Arbeitsgruppe 8.51 „Metrologische Software“ Stand: 03.07.2018

Merkblatt: Spezielle Anforderungen an Kryptografiemodule

Ergänzung zu den messtechnischen und sicherheitstechnischen Anforderungen bei Konformitätsbewertungen nach Modul B

Als Kryptografiemodule werden hier alle Komponenten, Baugruppen und Softwaremodule mit kryptografischen Funktionen bezeichnet, die Bestandteil von Messgeräten sind.

Bei Konformitätsbewertungen nach Modul B gelten für Kryptografiemodule (wie für alle anderen Bestandteile von Messgeräten) die messtechnischen bzw. funktionalen Anforderungen der jeweiligen Messgeräteart sowie die sicherheits- bzw. softwaretechnischen Anforderungen des WELMEC Softwareleitfadens 7.2.

Darüber hinaus gibt es messtechnische und sicherheitstechnische Anforderungen, die sich aus der spezifischen Aufgabe des Kryptografiemoduls im Messgerät ergeben.

Die vorliegende Liste von Anforderungen umfasst diese spezifischen messtechnischen und sicherheitstechnischen Anforderungen. Sie sind aus dem Mess- und Eichgesetz abgeleitet.

Es wird davon ausgegangen, dass je nach Einsatzgebiet ein mittleres oder ein hohes Schutzniveau gewährleistet werden muss. Dies entspricht im WELMEC Softwareleitfaden den Risikoklassen B-C (mittel) bzw. D-F (hoch).

Anforderungen

K1 Dokumentation

Schutzniveau mittel	Schutzniveau hoch
Anforderung K1: **Das Kryptografiemodul muss dokumentiert sein.** Details: 1. Die Dokumentation muss die Bauart und den Hersteller des Kryptografiemoduls nennen. 2. Die Dokumentation muss die für den Gebrauch wesentlichen Eigenschaften des Kryptografiemoduls beschreiben.	

Erläuterungen:

1. Sofern das Kryptografiemodul eine eigenständige (Hardware-)Komponente ist, wird diese Anforderung durch die WELMEC-Anforderung P1/U1 geprüft.
2. Zu den wesentlichen Eigenschaften gehören: die Funktionen, die implementierten Algorithmen mit Schlüssellängen und anderen Parametern, die implementierten kryptografischen Standards und Regeln, die Bestandteile (Karten, Libraries, Betriebssystem, …) sowie Zugangsregelungen.
3. Von den Eigenschaften des Kryptografiemoduls müssen nur die beschrieben sein, die im Messgerät verwendet werden oder von außerhalb des Messgeräts aufgerufen werden können.

K2 Identifikation

Schutzniveau mittel	Schutzniveau hoch
Anforderung K2: **Die Software des Kryptografiemoduls muss sich identifizieren lassen.** Details: 1. Die Software des Kryptografiemoduls muss eine Identifikation aufweisen, die bei Bedarf auf einfache Weise kontrollierbar ist. 2. Die Identifikation darf nicht änderbar sein. 3. Die Identifikation muss eindeutig sein.	
Erläuterungen: 1. Sofern das Kryptografiemodul eine eigenständige (Hardware-)Komponente ist, wird diese Anforderung durch die WELMEC-Anforderung P2/U2 geprüft. 2. Die Identifikation der Software des Kryptografiemoduls dient der Feststellung der Konformität von Seriengerät und Baumuster. Die Identifikation der Software des Kryptografiemoduls ist Bestandteil der Identifikation des Messgeräts, dessen Bestandteil sie ist. 3. Die Art der Identifikation ist nicht vorgeschrieben.	
-	4. Die Identifikation sollte geeignet sein, die Anwendbarkeit von eingereichten Sicherheitszertifikaten zu prüfen.

