Federal Office
for Information Security

BSI Technical Guideline 03138

Replacement Scanning

Title	RESISCAN – Replacement Scanning
Abbreviation	BSI TR 03138 RESISCAN
Version	1.1
Date	02.03.2017

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: resiscan@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Preliminary remarks

This chapter contains information on the labelling of this Technical Guideline (German: Technische Richtlinie, TR), the body responsible for this subject matter, the version management, the change management and the updating of this Technical Guideline.

1.1 Objective and title

This Technical Guideline aims at increasing the **legal certainty in the field of replacement scanning** and bears the title **"Replacement Scanning (RESISCAN)".**

The term "replacement scanning" refers to the process of the electronic recording of paper documents with the aim of electronic further processing and storage of the resulting electronic copy (scanned product) and the subsequent deletion of the paper-based original. In this respect, the scanning and destruction of paper copies or the replacement of conventional copies by scanned products is not replacement scanning within the meaning of this guideline.

The TR RESISCAN is intended to serve users in the judiciary, administrative, industry and healthcare sectors as an action guideline and aid to decision-making when it comes not only to scanning paper documents, but also to destroying them after the scanned product has been created. This applies particularly to those applications in which there are legally or otherwise justified storage and documentation requirements that entail a special handling of digitalised documents when the original is to be destroyed. Without special legal provisions, the Technical Guideline is only of a recommendatory nature.

Whereas there have been principles for the proper performance of electronic storage in some areas of application, such as the commercially or fiscally relevant environment, in accordance with to the General Tax Code (AO) and Commercial Code (HGB) since 1995, according to which replacement scanning is already carried out, there is a lack of specific implementation requirements for most of the other, but increasingly affected areas (exception: social security law). Moreover, there are also more and more documents that are not covered by this in the areas that have already been affected by varyingly detailed regulations (for example those that should not only be stored according to AO/HGB but also for the preservation of evidence according to civil law) that are also to be replacement scanned in future mainly for economic reasons. To be able to do this on the most secure technical/organisational basis possible, the recommendations in this Technical Guideline were developed. The objective is to compensate, minimize or make visible the reduction of the evidential value which is always associated with a destruction of the original document for the respective user by means of an evidential value of the scanned product, created in a demonstrably proper process, that approximates the original as closely as possible. Finally, the Technical Guideline can be used as reference within the framework of future regulation projects when it specifically comes, for example, to creating additional admissibility facts for replacement scanning in the field of electronic records management in particular.

The Technical Guideline is based on the many years of practical experience in different areas of application in the administrative and industry sectors. It takes into account the processes established there as comprehensively as possible. The added value for all scanning processes in which the scanned product is intended to actually replace the original relates in particular to the systematic description of the threats for the main basic objectives of information security that are relevant in a scanning process flow. They are described specifically in a structure analysis for, among other things, all data objects and communication relations affected. Based on a related careful protection requirements analysis and risk analysis carried out along the various scanning phases, specific security safeguards are described. This enables the user to identify the safeguards required for their specialist application and design "their" scanning process in an adequately secure manner. Already established scanning processes can also benefit from the Technical Guideline by checking them against the requirements of the Technical Guideline, optimizing the already existing correctness of the scanning process further if necessary and finally declaring the respective conformity.

Due to the enormous differences of the specialist requirements of each area of application, the Technical Guideline provides a modular requirements catalogue which includes different practice-oriented security levels. The basic level is primarily about a generally proper scanning process organized with basic security safeguards. In the advanced levels, special requirements for integrity, availability and confidentiality with accordingly adjusted and increased security safeguards are taken account of.

The subject of the Technical Guideline (and thus potential scope of certification) is the process of (replacement) scanning as such from a technical and organisational point of view, but not specific soft- or hardware components for the actual implementation of the scanning. As part of demonstrating proof of conformity by means of a certification of the scanning process, which is possible according to this Technical Guideline, soft- and hardware are therefore not considered explicitly. The long-term storage or archiving following a scanning process as part of a workflow system and/or document management system is not the subject of the Technical Guideline either. Concerning this matter, only the necessary interoperability and compatibility with common archive formats are taken into consideration.

The recommendations formulated in this guideline do not only contain functional safeguards and safeguards with regard to security features, but also equally important organisational recommendations that are particularly relevant to scanning. In no case may a scanning process be performed completely automatically, but it always requires the careful operation by humans who are thus a potential source of error of the scanning process that should not be underestimated.

1.2 Designation

This Technical Guideline is designated as “BSI TR 03138”.

1.3 Body responsible for the subject matter

The Federal Office for Information Security (BSI) is responsible for drafting and maintaining this Technical Guideline.

