portfolio@NESTEC: **ZERTIFIKATE**

S/MIME & SSL-Zertifikate von GlobalSign: provided by NESTEC

Die GlobalSign PersonalSign-Zertifikate verwenden die S/MIME-Technologie, damit Benutzer E-Mails digital signieren und verschlüsseln können.

Das digitale Signieren einer E-Mail weist die Urheberschaft nach und verhindert Manipulationen. Damit wird dem Empfänger der E-Mail versichert, dass die E-Mail von Ihnen und nicht einem Betrüger stammt und dass der Inhalt der E-Mail bei der Übermittlung nicht verändert wurde.

Das Verschlüsseln einer E-Mail gewährleistet den Datenschutz der Nachricht und verhindert, dass sensible Daten in die falschen Hände geraten.

Sichere E-Mail wird durch die digitale Zertifikats-Lösung von GlobalSign namens PersonalSign erreicht. PersonalSign-Zertifikate sind kryptografisch signierende Zertifikate, die Ihre verifizierte, physische Identität an das Zertifikat binden. Damit können Empfänger von E-Mail-Nachrichten verifizieren, dass die E-Mail tatsächlich von Ihnen stammt.

Digital-signierte & verschlüsselte E-Mail: Weist Urheberschaft nach und gewährleistet den Datenschutz der Nachricht!

E-Mails digital signieren & verschlüsseln

Sichere E-Mail: S/MIME

SSL: Vertrauen

Datenschutz & Sicherheit

GlobalSign SSL-Zertifikate bieten die stärkste Verschlüsselung und besten Vorteile, um Ihre Website zu schützen und die Anforderungen an heutige moderne Websites zu erfüllen. Kunden und Besucher Ihrer Website wissen, dass ihre Browser-Sitzung sicher ist und dass Zahlungsdaten und persönliche Daten sicher und verschlüsselt übertragen werden.

Stärkstes & schnellstes SSL: GlobalSign bietet die stärkste verfügbare SSL-Verschlüsselung durch die Verwendung von SHA-256 und 2048-Bit-RSA-Schlüsseln. Darüberhinaus bieten wir ECC-Unterstützung.

Universelle Geräteunterstützung: GlobalSigns SSL wird von allen gängigen Browsern, Anwendungen und Geräten vertraut. Besucher vertrauen automatisch Ihrer SSL-Sicherheit, egal welches Gerät sie verwenden.

Anerkannte Sicherheitsaudits: GlobalSign ist seit 2001 eine „Webtrust akkreditierte" Zertifizierungsstelle und hat von 1996 bis heute weltweit über 2,5 Mio. vertrauenswürdige SSL-Zertifikate ausgestellt.

Kostenlose SSL-Tools: Kostenlose Tools, die bei der CSR-Generierung (Auto-CSR), SSL-Installation (SSL-Server-Test) und beim SSL-Management (CIT) hilfreich sind.

Erstklassiger Support: Der SSL-Support von GlobalSign genießt einen ausgezeichneten Ruf, der nicht zuletzt aufgrund der zahlreichen lokalen Büros mit Unterstützung in der lokalen Sprache erarbeitet wurde.

Kostensparende und komfortable Features: Nutzen Sie kostenlose Premium-Features, wie z.B. Installation auf beliebig vielen Servern und die Verwendung desselben Zertifikats für „www.domain.com" und „domain.com".

NITROKEY - Security Hardware
Schützt gegen
- Massenüberwachung
- Verhindert Identitätsdiebstahl
- Verhindert Datenverlust

Ihre E-Mails, Dateien, Festplatten, Server-Zertifikate und Benutzerkonten werden kryptografisch gesichert. Ihre geheimen Schlüssel werden immer sicher in der Nitrokey-Hardware gespeichert und können nicht gestohlen werden. Das Gerät ist durch eine PIN geschützt und sicher gegen alle Arten von Angriffen. 2-Stufen Sicherheitsmechanismen helfen falls der Pin vergessen wurde.

Nitrokey ermöglicht: Sicheres Login: Login an Webseiten (z. B. Google, Facebook) mittels sicherer Einmalpasswörter (OTP), U2F oder gewöhnlicher statischer Passwörter. Login an Computern und Netzwerkdiensten (z. B. SSH) mittels Zertifikaten. **Verschlüsselter, mobiler Speicher:** Tragen Sie wichtige Daten herum, immer Hardware-verschlüsselt im Nitrokey Storage (8-64 GB). Kompatibel mit Windows, Linux und Mac OS. **E-Mail-Verschlüsselung:** Email-Verschlüsselung mittels GnuPG, OpenPGP oder S/MIME und Ihrem präferiertem Email-Programm. Ihre geheimen Schlüssel werden sicher im Nitrokey gespeichert. **Festplatten- & Dateiverschlüsselung:** Verschlüsseln Sie Ihre Festplatten und Dateien mittels TrueCrypt/VeraCrypt, GnuPG Tools und weiteren Tools. Ihre geheimen Schlüssel werden sicher im Nitrokey gespeichert. **Server-Sicherheit:** Schützen Sie Ihre Server-Zertifikate mit bis zu 43 ECC- und 35 RSA-Schlüssel mit dem Nitrokey HSM. Ideal für Sicherheits-Server.

portfolio@NESTEC: **ZERTIFIKATE**

S/MIME & SSL-Zertifikate
FAQ - Häufig gestellte Fragen

Sichere E-Mail: S/MIME

S/MIME Protokoll nutzen - Wie funktioniert's?
GlobalSigns PersonalSign Zertifikate verwenden das Secure/Multi-Purpose Internet Mail Extensions (S/MIME) - Protokoll zum digitalen Signieren von E-Mails. S/MIME-Verschlüsselung bietet Nachrichten-integrität, Authentifizierung, Datenschutz über Datenverschlüsselung und Unleugbarkeit über digitale Signaturen.
Die meisten Mail-Clienten unterstützen S/MIME, wie z. B. Microsoft Outlook, Thunderbird, Apple Mail, Lotus Notes und Mulberry Mail.

Sichere E-Mail für Unternehmen - Mehrere Zertifikate managen
Für Organisationen, die eine unternehmensweite sichere E-Mail-Lösung implementieren wollen, ist Managed PKI die Lösung, um mehrere PersonalSign-Zertifikate für S/MIME zu verwalten.
EPKI bietet vereinfachte Einsatzoptionen und alle Möglichkeiten zur Zertifikatsverwaltung, sodass Administratoren PersonalSign-Zertifikate im gesamten Unternehmen ausstellen, erneuern, neuausstellen und widerrufen können. EPKI bietet erhebliche Kosteneinsparungen gegenüber dem Kauf einzelner PersonalSign Zertifikate und ausführliche Reporting-Funktionen ermöglichen es Unternehmen, die Zertifikatsaktivität von einem zentralen Account aus zu überwachen.

SSL: Datenschutz & Sicherheit

Was ist ein SSL-Zertifikat?
SSL-Zertifikate sind kleine Dateien die einen kryptografischen Schlüssel mit den Unternehmensdetails digital verbinden. Wenn das Zertifikat auf dem Webserver installiert ist, wird das Schlosssymbol und das https-Protokoll (über Port 443) aktiviert und bietet so eine sichere Verbindung zwischen Webserver und Webbrowser.

Warum brauch ich ein SSL-Zertifikat?
SSL-Zertifikate sind ein wesentlicher Teil des Internets. Sie verschlüsseln nicht nur die Kommunikation zwischen Computer und dem Server, auf dem eine Website gespeichert ist, sondern bieten auch noch die Absicherung, dass die Seite wirklich von dem Unternehmen ist, als das es sich ausgibt.

Was sind die verschiedenen Arten von SSL?
Es gibt normalerweise drei verschiedene Levels an Überprüfung, auf die die meisten SSL-Zertifikate basieren: Domain Validierung (DV), Organization Validierung (OV), und Extended Validierung (EV).
Der Hauptunterschied zwischen den Zertifikaten betrifft die Informationen, die von der Zertifizierungsstelle, GlobalSign, geprüft werden. Je nach Überprüfungslevel werden unterschiedliche Informationen im Zertifikat und der Browser-Adresszeile angezeigt.

EV SSL aktiviert zum Beispiel die grüne Adresszeile im Browser und zeigt dort direkt Informationen zum Unternehmen an.

Optionales Bundle - READY-TO-USE

NITROKEY-Stick + Zertifikate
Durch NESTEC fertig konfiguriert nach dem Szenario des Anwenders!
Ein Sicherheitskonzept garantiert 100% Vertraulichkeit.
Sprechen Sie mit uns über Ihre Anforderungen, wir liefern die fertige Lösung.

15 JAHRE
nestec

https://nestec.at/cert
https://**nestec.at** | **office@nestec.at**