Tier-1 Evidence List - DRAFT

Corresponds to 24MM Cybersecurity Specification v1.5. Updated 2022-09-30

Not listing design review materials for items which PCG understands that Tier-1s do not have responsibility for.

Not listed in any particular. Future versions will group evidences more logically.

|  |  |  |
| --- | --- | --- |
| **Evidence ID** | **Description** | **Requirements** |
|  | Summary of ISO 21434 cybersecurity activities. See 21434 Appendix A.2. | 24MM.SEC.PRJ.PGM.1 |
|  | Supplier record of capability that meets ISO 21434 RQ-07-01. | 24MM.SEC.PRJ.PGM.2 |
|  | A summary of all industry standards and best practices initiatives and documentation that describes how security is being built into the software development process. | 24MM.SEC.PRJ.PGM.3 |
|  | Name(s) and contact information of the designated security specialist(s) Toyota can coordinate with for conducting and reviewing supplier risk assessments. | 24MM.SEC.PRJ.PGM.4 |
|  | Development schedules that include all cybersecurity features. AKA Feature Rollout Plan (FROP). | 24MM.SEC.PRJ.PGM.5, 6 |
|  | Software Bill of Materials (SBOM) | 24MM.SEC.PRJ.PGM.7-9,11-12 24MM.SEC.PLAT.OS.SFC.1,2 |
|  | Hardware Bill of Materials (HBOM) | 24MM.SEC.PRJ.PGM.10-12  24MM.SEC.QC.FDE.1 |
|  | Unencrypted flash images | 24MM.SEC.PRJ.PGM.9,12  24MM.SEC.PRJ.TST.7  24MM.SEC.PLAT.OS.SFC.1-4  24MM.SEC.PLAT.LOG.GEN.3  24MM.SEC.PLAT.OS.FS.1-3,5-6 24MM.SEC.PLAT.CRT.1-2  24MM.SEC.PLAT.COM.TLS.1-2,4,6-7  24MM.SEC.PLAT.COM.WIFI.1-2  24MM.SEC.APP.CRT.1  24MM.SEC.APP.HRD.1-4  24MM.SEC.QC.FDE.3-5 |
|  | Secure boot design review materials (If implemented by supplier)   * Including description of anti-rollback design. * Includes how startup parameters like Linux kernel command line values are protected from tampering. | 24MM.SEC.PRJ.PGM.13  24MM.SEC.HW.SB.1-2  24MM.SEC.PLAT.SB.1-3,11-20,22-32 24MM.SEC.PLAT.OS.GEN.1  24MM.SEC.APP.SB.1 |
|  | Secure update design review materials (If implemented by supplier)   * Include flows for both local and remote. * Includes any application specific update mechanisms. | 24MM.SEC.PRJ.PGM.13 24MM.SEC.PLAT.UPD.1-19 24MM.SEC.APP.UPD.1 |
|  | Secure debug design review materials (If implemented by supplier)   * Includes list of all debug interfaces and how they’re disabled or authenticated * Includes how debug and production keys are separated, including relevant eFuse settings. * Schema for debug identity | 24MM.SEC.PRJ.PGM.13  24MM.SEC.PLAT.DBG.GEN.1 24MM.SEC.PLAT.DBG.DEV.1-2  24MM.SEC.PLAT.DBG.PROD.2-23  24MM.SEC.APP.DBG.1-2 |
|  | Full disk encryption design review materials (If implemented by supplier)   * Include ICE configuration | 24MM.SEC.PRJ.PGM.13 24MM.SEC.PLAT.FDE.1-8  24MM.SEC.QC.FDE.2 |
|  | Key management design doc (if implemented by supplier) | 24MM.SEC.PLAT.KEY.3-10 |
|  | Document describing how SEI CERT standards are utilized as part of the development practices and code reviews. | 24MM.SEC.PRJ.SW.1 |
|  | Coding style specification used for software development. | 24MM.SEC.PRJ.SW.2 |
|  | Dates code reviews were completed for each software component. | 24MM.SEC.PRJ.SW.3  24MM.SEC.APP.LOG.1 |
|  | Linter tool configuration file. | 24MM.SEC.PRJ.SW.4 |
|  | Vulnerability scan configuration file. | 24MM.SEC.PRJ.SW.5 |
|  | Summary report of static analysis results that confirms no violations are left unresolved. | 24MM.SEC.PRJ.SW.6 |
|  | List of compiler options | 24MM.SEC.PRJ.SW.8-9  24MM.SEC.APP.HRD.5-7 |
|  | List of CVEs for each software component and “yes/no” status if that CVE is fixed in the version of the software component that is used. | 24MM.SEC.PRJ.SW.11 |
|  | Documentation on the security of their development and production environments. | 24MM.SEC.PRJ.SW.12 |
|  | Log level guidance provided within three months of the start of development. | 24MM.SEC.PRJ.SW.13 |
|  | Materials and documentation necessary to reproduce all cybersecurity requirements verification testing and penetration testing conducted by the supplier. | 24MM.SEC.PRJ.TST.1 |
|  | Suppliers shall provide all necessary wiring harnesses, test hardware, and documentation to enable vulnerability testing of the device. This includes artifacts for:   * Diagnostic modes. * Internal debug interfaces such as JTAG, serial ports, Ethernet, etc. * Internal diagnostic or analysis tools. * Test environments and emulators.   System internals documentation necessary for validation, to be specified by Toyota. | 24MM.SEC.PRJ.TST.2 |
|  | Production software builds at each release. | 24MM.SEC.PRJ.TST.4 |