Address: Federal Office for Information Security (BSI)
P.O.B. 20 03 63
D-53133 Bonn (Germany)
Phone: +49 228 99 9582-0
E-mail: resiscan@bsi.bund.de
Internet: https://www.bsi.bund.de

1.4 Version management

This Technical Guideline consists of this main document and the related normative audit specification for the conformity assessment (Annex P).

Moreover, there are different informative annexes that document the result of the risk analysis carried out in the course of the creation of this document (Annex A), contain legal explanations on how to facilitate the application of the Technical Guideline (Annex R) as well as provide exemplary process instructions (Annex V).

At the moment, the Technical Guideline thus consists of two normative and three informative parts:

Technical Guideline	Version	Status	Notes
TR RESISCAN – main document	1.1	normative	this document
TR RESISCAN – Anlage P [Annex P]: Prüfspezifikation [Audit Specification]	1.2	normative	referenced as [BSI-TR03138-P]
TR RESISCAN – Anlage A [Annex A]: Ergebnis der Risikoanalyse [Result of the Risk Analysis]	1.0	informative	referenced as [BSI-TR03138-A]
TR RESISCAN – Anlage R [Annex R]: Unverbindliche rechtliche Hinweise zur Anwendung der TR-RESISCAN [Non-Binding Legal Information on the Application of TR-RESISCAN]	1.0	informative	referenced as [BSI-TR03138-R]
TR RESISCAN – Anlage V [Annex V]: Exemplarische Verfahrensanweisung [Exemplary Process Instructions]	1.1	informative	referenced as [BSI-TR03138-V]

Table 1: Structure and parts of the TR Resiscan

1.5 Change management / updating

The different parts of the Technical Guideline are subject to a continuous updating process, in which new and/or changed requirements are taken into account. The updates are made in an orderly manner in which adjusted versions of the Technical Guideline are released in a formal act.

Formally authorized versions will be published on the BSI website.

1.6 Publication

The currently valid versions will be offered for download on the BSI's website.

1.7 Conventions

The requirements specified in this Technical Guideline for processes and systems for proper replacement scanning are labelled in an unambiguous manner.

For a better differentiation between normative and informative contents, the following English keywords written in capital letters corresponding to [RFC2119] are used:

- **MUST** means that it is an absolutely valid and normative definition or requirement.
- **MUST NOT** refers to the absolutely valid and normative exclusion of a property.
- **SHOULD** or **RECOMMENDED** describes a strong recommendation. Deviations from these definitions are possible in well-founded, exceptional cases.
- **SHOULD NOT** refers to the recommendation of excluding a property. Deviations are possible in justified cases.
- **CAN** means that the properties are voluntary or optional. These definitions are not of a standardizing or generally applicable recommendatory character.

1.8 Area of application

This Technical Guideline provides users from a wide variety of sectors, such as the judiciary, administrative, industry and healthcare sectors, with an action guideline for an as legally viable designing of the processes and systems for replacement scanning as possible.

By means of a defined conformity assessment, users or providers of scanning services can provide documented proof that their processes and systems for replacement scanning meet the technical and organisational requirements according to the respectively chosen module.

A proven conformation of conformity and a certificate issued by the BSI for this can be used by the requester for tendering processes as a performance criterion.

In addition to a certification, self-certifications[1] of scanning service providers or also users come also into consideration depending on the use case. Overall, the Technical Guideline is thus a practice-oriented action guideline for the correctness of a scanning process without a related obligation for certification.

Finally, the Technical Guideline can be referenced, for example for the compliance with the state of the art in the course of legislative procedures[2], as well as used on the sub-statutory level to specify technical/organisational requirements further.

1 As part of a self-certification which should be based on a completely filled audit specification according to [BSI-TR03138-P], a scanning service provider or user declares that they meet the requirements of this Technical Guideline. Whereas no formal audit is provided for these self-certifications, they can facilitate a certification process which is to be carried out afterwards.

2 See explanations on § 7 EGovG [E-Government Act] in [EGovG-MK].

2 General information and overview

In this chapter, the layout and contents of the Technical Guideline as well as the primary goals and challenges for the legally viable replacement scanning are explained.

2.1 Subject matter and important information

As shown in Figure 1, the “generic scanning process” on which the development[3] of this Technical Guideline is based includes

- document preparation,
- scanning,
- post-processing and finally
- securing the integrity.

