Encryption Changes in 9.4TS1M8 for Data at Rest & Data In-Motion

SAS released its 9.4 Maintenance version M8 in the end of January 2023. M8 comes with changes and new functionalities and some product and features that were deprecated. A new feature in SAS is how SAS encrypts **data at rest** and **data in motion**. A follow up article will discuss data encryption in more detail.

In SAS 9.4M8, Cryptographic Libraries provided by SAS/SECURE module; Foundation server, is **replaced** by libraries provided with an Operating System (OS). If encrypted stored passwords are to be used provision of required cryptographic libraries is a customer side task.

Note:

1. SAS 9.4M8 no longer supports OpenSSL versions 0.9.8 and 1.0.0.
2. On *Nix/Linux some of the OpenSSL library versions that are supported and tested with SAS software include **OpenSSL 3**, **OpenSSL 1.1.1**, and **OpenSSL 1.0.2**
3. On Windows, SAS uses **SChannel SSP** (Security Support Provider) that provides TLS internet standard authentication protocols and BCrypt that provides other encryption algorithms. All Windows system libraries are FIPS certified. Since SAS consumes OS provisioned cryptographic libraries not all cipher suites would be available on a given specific WIN OS version. It is recommended that in that case to opt for a cipher suite that is available on the WIN OS and supported with SAS.
4. SAS 9.4M8 no longer uses Crypto-C ME libraries.
5. SAS does not yet support IBM System SSL on z/64, but plans to provide support in the near future

The default cipher suites supported for TLS 1.2 are as follows:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The default cipher suites supported for TLS 1.3 are as follows:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_AES_128_CCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_CHACHA20_POLY1305_SHA256

Protocols in TLS/SSL (Schannel SSP) could be viewed at https://learn.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-

In the next two parts we will explore in detail SAS Encryption for Data at Rest and Data in Motion in SAS 9.4TS1M8.