



## IKE/IPsec Inspector

# Nachweisbare IT-Sicherheit mit flexiblen Software-Tools

## IKE/IPsec Inspector

### Etablierte Netzprotokolle als sicherer Standard

**Transport Layer Security (TLS)** und **Internet Key Exchange (IKE) / Internet Protocol Security (IPsec)** sind als Grundlage sicherer Netze anerkannte Standards. Die Implementierung und Konfiguration sind extrem komplex und bieten bei nicht korrekter Umsetzung Schlupflöcher für Cyberkriminelle.

Mit dem **IKE/IPsec Inspector** von achelos schließen Sie diese Schlupflöcher. Wir haben unsere leistungsfähige Testsuite mit einer akkreditierten Prüfstelle entwickelt, um die Sicherheit und Konformität Ihrer Produkte und Lösungen herstellerunabhängig zu prüfen. Der IKE/IPsec Inspector unterstützt Sie bei der Entwicklung, der Zulassung und im Feldbetrieb durch eine flexible Zusammenstellung Ihrer gewünschten Testfälle.

Die Testsuite lässt sich sowohl lokal wie auch remote als Testing as a Service (TaaS) einsetzen.

### Der IKE/IPsec Inspector von achelos unterstützt

- Hersteller von Netzwerkkomponenten,
  - Evaluatoren und Zertifizierer,
  - Betreiber von Systemen,
  - IT-Abteilungen in Unternehmen,
  - staatliche Institutionen,
- sich vor Cyberattacken zu schützen.

### IKE/IPsec-Inspector-Testabdeckung

Der IKE/IPsec Inspector prüft den kompletten Aufbau der IKE-Verbindung bis zur gegenseitigen Authentisierung, das Verhalten beim Rekeying und die Reaktion auf fehlerhaftes Verhalten, z. B.:

- fehlende oder falsche Kommunikationsteile
- fehlerhaftes Schlüsselmaterial
- fehlerhafte Zertifikate
- ungeeignete Cipher-Suiten
- fehlerhafte Reaktion auf Manipulationen

Der IKE/IPsec Inspector von achelos behandelt Testaspekte der IPsec-Ebene und simuliert einen IKE-Responder. Die Testsuite bietet ein effizientes Testmanagement und verschiedene Simulationsumgebungen bis hin zu automatisierten Testläufen. Die Implementierung der Sicherheitsprotokolle wird detailliert untersucht, und Ergebnisse sind nachweisbar protokolliert.

### Der Testfallkatalog wird kontinuierlich erweitert und basiert auf Anforderungen aus folgenden Quellen:

- funktionale Spezifikationen
- technische Richtlinien (TR)
- Zertifizierungen
- kryptographische Standards
- Application-Notes zur Common-Criteria-Zertifizierung
- Evaluierungsstandards
- Penetrationstests
- Anforderungen zur Dokumentation nach Common Criteria
- Definitionsgrundlagen der IKE/IPsec-Testsuite:
  - IETF RFC 3602 „The AES-CBC Cipher Algorithm

## Architektur der IKE/IPsec-Testumgebung

### IKE/IPsec Inspector – modular und flexibel

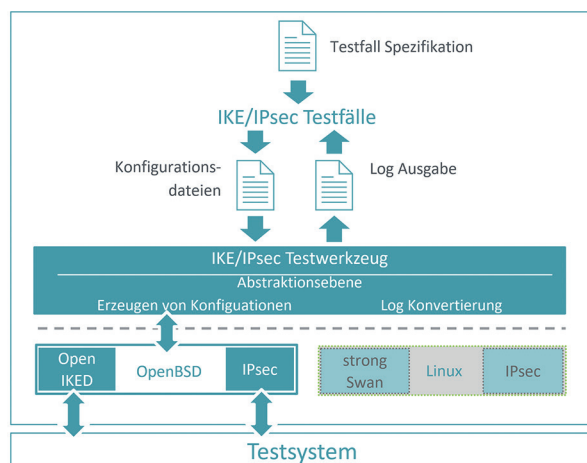
Die Architektur der Testsuite ist modular aufgebaut. Auf Basis von **Qumate by achelos** lassen sich verschiedene Testsuiten, Werkzeuge und Simulationen integrieren. Automatisierte Tests sowie ausführliche Testberichte messen die Produktqualität.

### Mehr als 130 IKE-Testfälle

Im IKE/IPsec Inspector sind mehr als 130 verschiedene Testfälle enthalten, die kontinuierlich weiter ausgebaut werden.

### Automatisierte Testverfahren für Profis

Eine Vielzahl von Test- und Evaluierungshäusern nutzt bereits Qumate by achelos, um Tests im Rahmen akkreditierter Prüfverfahren durchzuführen.



## Bedrohungspotenziale von Cybersicherheit

### Systeme kommunizieren über öffentliche Netzwerke

Internet, Funknetzwerke  
Daten können abgehört und verändert werden

### Schutz der Integrität der Daten

Sensordaten, Steuersignale

### Verhinderung des Mitlesens durch Dritte

Geschäftsgeheimnisse, personenbezogene Daten

### Identifikation der Kommunikationspartner

Verträge

### Häufig werden alle diese Maßnahmen benötigt

Bankgeschäfte, Kritische Infrastrukturen

### In achelos-Testsuiten steckt:

- das Expertenwissen unserer BSI-geschulten Mitarbeitenden
- die seit 2009 kontinuierliche Weiterentwicklung der Qumate-Plattform
- die Praxiserfahrung des etablierten Testcenters Qumate by achelos im Bereich Kritischer Infrastrukturen
- ein hoher Automatisierungsgrad: schnell, flexibel und mit nachweisbaren Ergebnissen

**Qumate**  
by achelos

## Vorteile für den Einsatz

- Herstellerunabhängige Testumgebung
- Einhaltung von BSI-Sicherheitsrichtlinien
- Kostenersparnis durch schnellere Zertifizierung
- Effizientes Testen durch hohen Automatisierungsgrad
- Mit einer akkreditierten Prüfstelle entwickelte Testsuiten
- Prüfungsumfang, Testtiefe und Angriffsszenarien individuell wählbar
- Reproduzierbare und revisions sichere Dokumentation der Testergebnisse