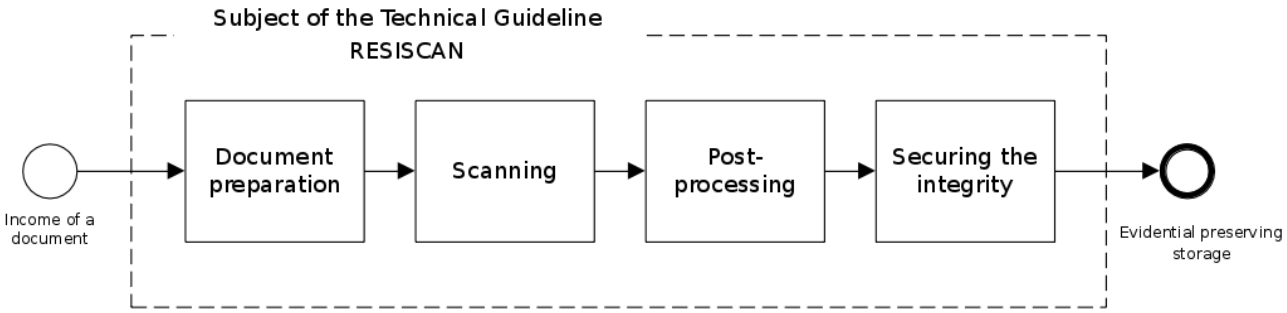

Figure 1: The "generic scanning process"

Process steps beyond securing the integrity (e.g. processing, temporary storage, long-term storage and archiving) are not the subject of this Technical Guideline. The specific requirements of the storage of cryptographically signed data by preserving the evidential value are not the subject of this Technical Guideline either, but are addressed in [BSI-TR03125].

In particular, this Technical Guideline does not govern the admissibility of replacement scanning as such. The admissibility of replacement scanning must be checked by each user in their area of application and responsibility on the basis of the respective relevant legal provisions. Legal considerations concerning this can for example be found in [RFJW08], [JaWi09], [RoNe14b] and [BSI-TR03138-R]. The results of the simulations study “Ersetzendes Scannen” [Replacement Scanning] carried out in 2014 can be found in [RoNe14a].

3 More information on the procedure applied when drawing up this Technical Guideline can be found in [SGHJ12].

3 Procedure to be followed when applying the guideline

This section describes the procedure to be followed when applying the guideline:

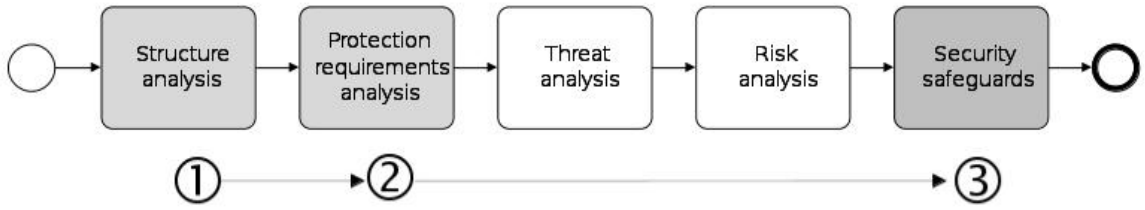

Figure 2: Procedure to be followed when applying the guideline

As shown in Figure 2, the application of the guideline involves three steps:

- Structure analysis
- Protection requirements analysis
- Security safeguards

Whereas a threat and risk analysis[4] was carried out when the Technical Guideline (see [SGHJ12]) was drawn up, users of the guideline can skip these steps. It is instead sufficient to implement the security safeguards from the modular safeguard catalogue that correspond to the defined protection requirements.

3.1 Structure analysis

In the first step, a user of the Technical Guideline must perform a structure analysis for their scanning system, identify the IT systems, networks, applications and data objects relevant to their scanning process and draw up an adjusted network plan[5].

3.2 Protection requirements analysis

In the next step, the user of the Technical Guideline must prepare a protection requirements analysis (cf. A.G.2, page 14 and [BSI-100-2], Section 4.3) for their specifically processed documents. In this respect, the results of the exemplary protection requirements analyses documented in [BSI-TR03138-R] can be used as orientation.

Since, as shown in [BSI-TR03138-A], the protection requirements of the other data objects results from the protection requirements of the paper-based originals, it is sufficient to determine the protection requirements of the latter with respect to the basic values integrity, confidentiality and availability. When determining the protection requirements, the classification[6] and summary of similar documents is recommended.

4 See [BSI-TR03138-A].
5 See [BSI-100-2], Section 4.2.3.
6 As part of the classification, documents can also be excluded from replacement scanning.

