

Spezifikation für das Zertifizierungsprogramm:

Test-Cases „TR-RESISCAN ready Software“ Konformitätsprüfung, Version 1.4

(Stand 10.12.2020)

KRITERIUM	ANFORDERUNGSTYP
Handbuch	
Handbuch existiert	MUSS
Bedienungsanleitung (Mindestvoraussetzungen erfüllt)	MUSS
Sicherheitshinweise für störungsfreien Betrieb	MUSS
Installationsanleitung	MUSS
Regelungen für sichere Installation von SW-Updates	MUSS
Fehlerbeseitigung	MUSS
Empfehlungen für einen sicheren Betrieb (Administrationsanleitung) -Maßnahmen zum Zutrittsschutz (z.B. abschließbarer Raum) -Maßnahmen zum Zugriffsschutz (z.B. PIN) -Konfigurationsempfehlung	SOLL
Sicherheitskonzept	
Sicherheitskonzept existiert	SOLL
<i>Inhalt:</i>	
Administration	SOLL
Beschreibung sichere Konfiguration (Empfehlungen)	SOLL
Sicherheitsmaßnahmen (Empfehlungen)	SOLL
Maßnahmenkatalog	SOLL
Checkliste f. sicheren Betrieb	SOLL
Einsatz von Kryptografie (Integritätsschutz)	SOLL
Rollenbeschreibung (User, Poweruser, Admin)	SOLL
Schnittstellenbeschreibung	
Schnittstellenbeschreibung existiert	MUSS
<i>Inhalt:</i>	
Schnittstelle z. Client-PC	SOLL
Schnittstelle z. externen Datenspeicher	SOLL
Schnittstelle z. einer Fachanwendung	SOLL
Schnittstelle z. DMS (Dokumentenmanagementsystem)	SOLL
Schnittstelle z. Archiv	SOLL
Schnittstellen z. Integritätssicherung / geeignete Verschlüsselung	SOLL
Externe Wartungsschnittstelle (Beschreibung der Absicherung)	SOLL
Sicherung der Schnittstellen (kann auch Bestandteil des Sicherheitskonzepts sein)	SOLL
Verschlüsselte Kommunikation möglich (Integrationsschutz)	SOLL
Besondere Administrationsschnittstelle	SOLL

Netzwerkfähigkeit (Netzwerkzugriff)	
<i>Netzwerkfähigkeit vorhanden dann:</i>	
Sicherer Zugang/Login (mind. Username + Password)	MUSS
Kryptographische Sicherung der Kommunikation bei Schutzbedarf „sehr hoch“	SOLL
Zugriff auf die Administrationsschnittstelle soll durch eine geeignete Netzwerk-Konfiguration auf die notwendigen Systeme eingeschränkt werden	SOLL
Protokollierung	
Protokollierung möglich	SOLL
Protokollierung Speicherdauer konfigurierbar (Datenschutz)	SOLL
<i>Protokollierte Ereignisse:</i>	MUSS
Anmeldung (Benutzername / Anmeldezeit	MUSS
Fehlerprotokollierung	MUSS
Konfigurationsänderung	MUSS
Speichern der Protokolle im internen Speicher	MUSS
Änderung von Passwörtern	SOLL
Anmeldung (erfolgreich/nicht erfolgreich)	SOLL
Konfiguration	
Integritätsschutz durch geeignetes Authentisierungsverfahren (ab Schutzbedarf „hoch“) und Zugriffswege	SOLL
Sicherung der alten Konfiguration vor Umstellung	SOLL
Protokollierung der Konfigurationsänderung	SOLL
Automatische Sicherung der Konfiguration (z.B. im tägl. Backup)	SOLL
Einsatz OCR-Verfahren (wenn Bestandteil der Lösung)	
OCR-Zonen werden unterstützt (Erstellen u. Löschen möglich)	SOLL
Stapel- und Dokumententrennungen nach OCR-Zone möglich	SOLL
Genauigkeitsanforderungen sind konfigurierbar (Geschwindigkeit)	SOLL
OCR-Sprache konfigurierbar	SOLL
OCR-(Zone) Test möglich	SOLL
Farb- oder Graustufenbilder als OCR-Quelle möglich	SOLL
Transfervermerk	
Für jedes Scanprodukt soll ein Transfervermerk erstellt werden.	SOLL
<i>Der Transfervermerk dokumentiert folgende Aspekte:</i>	SOLL
Ersteller des Scanprodukts	SOLL
Technisches und organisatorisches Umfeld des Erfassungsvorgangs	SOLL
Etwaige Auffälligkeiten während des Scanprozesses	SOLL
Zeitpunkt der Erfassung	SOLL
Ergebnis der Qualitätssicherung	SOLL
Tatsache, dass es sich um ein Scanprodukt handelt, das bildlich und inhaltlich mit dem Papierdokument übereinstimmt	SOLL
Der Transfervermerk muss mit dem Scanprodukt logisch verknüpft oder in das Scanprodukt integriert werden.	MUSS

