



HOUSING & HOSTING

# cityKEY

## Mehr Sicherheit und Vertrauen durch verschlüsselten Datenverkehr.



**Öffentlich zugängliche Webapplikationen bedürfen vor allem beim Thema Sicherheit besonderer Aufmerksamkeit. Schützen Sie den Datenverkehr von und zu sensiblen Webanwendungen mit cityKEY.**

Digitale Zertifikate ermöglichen den Schutz der Vertraulichkeit, Authentizität und Integrität von Daten durch eine korrekte Anwendung öffentlicher Schlüssel. Durch den Einsatz hochwertiger SSL-Zertifikate wird den Anwendern ein hohes Vertrauen entgegengebracht.

### Ihre cityKEY Vorteile auf einen Blick

- Erhöhte Sicherheit und Schutz vor Online-Betrug durch verschlüsselte Datenkommunikation
- Höhere Vertrauensbildung auf Kundenseite
- Entlastung bei administrativen Aufgaben
- Automatische Benachrichtigung vor dem Ablauf von Zertifikaten

### Das gewisse Extra. Verschlüsselte Datenübermittlung.

Mit cityKEY haben Sie die Möglichkeit, aus einer großen Bandbreite von SSL-Zertifikat-Produkten zu wählen. Wir unterstützen Sie bei der Auswahl des für Ihre Anwendung am besten geeigneten Zertifikates und wickeln alle, mit der Registrierung verbundenen organisatorischen Details, für Sie ab. Weiters stehen wir als technischer Ansprechpartner zur Verfügung und halten Sie stets über Neuerungen am Laufenden.

Informieren Sie sich auch über Housing & Hosting, Security & Monitoring, Vernetzung & Internet sowie Telefonie & Video. Am besten gleich auf [www.wir-sind-hier.at](http://www.wir-sind-hier.at)

**LINZ AG**  
TELEKOM

## SSL-Zertifikat-Optionen

### Details

#### Gesicherte Domains

- Single Domain
- Beliebig viele Subdomains einer Domain

#### Verschlüsselung

- 40 bis 256 Bit

#### Garantie

- USD 5.000,- bis USD 1.500.000,-

#### Gültigkeitsoptionen

- 1 Jahr bis 3 Jahre

#### Grüne Adressleiste

- Bei erweiterter Validierung (EV)

#### Trustlogo

abhängig vom gewählten Zertifikat:

- Norton secured
- Secured by RapidSSL
- Secured by thawte
- Dynamisches GeoTrust True Site Seal mit Firmennamen und Datum/Time Stamp

#### Validierungsmethode

- Domain Validierung
- Vollständige Unternehmensvalidierung
- Erweiterte Validierung\*

\* Im Validierungsverfahren muss die CA (Zertifikats-Autorität) sicherstellen, dass der Antragsteller für das Zertifikat der Eigentümer der Domain ist und die jeweilige genehmigte Person beim Antragsteller angestellt und befugt ist, Extended Validation SSL-Zertifikate zu erwerben. Zudem muss die Identität des Unternehmens überprüft werden. Extended Validation ist über eine grüne Adressleiste im Browser erkennbar.

**Es besteht die Möglichkeit von Volumenrabatten beim gleichzeitigen Erwerb mehrerer Zertifikate.**

LINZ AG TELEKOM zertifiziert nach ISO 27001, ISO 9001, ISO 45001

## Trustlogos für Webserver-Zertifikate und E-Mail-Zertifikate



Profitieren Sie von einem persönlichen Beratungsgespräch.