# Payment Card Industry (PCI)
# PTS HSM Security Requirements

## Summary of Changes from PCI PTS HSM Version 1.0 to 2.0

**May 2012**

| Document and Requirements Reference[1] | Change | Type[2] |
|---|---|---|
| SR General and DTRs A1, A5, A6 and A7 | Introduction of a two two-tier approval structure for HSMs. These tiers differentiate only in the "Physical Security Derived Test Requirements" section as delineated in the PCI PTS HSM Derived Test Requirements. HSMs may be approved as designed for use in controlled environments as defined in ISO 13491-2: Banking — Secure cryptographic devices (retail) or approved for use in any operational environment | Requirement Change |
| SR General | Restructuring of sequence of requirements to be consistent with POI v3 where requirements are similar | Requirement change |
| SR A1 | Added attack potential calculation to requirement | Requirement change |
| SR A2 | Additional clarification on role of tamper evidence | Additional Guidance |
| SR A3<br>(Old) | Deleted unique enclosure requirement as no longer valid - similar to POI - ~~The HSM design protects against substitution of the HSM such that it is not practical to construct a duplicate from commercially available components. For example, the enclosure is not commonly available~~. | Requirement change |
| SR A6<br>(Old) | Moved to C1 | Requirement change |
| SR A7 | New requirement based on POI - Determination of any PCI-related cryptographic key resident in the device or used by the device, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation with a minimum of 15 for exploitation | Requirement change |
| SR B5<br>(Old) | Merged into requirement B7 | Requirement change |
| SR B13 | Modified to address both keys contained in or protected by the HSM and that the HSM does not permit key usage to be changed to allow keys to be used in a way they could not previously be used. | Additional Guidance |

| Document and Requirements Reference[1] | Change | Type[2] |
|---|---|---|
| SR B17 | New Requirement derived from POI | Requirement change |
| SR B18 | New Requirement derived from POI | Requirement change |
| SR B20 | New Requirement | Requirement change |
| SR C1 | Created new Policies and Procedures section to more fully differentiate from Physical, Logical and Device Management sections. | Additional Guidance |
| SR D1 | Clarify that immediate re-certification is not required for changes which purely rectify errors and faults in software in order to make it function as intended and do not otherwise remove, modify, or add functionality. | Additional Guidance |
| SR D5 | Modified to reflect that HSMs may go through the hands of intermediaries between the manufacturer and the point of deployment | Requirement change |
| SR D6 | Modified to reflect that HSMs do not typically go to a key loading facility before deployment | Requirement change |
| SR D7 | New Requirement modified from POI | Requirement change |
| SR D8 | New Requirement modified from POI | Requirement change |
| SR E1 | Modified to reflect that HSMs do not typically go to a key loading facility before deployment and that they may go through the hands if intermediaries between the manufacturer and the point of deployment | Requirement change |
| SR E2 | Modified to reflect that HSMs do not typically go to a key loading facility before deployment and that they may go through the hands of intermediaries between the manufacturer and the point of deployment | Requirement change |
| SR E3 | Modified to reflect that HSMs do not typically go to a key loading facility before deployment | Requirement change |
| SR E4 | New Requirement - modified from POI | Requirement change |

| Document and Requirements Reference[1] | Change | Type[2] |
|---|---|---|
| SR E5 | New Requirement - modified from POI | Requirement change |
| SR E6 | New Requirement - modified from POI | Requirement change |
| SR E7 | New Requirement - modified from POI | Requirement change |
| DTRs | Updated algorithms and key sizes to be consistent with those stipulated in PTS POI Security Req. v3Added text clarifying applicability of module | Requirement change |
| DTR A1 | Added guidance to define immediately inoperable | Additional Guidance |
| DTR A7 | Clarification of scope of requirement | Additional Guidance |
| DTR B1 | Added detailed information defining types of self-tests required | Additional Guidance |
| DTR B5 | Added definitions for data, control and status interfaces | Additional Guidance |
| DTR B6 | Added criteria for reuse of buffers | Additional Guidance |
| DTR B7 | Additional guidance for authentication and use of sensitive services | Additional Guidance |
| DTR B8 | Stipulate criteria for external key loaders used to load secret and private plaintext keys to HSMs | Additional Guidance |
| DTR B8 | Added criteria for authentication and tracking of the actions of individuals | Additional Guidance |
| DTR B10 | Added guidance for the methods used to produce encrypted text that relies on “non-standard” modes of operations (e.g., format-preserving Feistel-based Encryption Mode (FFX)) | Additional Guidance |
| DTR B11 | Added stipulation that HSMs must support top level master keys with a strength of at least triple length TDES but may optionally provide support for legacy purposes support for double length equivalent strength TDES keys | Additional Guidance |
| DTR B11 | Added guidance for use of alternate key management schemes when HSM is in PCI mode. | Additional Guidance |

| Document and Requirements Reference[1] | Change | Type[2] |
|---|---|---|
| DTR B11 | Stipulate that the HSM must support use of the TR-31 Key Derivation Binding Method or an equivalent key bundling methodology and may optionally support, in addition, the TR-31 Key Variant Binding Method or an equivalent | Additional Guidance |
| DTR B11 | Introduce criteria to support remote key loading techniques using public key methods consistent with PTS PIN and POI | Additional Guidance |
| DTR B12 | Clarified that applies to both intentional and unintentional key loss. | Additional Guidance |
| DTR B13 | Clarified that it also applies to derived and negotiated keys, and not just calculated (variants) keys | Additional Guidance |
| DTR B15 | Updated to reflect new language in ISO 9564 | Additional Guidance |
| DTR B16 | Added additional guidance for protection of audit log data | Additional Guidance |
| DTR B17 | Added detailed guidance to address third party applications that are added to HSMs via use of vendor supplied software development toolkits | Additional Guidance |
| DTR B18 | Further guidance that firmware and software running on the device shall be designed to run with minimal privilege. | Additional Guidance |
| DTR B19 | Added guidance that HSM uniqueness identifiers may include acceptable cryptographic methods | Additional Guidance |
| DTR C1 | Updated to reflect new language in ISO 9564 | Additional Guidance |
| DTR C1 | Added additional information to be included in the HSM security policy, including all configurations setting necessary to meet the security requirements and the device decommissioning procedures. | Requirement change |
| DTR Appendix A | Attack calculation formulas updated to be consistent with POI | Additional Guidance |
| DTR Appendix C | Created new appendix to centrally locate stipulations for allowed cryptographic algorithms and minimum key sizes. | Additional Guidance |

| Document and Requirements Reference[1] | Change | Type[2] |
|---|---|---|
| VQ | Modifications and additions to reflect changes above | Additional Guidance |

| **Document and Requirements Reference[1]** | **Definition** |
|---|---|
| SR | PCI PTS HSM Security Requirements |
| DTR | PCI PTS HSM Derived Test Requirements |
| VQ | PCI PTS HSM Evaluation Vendor Questionnaire |
| **Type[2]** | **Definition** |
| Additional guidance | Provides clarification on intent of the requirement and additional guidance or information on the criteria applied. |
| Requirement change | To reflect the addition modification,  deletion or restructuring of requirements |
| *Note:  The changes above do not include those that are corrections of grammar or typographical errors or other rephrasing of existing statements.* | |