3.3 Security safeguards

The protection requirements analysis then leads to the classification of the classified documents according to the protection requirements categories “normal”, “high” and “very high”[7]. Based on this, it becomes clear which modules (basic module and advanced modules) are needed and which security safeguards from the modular safeguard catalogue (see Section 4) are required to achieve an adequate protection level.

7 See [BSI-TR03138-A] (Table 5).

4 Requirements for replacement scanning

4.1 Module concept

In order to be able to ensure a basic level of security in the case of replacement scanning, a basic module (see Section 4.2) which includes basic organisational, personal and technical safeguards as well as specific safeguards in the different phases of the “generic scanning process” (document preparation, scanning, post-processing, securing the integrity, cf. Figure 1) is provided.

In order to also be able to meet higher protection requirements regarding availability, integrity or confidentiality, corresponding “advanced modules” (see Section 4.3) are additionally provided. In addition to the general safeguards which must be generally implemented if documents with higher protection requirements are processed, there are specific safeguards for the processing of documents with protection requirements “high” or “very high” with respect to integrity, confidentiality and availability.

The requirements described in the different modules were derived from the risk analysis that was carried out when developing the Technical Guideline and is presented in more detail in [BSI-TR03138-A]. This risk analysis can thus be used when further information is required.

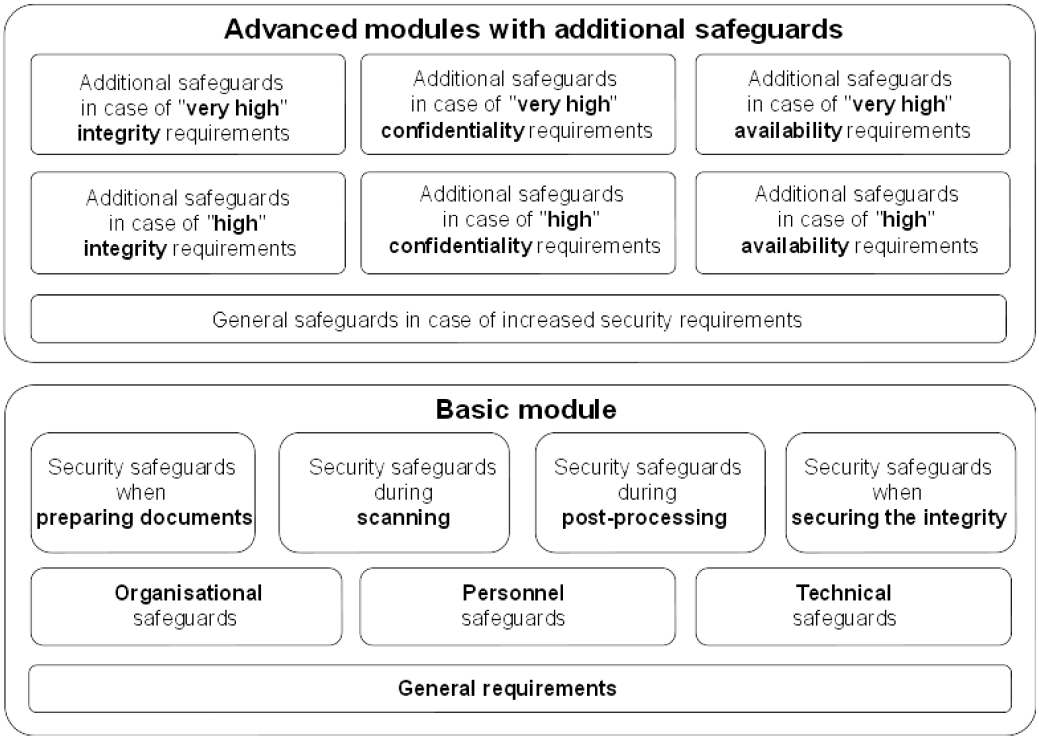

Figure 3: Module concept of the Technical Guideline

4.2 Basic module

By implementing the requirements from the basic module described below, a basic level of security is to be reached when performing replacement scanning. This is achieved by the combination of basic (A.G.x) and overall organisational (A.O.x), personnel (A.P.x) and technical safeguards (A.T.x) with specific safeguards in the individual phases of the generic scanning process. As shown in Figure 1 and Figure 3, this includes safeguards during document preparation (A.DV.x), safeguards during scanning (A.SC.x), safeguards during post-processing (A.NB.x) and finally safeguards when securing the integrity (A.IS.x).