Der Transfervermerk muss entsprechend dem Schutzbedarf der verarbeiteten Dokumente geschützt werden. (Integritätsschutz ab Schutzbedarf „hoch“)	MUSS
Für die Dokumentation des technischen und organisatorischen Umfelds kann der Transfervermerk auf die zu diesem Zeitpunkt gültige Verfahrensanweisung verweisen.	KANN
Für die Integritätssicherung des Scanproduktes bzw. des Transfervermerks sollen qualifizierte elektronische Signaturen oder Siegel und für die Integritätssicherung des dokumentierten Zeitpunktes des Scanvorgangs qualifizierte Zeitstempel eingesetzt werden, wenn	SOLL
Datenobjekte mit einem Schutzbedarf von ‚sehr hoch‘ bzgl. der Integrität verarbeitet werden.	SOLL
für Datenobjekte die Verkehrsfähigkeit gefordert ist.	SOLL
Die im Rahmen des Scanprozesses entstandenen Datenobjekte (Scanprodukt, Transfervermerk, Index- und Metadaten, Protokolldaten) voraussichtlich als Beweismittel genutzt werden.	SOLL
Einsatz qualifizierter elektronischer Signaturen und Zeitstempel	
Für die Integritätssicherung des Scanproduktes bzw. des Transfervermerks sollen qualifizierte elektronische Signaturen oder Siegel und für die Integritätssicherung des dokumentierten Zeitpunktes des Scanvorgangs qualifizierte Zeitstempel eingesetzt werden, wenn	
Datenobjekte mit einem Schutzbedarf von ‚sehr hoch‘ bzgl. der Integrität verarbeitet werden.	SOLL
für Datenobjekte die Verkehrsfähigkeit gefordert ist.	SOLL
Die im Rahmen des Scanprozesses entstandenen Datenobjekte (Scanprodukt, Transfervermerk, Index- und Metadaten, Protokolldaten) voraussichtlich als Beweismittel genutzt werden.	SOLL
Geeignete Erfassung von Metainformationen	
Index- und Metadaten sollen in geeigneter Weise übergeben werden.	SOLL
Eine zuverlässige Konfiguration der Applikation bzgl. der Erkennung und Gültigkeit der ausgelesenen Werte kann erfolgen	SOLL
Geeignete Scan-Einstellungen	
Die Scan-Einstellungen müssen für die jeweiligen Dokumente (Schutzbedarf) geeignet gewählt werden können.	MUSS
Es sollen geeignete Profile (Datentyp/Schutzbedarf) definiert werden können	SOLL
Qualitätskontrolle	
Zur Erkennung mangelhafter Scanvorgänge muss eine geeignete Qualitätskontrolle erfolgen.	MUSS
Die Ausgestaltung der Qualitätssicherung soll sich am Scan-Durchsatz und dem Schutzbedarf der verarbeiteten Dokumente orientieren (konfigurierbar).	SOLL
Die Größe der Stichprobe soll abhängig vom Schutzbedarf der Dokumente und der Zuverlässigkeit des Scansystems bestimmt (konfiguriert) werden.	SOLL

