Modernising Transport Layer Security

information guide

www.vodacommessaging.co.za
support@vodacommessaging.co.za
087 55 00 200

Contents

Overview

TLS (Transport Layer Security) is the primary protocol that secures HTTPS Websites and Webservices. It has a long history dating back over 20 years (TLS 1.0), 15 years (TLS 1.1), and 10 years (TLS 1.2) and even longer with its predecessor SSL. Over that time, the industry has learned a lot about how to build secure protocols.

The security TLS provides arises from the cooperation of various cryptographic algorithms. Moreover, TLS constantly evolves with the security industry - new technology and business requirements must be satisfied, while the latest security threats must be mitigated. Algorithms can become obsolete over time, or practices can be abandoned, with each change affecting the overall security of a TLS instance.

Purpose

The volatility in security TLS provides, has motivated various standards organisations to publish guideline documents, so that a minimum baseline for TLS security can be established in a particular market, sector, or service.

The objective of this communication is to notify our clients, their technical teams, and stakeholders of our sunsetting of the various older protocols, ciphers, cipher suites to maintain a default high standard of security, comply with Industry Standards & Compliances, and for modernising Transport Security within our organization(s) and service offerings.

Scope

Protocol:

Both TLS 1.0 and TLS 1.1 protocols are insufficient for protecting information due to known vulnerabilities. Standards, such as PCI-DSS, require TLS 1.0 and TLS 1.1 to be retired.

TLS 1.2 was published to address weaknesses in TLS 1.0 and 1.1 and has enjoyed wide adoption. Having offered this protocol for many years, with 98% of our traffic defaulting to this currently, we will be retiring support for the following protocols on **1 July 2021**:

- TLS 1.0
- TLS 1.1

Cipher and Cipher Suites:

At the same time, we are enhancing our security posture by adjusting and preferring:

- Modern authentication encryption, Authenticated Encryption with Associated Data (AEAD) cipher suites, namely AES-GCM.
- Ephemeral keys providing Perfect Forward Secrecy (PFS) ciphers, namely ECDHE.

Resulting in these recommended TLS configurations:

- For ECDSA keys:
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- For RSA keys:
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Private key and Certificates:

Where possible, we are taking this opportunity to roll out Elliptic Curve (ECDSA) Certificates for better scalability beyond the standard 112 bits of security currently offered on our RSA 2048-bit keys. We will begin with offering the same level of security with ECDSA 256-bit keys, and only scale when needed in the future.

Enforcement

All connections to our Websites and Webservices will be required to use HTTPS for communication, as such we will strengthen our implementation of HTTPS enforcement/redirection on the server-side. To avoid additional round trip latencies, clients are advised to make secure HTTPS calls initially.