



Zwischenzertifikate

Intermediate Certificates

Vorteile vs. Nachteile

Nachteile

- Komplexität**
 - Erhöhte Komplexität bei der Konfiguration und Verwaltung von Zertifikaten.
- Fehleranfälligkeit**
 - Potenzielle Fehler bei der Konfiguration oder Implementierung von Zwischenzertifikaten.
- Abhängigkeit von Zertifizierungsstellen**
 - Abhängigkeit von vertrauenswürdigen Zertifizierungsstellen für die Ausstellung von Zwischenzertifikaten.
- Kosten**
 - Mögliche zusätzliche Kosten für den Erwerb und die Verwaltung von Zwischenzertifikaten.
- Zertifikatskettenlänge**
 - Möglichkeit, dass lange Zertifikatsketten die Leistung beeinträchtigen können.
- Sicherheitsrisiken**
 - Potenzielle Sicherheitsrisiken bei unzureichender Konfiguration oder unerwarteten Zertifikatsfehlern.
- Zeitaufwand**
 - Erfordert Zeit und Ressourcen für das Management und die Aktualisierung von Zwischenzertifikaten.
- Kompatibilitätsprobleme**
 - Mögliche Kompatibilitätsprobleme mit älteren Systemen oder Anwendungen.
- Vertrauensfrage**
 - Notwendigkeit, Vertrauen in die Zertifizierungsstellen zu setzen, die Zwischenzertifikate ausstellen.
- Übertragungsgröße**
 - Erhöhung der Übertragungsgröße durch die Einbeziehung von Zwischenzertifikaten in die Zertifikatskette.

Vorteile

- Vertrauenskette (Chain of Trust)**
 - Bildung einer Vertrauenskette zwischen Serverzertifikat und Stammzertifikat.
- Sicherheit**
 - Schutz des Stammzertifikats und zusätzliche Sicherheitsmaßnahmen gegen Kompromittierung.
- Hierarchische Organisation**
 - Organisatorische Struktur für Zertifikatsdienste und -verwaltung.
- Flexibilität**
 - Flexible Anpassung an Änderungen oder Aktualisierungen in der Zertifizierungsinfrastruktur.
- Zertifikatsmanagement**
 - Effizientes Management von Zertifikatsdiensten und -infrastruktur.
- SSL/TLS-Zertifikate**
 - Integration von Zwischenzertifikaten in SSL/TLS-Verschlüsselung für sichere Kommunikation.
- Skalierbarkeit**
 - Einfache Skalierung und Verwaltung von Zertifikaten für verschiedene Dienste.
- Zertifikatsüberprüfung**
 - Überprüfung der Gültigkeit des Serverzertifikats durch den Client.
- Authentizität**
 - Verbesserung der Authentizität des Servers und der Kommunikationspartner.
- Integrität**
 - Sicherstellung der Integrität der Kommunikation durch verschlüsselte Kanäle.

