9. Mandatory Cipher Suites

In the absence of an application profile standard specifying otherwise, a TLS-compliant application MUST implement the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA (see Appendix A.5 for the definition).