K3 Funktionale Anforderungen

K31 Vorhandensein aller benötigten Funktionen

Schutzniveau mittel	Schutzniveau hoch
Anforderung K311: **Das Kryptografiemodul muss die Funktion Schlüsselgenerierung oder -laden aufweisen.**	

Details:

1. Die Messgeräte besitzen individuelle oder einheitliche Schlüssel / Schlüsselpaare. 2. Für die Signierung sind symmetrische und asymmetrische Verschlüsselungen zulässig. 3. Bei Bedarf kann ein neuer Schlüssel / ein neues Schlüsselpaar im Kryptografiemodul generiert oder in das Kryptografiemodul geladen werden. Die Dokumentation enthält entsprechende Anweisungen.	1. Die Messgeräte besitzen individuelle Schlüsselpaare. 2. Für die Signierung sind nur asymmetrische Verschlüsselungen zulässig. 3. Während der Inbetriebnahme sowie bei Bedarf kann ein neues Schlüsselpaar im Kryptografiemodul generiert werden. Die Dokumentation enthält entsprechende Anweisungen.

4. Die Erneuerung des Schlüssels / Schlüsselpaars ist nur nach äußerlich sichtbarer Verletzung einer Schutzmaßnahme (Siegel) möglich.
5. Weist das Kryptografiemodul aus Sicherheitsgründen die Funktion nicht auf, muss dies dokumentiert sein.
6. Bei asymmetrischer Verschlüsselung kann der öffentliche Schlüssel bei Bedarf ausgegeben werden. Die Dokumentation enthält entsprechende Anweisungen. Ist keine Ausgabe möglich, muss dies dokumentiert sein.

-	7. Ein für das Kryptografiemodul gültiges Sicherheitszertifikat weist nach, dass die Funktion Schlüsselgenerierung vorhanden und zertifiziert ist.

Erläuterungen:

1. Bedarf an einer Erneuerung des Schlüssel / Schlüsselpaars kann nach der Kompromittierung des Messgeräts bestehen.
2. Die Ausgabe des öffentlichen Schlüssels kann über Anzeigen, Ausdrucke, den Export von Schlüssel-Zertifikaten oder den Export von signierten Daten, die den Schlüssel enthalten, erfolgen.

3. Falls die Signaturen auch für den Herkunftsnachweis der signierten Daten verwendet werden sollen, müssen individuelle Schlüssel / Schlüsselpaare verwendet werden.	3. Eine Prüfung, ob mit den dokumentierten Anweisungen tatsächlich eine Schlüsselgenerierung veranlasst wird, erfolgt bei Anforderung K34.

Schutzniveau mittel	Schutzniveau hoch

Anforderung K312:
Das Kryptografiemodul muss die Funktion Signaturerstellung und bei Bedarf die Funktion Signaturprüfung aufweisen.

Details:

1. Das Kryptografiemodul erzeugt ein Sicherheitsmerkmal, das an Messdaten angefügt wird und das im Messgerät oder durch externe Programme geprüft werden kann.
2. Die Dokumentation beschreibt das Sicherheitsmerkmal als Signatur.

3. Die Anzeige von Messdaten mit gültiger Signatur unterscheidet sich klar von der Anzeige von Messdaten mit ungültiger Signatur. Die Dokumentation benennt die Unterschiede.	
-	4. Ein für das Kryptografiemodul gültiges Sicherheitszertifikat weist nach, dass die Funktionen Signaturerzeugung und ggf. Signaturprüfung vorhanden und zertifiziert sind.
Erläuterungen: 1. Die Funktion Signaturprüfung ist nur erforderlich, wenn das Messgerät Signaturen selbst überprüfen können muss. Häufig erfolgt die Überprüfung der Signaturen nicht durch das Messgerät, sondern durch ein externes Programm. 2. Bei Messdaten mit ungültiger Signatur wird vorzugsweise statt der Messdaten eine Fehlermeldung ausgegeben.	
-	3. Eine Prüfung, ob mit den dokumentierten Funktionen tatsächlich eine Signatur erzeugt bzw. geprüft wird, erfolgt bei Anforderung K34.

