Qumate.Security.TLS and Qumate.Security.IKE/IPsec

Protect your network from cyber attacks

The fear of cyber attacks is increasing

The Federal Office for Information Security (BSI) has reported a significant increase of in the number of malicious program variants in the 2018 report on IT security in Germany. There are over 800 million malicious programs and around 380,000 new variants are added every day.

The focus is on attacks on companies and critical infrastructures

The methods of the attackers have become more professional: from the watering can principle to precisely selected cyber attacks on individual targets. Hackers are acting very strategic.

Gateways in companies remain frequently wide open for hackers

Consequences of a cyber attack for manufacturers of products and systems operators include:

- loss of confidence in safety measures and data transmission networks
- Sustainable image damage for the company or the organisation
- An enormous cost of restoration of no longer decryptable data
- Extreme time pressure and high effort for renewed protection of hacked data
- Claims for compensation by affected customers

Established network protocols as a safe standard

Transport Layer Security (TLS) and **Internet Key Exchange (IKE)/Internet Protocol Security (IPsec)** are available as the common standard for secure networks.
The implementation and configuration is extremely complex and, if not correctly implemented, offers loopholes for attackers.

Proven IT security with flexible software tools

achelos provides you with powerful test equipment to find these gaps and errors, to ensure that your network connections are safe. Test objectives are from the verification of the complete structure of the TLS or IKE/IPsec connection up to the mutual authentication and the reaction to erroneous behavior, e.g.:

- Missing or incorrect communication parts
- Incorrect key material
- Incorrect certificates
- Unsuitable cipher suites
- Vulnerabilities
- Incorrect response to manipulations

The test suites of achelos can be used flexibly including automated test runs. This is achieved by a very efficient test management and different simulation environments. The implementation of the security protocols is examined in detail and results are verifiable documented.

achelos test suites ensure your network

We have developed our test suites in close cooperation with an accredited testing laboratory. The test case catalog is continually expanded and is based on requirements from the following sources:

- Functional specifications
- Technical guidelines (TR)
- Certifications
- Cryptographic standards
- Application notes for common criteria certification (CC)
- Evaluation Standards
- Penetration testing
- Requirements for documentation according to CC

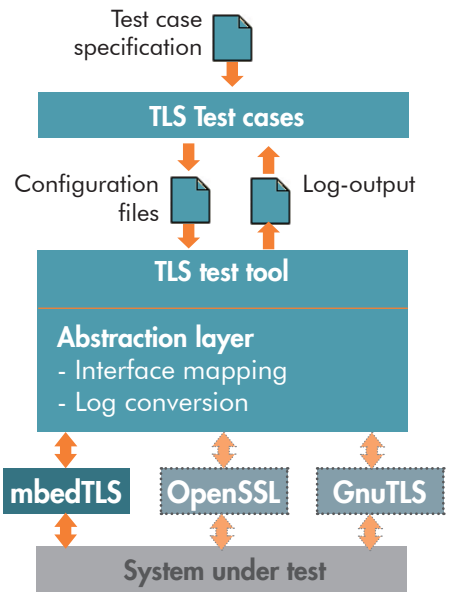
Trust Seal
www.teletrust.de/itsmig

Secur IT y
made in Germany

Automated test procedures for professionals

A large number of test houses and evaluation bodies are already using the test suites from our Qumate.World to carry out tests under accredited testing procedures. The architecture and implementation of the test suites have a modular design. Various test suites, tools, and simulations can be integrated with the Qumate.Testcenter. Automated tests and detailed test reports will substantiate the quality of your products. You do not need any additional IT infrastructure or expensive laboratory equipment.

Architecture of the Qumate.Security.TLS test environment



Advantages for using the TLS and IKE/IPsec test suites:

- Avoid IT configuration errors
- Compliance with BSI security guidelines
- Cost savings through faster certification
- Efficient testing due to high degree of automation
- Comfortable simulation environment and easy to use
- Test scope, test depth and attack scenarios individually selectable
- Reproducible and audit-proof documentation of the test results

Start immediately – cyber security is manageable

Use our manufacturer-neutral test suites developed with an accredited test center to ensure the security of your TLS and IKE/IPsec network connections. Due to a flexible architecture and implementation, the achelos test suites are product-independent and can be used immediately!

achelos supports e.g.

- Manufacturers of network components
- Evaluators and certification bodies
- Operators of IT systems
- IT departments in companies
- Governmental institutions

to protect themselves against cyber attacks.

Our test suites contain:

- The expertise of our BSI trained staff
- The ongoing development of the Qumate platform since 2009
- The vast experience of the established Qumate.Testcenter in the area of critical infrastructures
- A high degree of automation: fast, flexible and with verifiable results

Qumate.Security.World

Product variants:

- Qumate.Security.TLS-Client
- Qumate.Security.TLS-Server
- Qumate.Security.TLS-Checklist
- Qumate.Security.IKE/IPsec

Optional:

- simulation environment
- software development kit (SDK)

Flexible test management licensing:

All product variants are available for on premise or Testing as a Service (Taas) usage.

achelos GmbH Vattmannstraße 1 33100 Paderborn Germany T +49 5251 14212-0 info@achelos.de www.achelos.de