|  | Toyota shall be provided with the necessary documentation and tools such that it can install updates independently from the supplier during development and testing. | 24MM.SEC.PRJ.TST.5 |
|  | Full update packages | 24MM.SEC.PRJ.TST.6 |
|  | Change log that includes security functions. | 24MM.SEC.PRJ.TST.8 |
|  | Secure boot source code or access to it | 24MM.SEC.PRJ.TST.9 |
|  | TEE source code or access to it | 24MM.SEC.PRJ.TST.10 |
|  | Fuzz test configuration | 24MM.SEC.PRJ.TST.13-14 |
|  | Fuzz test report | 24MM.SEC.PRJ.TST.11-12 |
|  | Document describing the security controls of the factory trusted area. | 24MM.SEC.PRJ.FCT.1-4 |
|  | Wi-Fi chipset datasheet | 24MM.SEC.HW.COM.WIFI.1-2 |
|  | Bluetooth datasheet | 24MM.SEC.HW.COM.BLT.1 |
|  | Board schematics | 24MM.SEC.HW.PER.1-4  24MM.SEC.PLAT.DBG.PROD.1 |
|  | PCB routing diagrams | 24MM.SEC.HW.PER.2 24MM.SEC.HW.MEM.4  24MM.SEC.PLAT.DBG.PROD.1 |
|  | Serializer datasheet | 24MM.SEC.HW.PER.4 |
|  | List of GPIO / peripheral configuration | 24MM.SEC.HW.PER.2 |
|  | Documentation showing certifications of secure environment | 24MM.SEC.HW.MEM.1 |
|  | Datasheet of flash storage | 24MM.SEC.HW.MEM.2 24MM.SEC.QC.FDE.1 |
|  | Use case list of cryptographic functions (signatures, encryption, hashes, etc.) | 24MM.SEC.PLAT.CRYP.1-7 24MM.SEC.APP.CRYP.1 |
|  | List of each key provisioned on the device and its algorithm type, bit length, storage location, and operation location. | 24MM.SEC.PLAT.KEY.2  24MM.SEC.APP.KEY.1 |
|  | Processor datasheets implementing secure boot | 24MM.SEC.PLAT.SB.4-6,8-11,21 24MM.SEC.PLAT.STG.5 |
|  | Confirmations from processor suppliers for secure boot design elements (if needed) | 24MM.SEC.PLAT.SB.5-10,12,21 |
|  | Rationale for resource limit settings | 24MM.SEC.PLAT.OS.GEN.3 |
|  | Consolidate, final Linux kernel configuration | 24MM.SEC.PLAT.OS.GEN.5  24MM.SEC.PLAT.OS.KRN.1-29  24MM.SEC.PLAT.COM.FWL.5-6 |
|  | Documentation of the RNG initialization process   * Include documentation of KASLR RNG source. | 24MM.SEC.PLAT.OS.GEN.6 |
|  | List of all passwords and PINs and corresponding hashing algorithm. | 24MM.SEC.PLAT.OS.GEN.7 |
|  | List of all processes running as root and why it’s necessary | 24MM.SEC.PLAT.OS.USR.1 |
|  | List of all users and purpose for each | 24MM.SEC.PLAT.OS.USR.2 |
|  | List of all groups and purpose for each | 24MM.SEC.PLAT.OS.USR.3 |
|  | Rationale for umask setting. | 24MM.SEC.PLAT.OS.FS.4 |
|  | List of which processors on the SoC can reach each peripherals | 24MM.SEC.PLAT.SOC.1 |
|  | Listing of memory ranges accessible by each processor. | 24MM.SEC.PLAT.SOC.2 |
|  | Listing of each peripheral that has bus master capabilities and the allowed memory ranges. | 24MM.SEC.PLAT.SOC.3  24MM.SEC.PLAT.PER.7 |
|  | Documentation of the implementation and configuration mechanisms for SoC memory controls. | 24MM.SEC.PLAT.SOC.4 |
|  | Default firewall configuration. | 24MM.SEC.PLAT.COM.FWL.1-4,7-8 |
|  | Documentation describing Wi-Fi default process generation process. | 24MM.SEC.PLAT.COM.WIFI.4 |
|  | Documentation describing how MAC address randomization is implemented | 24MM.SEC.PLAT.COM.WIFI.3 |
|  | List of USB devices supported by ECU | 24MM.SEC.PLAT.COM.INT.1 |
|  | CAN whitelist | 24MM.SEC.PLAT.COM.INT.3 |
|  | Design review materials for automated testing | 24MM.SEC.PLAT.AT.1 |
|  | Documentation and tools necessary to extract and review log records. | 24MM.SEC.APP.LOG.2-12 |
|  | Documentation on how Bluetooth is configured to be compliant with NIST SP 800-121 rev2. | 24MM.SEC.APP.COM.BLT.1 |
|  | List of available services on CAN, Ethernet, etc. and the corresponding authentication mechanism. | 24MM.SEC.APP.COM.INT.1 |
|  | If supported, documentation of how code and data is loaded from USB and authenticated before use. | 24MM.SEC.APP.COM.INT.2-3 |
|  | Rationale for capabilities assigned to each application and service. | 24MM.SEC.APP.SBX.2 |
|  | List of processes and whether the user ID is unique or common. Rationale for all common user IDs. | 24MM.SEC.APP.SBX.3 |
|  | Listing of Qualcomm eFuse settings. | 24MM.SEC.QC.SB.1,4-7,9,11 |
|  | QTEE configuration | 24MM.SEC.QC.TEE.1-5 |

Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
| 1.4 | July 29th, 2022 | ・Initial version. |
| 1.5 | September 30th, 2022 | ・Added revision history.  ・Changed reference to "24MM Cybersecurity Specification v1.5 Updated 2022-09-30". [AGLSD-2664]  ・Deleted “24MM.SEC.PLAT.KEY.1” from Evidence ID 44. [AGLSD-2664] |
|  |  |  |