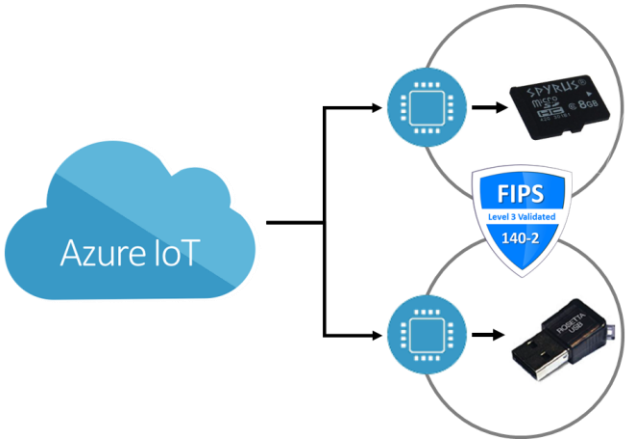
SPYRUS®

Rosetta® Azure IoT Enhanced Software Development Kit

Hardware Backed Security for the Internet of Things

Enhance the security of Azure IoT connected endpoints with the assurance that comes with hardware backed cryptography. The Rosetta Azure IoT Enhanced SDK provides hardware backed key storage and cryptography in several convenient form factors. The SDK consists of SPYRUS Rosetta HSM's, example code and documentation that illustrate how to raise the assurance of authentication and communication with Microsoft's Azure IoT Hub.

The Enhanced SDK supports device registration with Azure IoT Hub as well as generating Shared Access Signatures (SAS) permitting authentication while avoiding sending keys or secrets over the wire/air. In addition, the Enhanced SDK also supports securing communications with Azure IoT Hub through TLS/SSL integration for X.509 certificate based authentication and session encryption.



Quick Start

1. Begin by setting up and verifying the Rosetta HSM in your SDK Package, refer to the **Rosetta Hardware Getting Started Guide** included in the SDK
2. Create Azure IoT Account if you don't have one
   https://azure.microsoft.com/pricing/free-trial/
3. Get the Microsoft Azure IoT SDK for C from GitHub
   https://github.com/azure/azure-iot-sdk-c
4. Read Rosetta Azure IoT Enhanced SDK Developers Guide for a complete explanation of how to integrate Rosetta HSM's with the Microsoft IoT SDK

Corporate Headquarters
1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@SPYRUS.com

East Coast Office
+1 (732) 329-6006 phone
+1 (732) 832-0123 fax

UK Office
+44 (0) 113 8800494

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au

Document Number 515-328001-01