K32 Kryptografische Stärke der Funktionen

Schutzniveau mittel	Schutzniveau hoch
Anforderung K32: **Die verwendeten kryptografischen Funktionen des Kryptografiemoduls müssen kryptografisch stark sein.** Details:	
1. Die verwendeten Algorithmen, Schlüssellängen und sonstigen Parameter müssen den Vorgaben des Regelermittlungsausschusses nach §46 des Mess- und Eichgesetzes entsprechen oder allgemein als sicher anerkannt sein.	1. Die im Sicherheitszertifikat genannten Algorithmen, Schlüssellängen und sonstigen Parameter müssen den jeweils aktuellen Vorgaben der Institute, die für die Datensicherheit verantwortlich sind (BSI, BNetzA, NIST, …), entsprechen.
Erläuterungen: 1. Bei unbekannten oder neu entwickelten Algorithmen oder unüblichen Schlüssellängen oder Parametern fehlt die Bewertung der Schwachstellen durch die Fachöffentlichkeit.	

K33 Korrekte Implementierung der kryptografischen Funktionen

<table>
<tr><th>Schutzniveau mittel</th><th>Schutzniveau hoch</th></tr>
<tr><td colspan="2">Anforderung K33:
Die verwendeten kryptografischen Funktionen müssen korrekt implementiert sein.

Details:</td></tr>
<tr><td>1. Die korrekte Implementierung wird durch Tests beim Hersteller nachgewiesen.

2. Die Dokumentation enthält eine Beschreibung der durchgeführten Tests, der Langzahlbibliothek, des Zufallszahlengenerators und ggf. der Primzahltests.</td><td>1. Ein für das Kryptografiemodul gültiges Sicherheitszertifikat weist die korrekte Implementierung nach.</td></tr>
<tr><td colspan="2">Erläuterungen:</td></tr>
<tr><td>1. Die Dokumentation muss mindestens folgende Tests umfassen:
• Tests, die nachweisen, dass bei mehrmaligem Aufruf der Funktion Schlüsselgenerierung jedes Mal neue, unterschiedliche Schlüssel bzw. öffentliche Schlüssel entstehen,
• positive und negative Tests, die nachweisen, dass Signaturerstellung und -prüfung zueinander passen,
• Einzeltests der Hashwertberechnung, der Verschlüsselung und der Entschlüsselung und Vergleich der Ergebnisse mit veröffentlichten Sollergebnissen,
2. Die Testbeschreibungen enthalten: Testziel, getestete Software/Hardware, Eingaben, Sollausgaben, Istausgaben, Datum.
3. Die Dokumentation muss mindestens folgende Beschreibungen umfassen:
• eine Beschreibung der verwendeten Langzahlbibliothek, insbesondere ihrer Qualität bzw. Betriebsbewährtheit,
• eine Beschreibung des verwendeten Zufallszahlengenerators, insbesondere seiner statistischen Qualität,
• bei asymmetrischen Verfahren eine Beschreibung der angewendeten Primzahltests.</td><td>1. Bei Zertifikaten nach den Common Criteria (CC-Zertifikaten) ist der Nachweis über die Vertrauenswürdigkeitsstufe EAL 4 oder höher möglich.
2. Bei Zertifikaten nach den Information Technology Security Evaluation Criteria (ITSEC-Zertifikaten) ist der Nachweis über die Evaluierungsstufe E3 (hoch) oder höher möglich.</td></tr>
</table>

K34 Korrekte Implementierung der Schnittstellen zu den kryptografischen Funktionen

