei, die mit dem öffentlichen Schlüssel verschlüsselt wurde, nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden kann.

DAS DIGICERT QUOVADIS SECURE E-MAIL ZERTIFIKAT …

unterstützt S/MIME (Secure/Multipurpose Internet Mail Extensions), so dass Benutzer ihre E-Mails signieren oder verschlüsseln können und sicher sein können, dass eine Nachricht auch wirklich von dem identifizierten Absender (Authentisierung) gesendet wurde. Wurde die Nachricht verschlüsselt, dann kann diese nur der Empfänger öffnen, der ein kompatibles Zertifikat besitzt.

SIGNIEREN

Durch die Signatur gewinnt Ihr Dokument an Vertrauen und Sicherheit für den Empfänger.

1. **Authentizität:**
   Stellt die elektronische Identität einer Person sicher und der Unterzeichner eines Dokumentes oder einer E-Mail-Nachricht, inkl. Anhänge, wird überprüfbar.
2. **Senderintegrität:**
   Stellt die Unveränderbarkeit und Unverfälschbarkeit von elektronischen Informationen und Dokumenten sicher.
3. **Nicht Anfechtbarkeit/Unleugbarkeit:**
   Unterstützt das ultimative Ziel, Authentizität zu beweisen und die Integrität zu schützen. Die Nichtabstreitbarkeit und damit Beweisbarkeit ergeben in der elektronischen Kommunikation die Möglichkeit, den Absender für die elektronisch übermittelten Informationen in einem Rechtsstreit haftbar zu machen.

VERSCHLÜSSELN

1. **Vertraulichkeit:**
   Durch Nachrichtenverschlüsselungen werden die Inhalte von E-Mail-Nachrichten geschützt. Die Inhalte können nur vom vorgesehenen Empfänger angezeigt werden und bleiben vertraulich. Sie können nicht von anderen Personen gelesen werden, die diese Nachricht möglicherweise empfangen oder anzeigen. Durch Verschlüsselung wird die Vertraulichkeit einer Nachricht auf dem Versandweg und am Speicherort gewährleistet.
2. **Datenintegrität:**
   Wie bei digitalen Signaturen stehen durch Nachrichtenverschlüsselung Datenintegritätsdienste als Ergebnis der spezifischen Operationen zur Verfügung, durch die die Verschlüsselung ermöglicht wird.

Durch unsere Secure E-Mail Zertifikate wird Ihr Geschäftsverkehr sicher und vertraulich. Sie und Ihre Kunden können sich vor Phishing-Attacken schützen.

NUTZEN UND VORTEILE BEI DER VERWENDUNG VON QUOVADIS S/MIME ZERTIFIKATEN

Erfahrung und Expertise

Digicert QuoVadis ist spezialisiert für Dienstleistungen auf dem Gebiet der Public-Key-Infrastruktur (PKI) mit digitalen Zertifikaten und elektronischen Signaturen und kann auf eine über 20-jährige Erfahrung und Unternehmensgeschichte zurückblicken. Darum sind Sie mit unseren Zertifikaten auf der sicheren Seite.

State of the Art E-Mail Verschlüsselung (S/MIME)

1. Schutz vor Cyberangriffen
2. Revisionsschutz [ISO 9001]
3. Schutz von Kundendaten/Datenschutz [z. B. DSGVO]

Kommunzieren Sie, auch im **digitalen** Bereich, sicher und vertrauenswürdig! Setzen Sie S/MIME Zertifikate problemlos für jede Kommunikation mit **Ihren Geschäftspartnern** und Ihrer **Sparkasse** ein.

S/MIME ist ‚state of the art'. Das Verfahren gilt derzeit als die beste und sicherste Verschlüsselungsmethode am Markt und definitiv als eine der Technologien der Zukunft.

Erhöhung des Digitalen Brands und des Vermarktungspotenziales: Nutzen Sie S/MIME zur aktiven Kommunikation und zeigen Sie Ihren Kunden und Geschäftspartnern: „Wir kommunizieren sicher und gehen sensibel mit Ihren Daten um! Wir nutzen die gleiche, hochprofessionelle Verschlüsselungsmethode, die auch die Sparkasse nutzt!"

Geringe Kosten im Vergleich zu Datendiebstahl, Cyber-Attacken und daraus eventuell resultierenden Klagen.

Leicht zu installieren, wartungsfrei, leicht zu erneuern.

S/MIME Zertifikate sind **absolut vertrauenswürdig**, eineindeutig zuzuordnen (Signatur) und bieten die Möglichkeit zur verschlüsselten Kommunikation.

Die **Verwendbarkeit** ist **unabhängig von der Sparkasse** – S/MIME Zertifikate können für sämtliche Kommunikation im eigenen Eco-System genutzt werden.

Techn. Support und **Produktstabilität** sichergestellt. Zusammenarbeit mit zertifizierten Anbietern garantiert.

digicert® + QuoVadis

SUPPORT

Team Sparkasse

Dr. Norman Hoppen
Peter Hupfauer
Pascal Wernli

info.de@quovadisglobal.com

+49 89 452 45 85 0

Ismaninger Str. 52
D-81675 München