

Implementation of TLS Certificate on Email Gateways

TLS Version and Upgrade Requirements

TLS version 1.0 is recommended, however, newer versions of TLS i.e. TLS 1.1 and TLS 1.2 are all backward compatible to TLS 1.0 and SSL 3.0.

There is no mandatory requirement to upgrade to the latest TLS versions as all TLS versions are backward compatible. However, technical teams of FI(s) should keep themselves updated with TLS versions and its compatibility and security issues.

SBP is providing flexible timelines to enable all FI(s) to implement TLS over SMTP. FI(s) shall enable TLS which will automatically enable required security/encryption with TLS-enabled domains, whereas unencrypted email exchange will continue with non-TLS FI(s).

However, after expiry of final implementation and testing time, all FI(s) would be required to enforce TLS on all other FI's domains within Pakistan.

Timelines for TLS Implementation

Phase-I	Procurement and Installation	All FI(s) shall complete procurement and installation of TLS certificates by <u>October 31, 2013.</u>
Phase-II	Soft Launch and Testing	All FI(s) shall start testing their TLS connections and resolve problems, if any, by January <u>31st, 2014.</u>
Phase-III	Final Implementation	All banks shall be fully ready and compliant to the above instruction by <u>February 1st, 2014.</u>

Contact Details

Please contact **021-3245-5535** in case of any queries on the above instructions.