Schutzniveau mittel	Schutzniveau hoch
Anforderung K34: **Die Schnittstellen zwischen Kryptografiemodul und Messgeräteprogramm müssen korrekt implementiert sein.** Details:	
1. Die korrekte Implementierung wird durch Tests beim Hersteller nachgewiesen. 2. Die Dokumentation enthält eine Beschreibung der durchgeführten Tests.	1. Die Dokumentation enthält die Schnittstellenbeschreibung des Kryptografiemoduls sowie den Code der Schnittstellen.
Erläuterungen:	
1. Die für Anforderung K33 durchgeführten Tests können so gestaltet sein, dass die Schnittstellen mit erfasst sind. Ist dies nicht der Fall, müssen die Tests mit erweitertem Testgegenstand wiederholt werden.	1. Die Schnittstellen werden einer Codeinspektion unterzogen. Die Aufrufe der kryptografischen Funktionen müssen hinsichtlich Parameterliste, Rückkehrwerten, Vor-/Nachbereitungen und Fehlerauswertung der Schnittstellenbeschreibung des Kryptografiemoduls entsprechen.

K4 Sicherheitsanforderungen

K41 Schutz des Kryptografiemoduls vor Defekten und Manipulation

Schutzniveau mittel	Schutzniveau hoch
Anforderung K41: **Das Kryptografiemodul muss vor Defekten und Manipulation geschützt sein.** Details:	
1. Das Kryptografiemodul muss Schutzmaßnahmen aufweisen, die Funktionen, Parameter und Messdaten vor Defekten und Manipulation schützen oder diese nachweisen. Die Dokumentation muss die Schutzmaßnahmen beschreiben.	1. Ein für das Kryptografiemodul gültiges Sicherheitszertifikat weist den Schutz vor Defekten und Manipulation nach.
Erläuterungen:	
1. Der Schutz muss sich auf den Code und die relevanten Parameter (Schlüssel, Parameter des Hashverfahrens, Parameter von Ver-	1. Der Schutz muss sich auf den Code, die relevanten Parameter (Schlüssel, Parameter des Hashverfahrens, Parameter von Ver- und Entschlüsselung, Anmeldedaten, ...) und

und Entschlüsselung, Anmeldedaten, ...) beziehen. 2. Sofern das Kryptografiemodul eine eigenständige (Hardware-)Komponente ist, wird diese Anforderung durch die WELMEC-Anforderungen P3-P7/U3-U7, L und T geprüft.	falls erforderlich die relevanten temporären Daten (zu hashende Daten, Hashwerte, berechnete Signaturen) beziehen. 2. Bei CC-Zertifikaten erfolgt der Nachweis über die Sicherheitsziele des zugehörigen Security Targets (Integritätsschutz für die o.g. Informationen). 3. Bei ITSEC-Zertifikaten erfolgt der Nachweis über die zertifizierte Mindeststärke der Algorithmen "hoch" (E3 hoch).

K42 Vertraulichkeit des Schlüssels und anderer Informationen

Schutzniveau mittel	Schutzniveau hoch
Anforderung K42: **Die Vertraulichkeit des Schlüssels bzw. des privaten Schlüssels und vergleichbarer Parameter muss gesichert sein.** Details:	
1. Das Kryptografiemodul muss Schutzmaßnahmen aufweisen, die die Vertraulichkeit des Schlüssels bzw. des privaten Schlüssels und vergleichbarer Parameter sichern. Die Dokumentation muss die Schutzmaßnahmen beschreiben. 2. Bei symmetrischen Schlüsseln muss die Vertraulichkeit des Schlüssels auch an Aufbewahrungs- und Verwendungsorten außerhalb des Kryptografiemoduls gewährleistet sein.	1. Ein für das Kryptografiemodul gültiges Sicherheitszertifikat weist die Vertraulichkeit für private Schlüssel und vergleichbare Parameter nach.
Erläuterungen: 1. Der Schutz muss sich auf den Schlüssel bzw. den privaten Schlüssel sowie ggf. auf Zugangs- oder Anmeldedaten beziehen.	
2. Der Schutz des Schlüssels außerhalb des Kryptografiemoduls muss ggf. durch zusätzliche technische oder organisatorische Schutzmaßnahmen sichergestellt werden.	2. Bei CC-Zertifikaten erfolgt der Nachweis über die Sicherheitsziele des zugehörigen Security Targets (Vertraulichkeit für die o.g. Informationen).