Secure online transactions policy for .POST domains

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

Introduction

Transport Layer Security (TLS) is an open standard for encryption which enables people and applications to communicate in private over the Internet.

TLS is the successor to Secure Sockets Layer (SSL) technology, and it provides three essential services to help ensure security on the Internet: i) message confidentiality; ii) authentication; and iii) message integrity.

Message confidentiality: TLS provides a mechanism for encrypting the messages between application clients and servers with the aim of ensuring that, even if someone captures the messages as they are in transit between the sender and destination, the messages cannot be read.

Authentication: TLS provides a mechanism to validate the identity of the end points of the communications.

Message integrity: TLS provides a mechanism to ensure that messages are not changed as they move between client and server.

TLS policy

TLS policy defines security requirements for all communication under .POST domains.

Req. #	*Description*	*Requirement Type*	*Explanatory Notes*
TLS.R01	All content for the website without exception SHALL always be served over https protocol	REQUIRED	See RFC 7525 for more details
TLS.R02	Version 1.2 (or above) of TLS protocol SHALL be used for transferring data over https. TLS v1.2 is the only version that offers modern authenticated encryption (i.e. AEAD)	REQUIRED	See [RFC 5288] and [RFC 5246]
TLS.R03	Secure cypher suites like the AES-GCM family SHALL be used for transferring data over https	REQUIRED	
TLS.R04	2,048-bit RSA private keys SHALL be used to sign Digital Certificates	REQUIRED	
TLS.R05	Digital Certificates SHALL use SHA256 Signature Algorithm	REQUIRED	

Req. #	*Description*	*Requirement Type*	*Explanatory Notes*
TLS.R06	Digital Certificates SHOULD be obtained from a reliable Certificate Authority (CA)	RECOMMENDED	Suggested criteria to select a reliable CA are: i) CAs undergo regular audits; ii) CA has a business focus; iii) CA should provide support for both CRL and OCSP revocation methods; iv) certificate management options are available; and v) CA should provide support
TLS.R07	Digital certificates SHOULD cover all the DNS names used for a site	REQUIRED	
TLS.R08	Private keys used to sign digital certificates SHOULD be protected	RECOMMENDED	
TLS.R09	Implement HTTP Strict Transport Security (HSTS) which define userAgent-side and server-side security policy in order to avoid man-in-the-middle attacks. This mitigates the risk of SSL Stripping[1]	REQUIRED	See RFC 6797, section 2.4 for the detailed core requirements

.POST will be monitoring implementation of these requirements on a regular basis. If any domain is not compliant with the Policy the domain owner will be informed within 3 business days. After that, the incident management procedures will be applied, and the owner of the domain will need to comply with it and resolve the issue to prevent the domain name from being decommissioned.

The validity and accuracy of your TLS certificate can be verified online using dedicated tools. Examples of available tools are www.ssllabs.com/ssltest/ and www.htbridge.com/ssl/.

[RFC 2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, Available at: www.rfc-editor.org/info/rfc2119
[RFC 6797]	Hodges, J., Jackson, C., and A. Barth, “HTTP Strict Transport Security (HSTS)”, RFC 6797, November 2012, Available at www.rfc-editor.org/info/rfc6797
[RFC 5288]	Salowey, J., Choudhury, A., and D. McGrew, “AES Galois Counter Mode (GCM) Cipher Suites for TLS”, RFC 5288, August 2008, Available at www.rfc-editor.org/info/rfc5288
[RFC 5246]	Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2”, RFC 5246, DOI 10.17487/RFC5246, August 2008, Available at www.rfc-editor.org/info/rfc5246
[RFC 7525]	Sheffer, Y., Holz R. and P. Saint-Andre, “Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”, RFC 7525, May 2015, Available at tools.ietf.org/html/rfc7525

[1] “SSL Stripping” attacks attempt to remove the use of Secure Socket Layer/Transport Layer Security (SSL/TLS) altogether by modifying unencrypted protocols that request the use of TLS.