Parasol Island

Arbeitsanweisung zur Authentifizierung und Kryptographie

Dateiname:	03_05_PSL_ISMS_Authentifizierung_und_Kryptographie_v01.00_cW
Dokumentenebene:	03_Arbeitsanweisungen
Erstellt von:	Philip Hansen
Version:	01.00
Status:	Freigegeben
Letzte Aktualisierung am/von:	07.11.2017 | Cedric Wolffs
Exportiert am:	07.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	07.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	10.1

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	20.09.2017	Justus Heinser	Anpassungen
00.03	19.10.17	Cedric Wolffs	Information Passwortlänge angepasst
01.00	07.11.17	Cedric Wolffs	Finalisierung

Parasol Island

Inhaltsverzeichnis

1. Zielsetzung

Dieser Leitfaden soll die vorangegangene Allgemeine Sicherheitsrichtlinie erweitern und konkretisieren.
Ziel der Arbeitsanweisung ist es, Regeln zur Nutzung von Kryptographie vorzugeben, und zu definieren, wann Kryptographie genutzt werden muss und welche Methoden sich dazu eignen.

2. Geltungsbereich

Diese Arbeitsanweisung gilt verbindlich für alle Mitarbeiter ohne Ausnahme. Verstöße gegen die Inhalte der Richtlinie können zu arbeitsrechtlichen Konsequenzen führen.
Die Regelungen dieser Richtlinie gelten uneingeschränkt. Sie dürfen nicht umgangen werden. Ausnahmen von der Richtlinie sind nicht zulässig, es sei denn, sie sind in der Richtlinie ausdrücklich aufgeführt.
Diese Ausführung ersetzt weder die Allgemeine Sicherheitsrichtlinie *(02_01)* noch andere Regelungen, sondern dient ausschließlich als ergänzende Information.
Mit Veröffentlichung einer neuen Version werden vorangegangene Versionen, die bis dahin veröffentlicht wurden, ungültig.

3. Verschlüsselungsarten

Um die Integrität und Vertraulichkeit der Informationen sicherzustellen, ist es notwendig, dass ausschließlich Verfahren eingesetzt werden, welche nach derzeitigem Stand als sicher gelten. Kryptographische Verfahren lassen sich in drei Arten einteilen:

- Symmetrische Verschlüsselungsverfahren
- Asymmetrische Verschlüsselungsverfahren
- Hash-Verfahren

Zugelassene symmetrische Verschlüsselungstechnik

Algorithmus	Minimale Schlüssellänge(Bit)	Empfohlene Schlüssellänge (Bit)
AES	128	256
Triple-DES	112	112
RC4*	128	256
RC5	128	256
RC6	128	256
Blowfish	128	256
Twofish	128	256
CAST	128	256
Camelia	128	256

**Die Verwendung von RC4 ist nur für SSL/TLS auf Windows erlaubt, bis ein sicherer Algorithmus zur Verfügung steht. Jegliche andere Nutzung ist nicht erlaubt.*

Zugelassene asymmetrische Verschlüsselungsverfahren

Algorithmus	Minimale Schlüssellänge(Bit)	Empfohlene Schlüssellänge (Bit)
RSA	1024 / 2048 wenn möglich	4096
DSA	1024 / 2048 wenn möglich	4096

Zugelassene Hashfunktionen

- SHA-224
- SHA-256
- SHA-384
- SHA-512

Alternativ, falls die oben Genannten technisch nicht möglich sind

- SHA-160
- RIPEMD-160
- MD5
- Whirlpool-512

4. Mobile Geräte

Falls vertrauliche oder streng vertrauliche Daten auf mobilen Geräten vorliegen, sind diese nach aktuellstem Stand sicher zu verschlüsseln.
Es empfiehlt sich der Einfachheit halber eine generelle Verschlüsselung, sofern diese möglich ist.

5. Authentifikationsmethoden

Authentifikation beschreibt die Möglichkeit einer eindeutigen Identifikation der Person. Grundsätzlich unterscheidet man schwache Authentifikation und starke Authentifikation

Schwache Authentifikation

Schwache Authentifikation nutzt nur eines der folgenden Merkmale zur Identitätsprüfung:

- Wissen (z.B. Passwort, Pin)
- Besitz (z.B. Software Zertifikate, Schlüssel, Yubikey)
- Eigenschaften (z.B. Fingerabdruck)

Starke Authentifikation

Starke Authentifikation nutzt hingegen 2 der oben genannten Merkmale. Der Einsatz biometrischer Verfahren ist prinzipiell nicht erlaubt.
Das Merkmal „Besitz“ ist über die nachfolgenden Eigenschaften definiert:

- Befindet sich im Besitz der zu authentifizierenden Person.
- Steht dieser exklusiv zur Verfügung.
- Eine Vervielfältigung ist nicht ohne Weiteres möglich (Ausnahmen können z.B. in der ausstellenden / ausgebenden Stelle liegen).

Das Merkmal „Besitz“ muss eine Reihe von speziellen Anforderungen erfüllen

- Das Merkmal „Besitz“ darf nicht auf der authentifizierenden Instanz installiert / verortet sein.
- Im Falle eines Tokens darf dieser ausschließlich zu Authentifizierungszwecken verwendet werden. Eine Speicherung weiterer Daten auf diesem Device ist nicht zulässig.
- Es sind ausschließlich zertifizierte Devices zu verwenden (Zertifizierung nach FIPS 140-2 oder Common Criteria EAL 4+).
- Das Merkmal „Besitz“ darf nicht beliebig vervielfältigbar sein.
- Vervielfältigungen dürfen lediglich im Recovery- oder Archivierungsprozess der herausgebenden Stelle und nur unter Einwilligung des jeweiligen „Besitzers“ möglich sein.

Als „Besitz“ Merkmal wird bei der Parasol Island GmbH ein Yubikey benutzt. Dieser erfüllt bei sachgerechter Nutzung alle geforderten Kriterien. Er wird vom Administrator zusammen mit einem Passwort an berechtigte Personen ausgegeben.

6. Anforderungen in Abhängigkeit zur Datenklassifikation

Einstufung / Klassifikation	Anforderung Verschlüsselung	Anforderung Authentifizierung
Öffentlich	keine	keine
Intern	keine	schwache Authentifikation
Vertraulich	Transportverschlüsselung, wenn möglich Ablageverschlüsselung	starke Authentifikation *
Streng Vertraulich	Transportverschlüsselung und Ablageverschlüsselung	starke Authentifikation

** Sofern eine starke Authentifikation technisch nicht möglich ist, ist der Einsatz einer schwachen Authentifikation mit einer weiteren Absicherung wie eine zusätzlich authentisierte Ablageverschlüsselung gestattet. Hierbei ist zu beachten, dass für beide Verfahren unterschiedliche Authentifizierungsinformationen und -instanzen (z.B. unterschiedliche Passwörter in verschiedenen Systemen) zu verwenden sind.*

Administrative Tätigkeiten sind, soweit technisch möglich, stark zu authentifizieren. Sofern dies technisch nicht möglich ist, sind die folgenden Anforderungen einzuhalten:

Für administrative Benutzerkennungen, die personenbezogen zur Verwaltung von IT-Systemen auf der Basis von umfassenden Zugriffsrechten genutzt werden, ist für Passwörter eine mindestens 16-stellige Kombination aus mindestens 3 der folgenden 4 Kriterien zu verwenden:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen