**Course Title:** Secure-by-Design Bootcamp for the Internet of Things

**Duration:** 5-months

- CL1.0 - Network/System Cybersecurity Intro
- CL1.1 - Device Architecture Overview
- CL2.0 - Secure Component Technologies
- CL3.0 - Cryptocell as Security Sub-System
- CL4.0 - PKI/Cryptography Concepts and Applied Cryptography
- CL5.0 - TLS/Secure Communication
- CL6.0 - Design, Development, Certification and Regulatory Compliance Regimes
- HL1.0 - NIST/NCCoE Trusted Network-Layer Onboarding & Lifecycle Management
- HL2.0 - FIDO (Secure) Device Onboarding (FDO/SDO)
- HL3.0 - NIST/NCCoE Trusted Network-Layer Onboarding Scenarios (PoC) with FIDO FDO
- Hands-on learning through actual development, leveraging a "prescriptive" set of IoT application use cases & code that replicates the five NIST/NCCoE demo scenarios i.e. NIST/NCCoE Trusted Network -Layer Onboarding & Lifecycle Management Scenarios, while utilizing:
    - A Global Semiconductor Alliance and GlobalPlatform-compliant Secure-MCU (SMCU), that is enabled by a GlobalPlatform_TEE-based Secure Component as HRoT,
    - HRoT-based Chain of Trust (CoT) to comply with (or meet) Zero-Touch Onboarding and Zero-Trust Architecture requirements (for Network -Layer Onboarding & Lifecycle Management),
    - FIDO FDO-based bootstrapping of root credentials and connectivity, to support and enable the five NIST/NCCoE demo scenarios. i.e. NIST/NCCoE Trusted Network -Layer Onboarding & Lifecycle Management Scenarios.