Security Guidance for Core Components

In the open-source code, we’ve provided access to Web-based application programming interfaces (APIs) and database software. As a part of this, we also wanted to provide some high-level security guidelines for these core components.

Database Guidance:

* + Ensure connection strings have Encrypt=True and TrustServerCertificate=False.
  + Provide the customer guidance on establishing encryption at rest using [TDE](https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-with-azure-sql-database).

Personally Identifiable Information (PII) Data (PII data is any data that has any personally identifiable metadata about an individual, e.g. email address, social security number (or government ID number), phone number, etc.):

* It is your responsibility to treat PII data appropriately based on regional rules. When deploying applications to the Cloud, you must ensure that you are both familiar with your regional data policies and conform to them.

Web API:

* + Provide customer guidance against XSS and CSRF.
    - Another thing to explore is the [Web Application Firewall](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-application-firewall-overview)
  + Provide customer guidance around certificate generation and consumption.

|  |  |  |  |
| --- | --- | --- | --- |
| **Algorithm Type** | **Not Allowed**  crypto algorithms / Keys must be replaced in existing code or used only for decryption | **Minimally Acceptable**  Crypto algorithms/key lengths okay for existing code | **Recommended**  Crypto algorithms / Key lengths for new code |
| Symmetric Block | DES, 2 Key 3DES, DESX, RC2, SKIPJACK | 3 Key 3DES\*\*\* | AES (>=256 bit)  AES (>=128 bit) for Service Bus |
| Block Cipher Modes | ECB |  | CBC, CCM, GCM\* |
| Symmetric Stream | SEAL, CYLINK\_MEK, RC4 (<128bit or unreviewed) | RC4 (>= 128bit) | None – Block cipher is preferred |
| Asymmetric | RSA (<2048 bit),  Diffie-Hellman (<2048 bit), 1024 bit DSA, exception process for smart cards and other HW able to support 1024  but less than 2048 bits | RSA (>= 2048bit),  Diffie-Hellman (>= 2048bit) | RSA (>=2048bit),  Diffie-Hellman (>= 2048bit),  ECC (>= 256bit),  Elliptic Curve Cryptography P-256 or greater |
| Hash, including HMAC usage | SHA-0 (SHA), SHA-1\*\*, MD2, MD4, MD5 | 3DES MAC  SHA-2 (SHA-224), 3DES MAC for Service Bus | SHA-2  (SHA-256,  SHA-384,  SHA-512) |
| HMAC Key Lengths | <112bit | 112bit =< x < 128bit | >= 128bit |
| Symmetric Block | DES, 2 Key 3DES, DESX, RC2, SKIPJACK | 3 Key 3DES | AES (>=256 bit)  AES (>=128 bit) for Service Bus |