Bei automatisierten Qualitätskontrollen soll eine manuelle Prüfung der automatisch identifizierten Probleme erfolgen.	SOLL
Vollständigkeitsprüfung	
In einem automatisierten Prozess müssen geeignete Maßnahmen zur Sicherstellung der Vollständigkeit getroffen werden.	MUSS
Unterstützung von Patch- und/oder Barcodes zur Dokumententrennung und Übergabe von Meta-Informationen	KANN
Einsatz kryptografischer Mechanismen zum Integritätsschutz (ggf. wird Zusatz-Software benötigt)	
Bei der Verarbeitung von Dokumenten mit Schutzbedarf von zumindest „hoch“ bezüglich der Integrität sollen geeignete kryptographische Mechanismen in Form von fortgeschrittenen elektronischen Signaturen, fortgeschrittenen elektronischen Siegeln und/oder elektronischen Zeitstempeln zum Einsatz kommen.	SOLL
Sofern keine kryptographischen Mechanismen in Form von fortgeschrittenen elektronischen Signaturen, fortgeschrittenen elektronischen Siegeln und/oder elektronischen Zeitstempeln eingesetzt werden, Andernfalls muss ein schriftlicher Nachweis erbracht werden, dass der für den Integritätsschutz eingesetzte Mechanismus ausreichend widerstandsfähig (siehe Fußnote 35 in A.IS.1) ist.	MUSS
Für den Integritätsschutz des dokumentierten Zeitpunktes des Scan-Vorgangs (als Meta-Datum) sollen (qualifizierte) Zeitstempel (Art. 3 Nr. 34 eIDAS) verwendet werden.	SOLL
Kennzeichnung der Dokumente bzgl. Sensitivität	
Dokumente, die einen Schutzbedarf von „sehr hoch“ bzgl. der Integrität besitzen, sollen als solche gekennzeichnet werden.	SOLL
Die Kennzeichnung soll deutlich sichtbar angebracht werden.	SOLL
Löschen von Zwischenergebnissen	
Bei der Verarbeitung von Dokumenten mit einem Schutzbedarf hinsichtlich der Vertraulichkeit von zumindest „hoch“ müssen die in der Verarbeitung entstehenden Zwischenergebnisse (z. B. rohe Scanprodukte, Daten im Scan-Cache) zuverlässig gelöscht werden.	SOLL
Scan Cache (SW-Zugriff)	
Sicherer Zugriff (z.B. durch Username – Password oder PIN)	MUSS
Sicheres Löschen von Authentisierungsinformationen	MUSS
Sicheres Löschen von Zwischenergebnissen bei der Verarbeitung von Dokumenten mit einem Schutzbedarf hinsichtlich der Vertraulichkeit von mindestens „hoch“	MUSS
Verschlüsselte Datenübertragung zwischen Scanner und Scan-Workstation, Scan-Cache bei Schutzbedarf „sehr hoch“	SOLL

Unterstützung geeigneter Bildkompressionsverfahren	
Unterstützung geeigneter Bildkompressionsverfahren (als grundsätzlich geeignet werden sowohl verlustfreie als auch verlustbehaftete Verfahren angesehen.)	SOLL
Backupfunktion	
Integrierte Backup-Funktion zur Sicherung der Konfiguration	KANN
Schulungsangebote des Herstellers	
Hersteller bietet Schulungen für Anwender, Administratoren und Wartungspersonal des Kunden an	SOLL
Vorbereitete Verträge/Erklärungen	
Es existieren vorbereitete Verträge/Erklärungen (z.B. Muster-Auftragsverarbeitungsvertrag oder Verschwiegenheitserklärung) für den Einsatz von Wartungs-Technikern des Herstellers	KANN