Below, please find at least the 'major' part of what's missing in Craig's original list – so see this as an addition to the original list.

- From **PCI PTS POI** – the 'main' document from PCI specifying EPP security requirements (physical as well as logical):

Reference	***Publication Title***
X9.119-1	*Retail Financial Services – Requirements for Protection of Sensitive Payment Card Data Part 1: Using Encryption Methods*
X9.119-2	*Retail Financial Services – Requirements for Protection of Sensitive Payment Card Data – Part 2: Using Tokenization Methods*
ANSI X9.24	*Banking – Retail Financial Services Symmetric Key Management*
ANSI TR-31	*Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms*
ANSI TR-34	*Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport*
EMV 4.3	*Integrated Circuit Card Specification for Payment Systems – Book 2: Security and Key Management, Version 4.3, November 2011*
ISO 7816	*Identification Cards – Integrated Circuit Cards*
ISO 9564	*Personal Identification Number (PIN) Management and Security*
ISO 9797-1	*Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*
ISO 11568	*Banking – Key Management (Retail)*
ISO 13491	*Banking – Secure Cryptographic Devices (Retail)*
ISO 16609	*Financial services -- Requirements for message authentication using symmetric techniques*
ISO/IEC 18033-1	*Information Technology – Security techniques – Encryption algorithms – Part 1: General*
ISO/IEC 18033-3	*Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers*
ISO/IEC 18033-5	*Information Technology – Security techniques – Encryption algorithms – Part 5: Identity Based Ciphers*
ISO TR 19038	*Guidelines on Triple DES Modes of Operation*.
NIST SP 800-21	*Guideline for Implementing Cryptography in the Federal Government*
NIST SP 800-22	*A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*

- From **PCI PTS HSM** – the document from PCI specifying the HSM security requirements (physical as well as logical):

Reference	***Publication Title***
ANSI X9.24	*Banking—Retail Financial Services Symmetric Key Management*
ANSI X9.44	*Key Establishment Using Integer Factorization Cryptography*
ANSI X9.62	*Public Key Cryptography for the Financial Services ECDSA*
ANSI 9.63	*Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*
ANSI TR-31	*Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms*
FIPS	*FIPS PUB 140-2: Security Requirements for Cryptographic Modules*
ISO 9564	*Personal Identification Number (PIN) Management and Security*
ISO 9797-1	*Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*
ISO 11568	*Banking—Key Management (Retail)*
ISO 11770-2	*Information Technology – Security Techniques – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques*
ISO 11770-3	*Information Technology – Security Techniques – Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA and Diffie-Hellman)*
ISO 13491	*Banking—Secure Cryptographic Devices (Retail)*
ISO 16609	*Financial services — Requirements for message authentication using symmetric techniques*
ISO/IEC 18033-1	*Information Technology – Security techniques – Encryption algorithms – Part 1: General*
ISO/IEC 18033-3	*Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers*
ISO/IEC 18033-5	*Information Technology – Security techniques – Encryption algorithms – Part 5: Identity Based Ciphers*
ISO TR19038	*Guidelines on Triple DES Modes of Operation*
NIST SP 800-22	*A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*
NIST SP 800-38B	*Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*
NIST SP 800-57	*Recommendations for Key Management – Part 1:General*
NIST SP 800-67	*Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*

- From **PCI PIN** – the overall document from PCI, stating requirements to *all* devices and systems involved in PIN handling (incl. EPP's, HSM's, provisioning services etc.):

Source	***Publication***

ANSI	*ANSI X3.92: Data Encryption Algorithm*
	ANSI X9.24 (Part 1): Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
	ANSI X9.24 (Part 2): Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
	ANSI X9.24 (Part 3): Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction
	ANSI X9.42: Public-key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
	ANSI X9.44: Key Establishment Using Integer Factorization Cryptography
	ANSI X9.62: Public Key Cryptography for the Financial Services ECDSA
	ANSI X9.63: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography
	ANSI TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
	ANSI TR-34: Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport
EMV	*Integrated Circuit Card Specification for Payment Systems, version 4.2 (June 2008)—Book 2: Security and Key Management*
FIPS	*FIPS PUB 140–2: Security Requirements for Cryptographic Modules*
	FIPS PUB 186-4: Digital Signature Standard (DSS)
ISO	*ISO 9564: Financial services - Personal Identification Number Management and Security*
	ISO 11568: Banking – Key Management (Retail)
	ISO 11770–2: Information Technology – Security Techniques – Key Management, Part 2: Mechanisms Using Symmetric Key Management Techniques
	ISO 11770–3: Information Technology – Security Techniques – Key Management, Part 3: Mechanisms Using Asymmetric Techniques (RSA and Diffie-Hellman)
	ISO 13491: Banking – Secure Cryptographic Devices (Retail)
	ISO TR 14742: Financial services - Recommendations on cryptographic algorithms and their use
	ISO 16609: Banking – Requirements for message authentication using symmetric techniques
	ISO 18031: Information technology -- Security techniques -- Random bit generation
	ISO/IEC 18033-3: Information Technology – Security techniques – Encryption algorithms – Part 3: Block Ciphers
	ISO TR 19038: Guidelines on Triple DEA Modes of Operation
	ISO 20038: Banking and related financial services -- Key wrap using AES
NIST	*NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*
	NIST Special Publication 800-57: Recommendation for Key Management
	NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management
	NIST Special Publication 800-131: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
PCI	*Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements*
	Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements
	Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Security Requirements
	Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM) Derived Test Requirements

As you may note, I didn't remove redundant info across the tables above – and I reckon that some of the entries point to slightly different versions, but as a note in HSM states:

> *These documents are routinely updated and reaffirmed. The current versions should be referenced when using these requirements.*