4.2.1 General requirements

ID	General requirements
A.G.1	Process documentation
A.G.2	Protection requirements analysis

Table 2: General requirements

A.G.1 – Process documentation

In order to allow an orderly process flow when performing replacement scanning, there MUST be a process documentation. This process documentation MUST include the following aspects in particular:

(a) the type of the processed documents (see also A.G.2, below) and rules for documents which cannot be processed[8], the specification of responsibilities, processes and task during the scanning process (see also A.O.1),

(b) the definition of safeguards for the qualification of staff members and making them aware of information security issues (see also A.P.1),

(c) the description of the requirements for the rooms, IT systems, applications and securing measures involved in the scanning process, which comply with the protection requirements,

(d) regulations governing administration and maintenance of the IT systems and applications (see also A.O.2) as well as

(e) if necessary, the specification of suitable security safeguards for IT systems, networks and applications (see also A.T.1).

The process documentation[9] particularly includes process instructions which address the persons involved in the scanning process. Exemplary process instructions can be found in [BSI-TR03138-V]. In addition to the process instructions, the process documentation will also regularly include further documents, such as a corresponding security concept (cf. e)). The process instructions can refer to further applicable documents, such as concepts, specifications, manuals, work instructions, job descriptions.

A.G.2 – Protection requirements analysis

In order to ensure that a security level adequate to the respectively processed documents can be reached, a carefully justified protection requirements analysis[10] with respect to the different basic values of IT security[11] ("integrity", "confidentiality" and "availability") MUST be carried out for them in order to determine the respective protection requirements class ("normal", "high" or "very high").

4.2.2 Organisational safeguards

In the basic module, the organisational safeguards listed in Table 3 are provided.

8 For example, this can include valuable deeds and/or deeds with an official seal cord or documents in formats which cannot be processed technically.

9 The scope of the documentation required in the individual case is determined by what is necessary to understand the scanning process as well as the documents to be stored. The process documentation must be comprehensible and it must thus be possible for a third party expert to verify this within an appropriate period of time.

10 Exemplary protection requirements analyses for different areas of application can be found in [BSI-TR03138-R].

11 The definition of the basic values of IT security and the differentiated security objectives ("integrity", "authenticity", "completeness", "availability", "readability", "negotiability", "confidentiality" and "deletability") which can be assigned to them can be found in the informative annex [BSI-TR03138-A] (Table 6).

ID	Organisational safeguards	see also[12]
A.O.1	Specification of responsibilities and provisions	M2.1[13], M2.5, M2.225
A.O.2	Maintenance / repair regulations	M2.4
A.O.3	Acceptance and approval procedure for hardware and software	M2.62
A.O.4	Maintaining information security	M2.199
A.O.5	Requirements when outsourcing the scanning process	B1.11

Table 3: Overview of organisational safeguards

A.O.1 – Specification of responsibilities, processes and tasks during the scanning process

In order to ensure the correctness of the workflow when performing replacement scanning, the responsibilities, processes and tasks during the scanning process must be specified. This particularly includes defining

(a) which steps have to be carried out by whom and how they have to be performed in detail,

(b) which documents are scanned and what data[14] is created,

(c) which quality controls must be performed at which time intervals and according to which criteria and

(d) what backup data or security systems are provided for the protection of the integrity of this data.

(e) Quality controls MUST be performed at least on a random basis and SHOULD be carried out at regular intervals by staff members who are not assigned the operative implementation of the working step to be controlled.

(f) For the data objects involved in the scanning process (original document, scanned product etc.) as well as for the IT systems and applications used during the scanning process, persons responsible SHOULD[15] be appointed.

(g) When assigning staff members the operative tasks during the scanning process, potential conflicts of interest MUST be taken into account and SHOULD be avoided where possible.

(h) Moreover, typical sources of errors[16] MUST be taken into consideration and appropriate precautions SHOULD be defined.

(i) Furthermore, it MUST be specified, taking the applicable legal regulations into account, under which conditions and at what point in time the original document may be destroyed.

(j) In addition, a procedure to clarify "questions of doubt"[17] MUST be established.

(k) It is RECOMMENDED to carry out the scanning prior to the workflow processing ("early scanning"). The simulation study [RoNe14a] has clarified the relevance of the time of scanning: "Scanning at an early stage as well as the implementation of the scanning process by a third party makes it easier to demonstrate proof, because there could often not have been an interest in manipulation at that point in time. Time stamps or a document management system that is independent from the person

12 The references (e.g. to safeguards in [BSI-GSK]) are for further explanatory purposes only and only have an informative character.

13 The references S x.y given refer to safeguards of the IT-Grundschutz Catalogues [BSI-GSK] which were profiled in [BSI-TR03138-A] for the present case of replacement scanning.

14 See Table "List of data objects" in [BSI-TR03138-A].

15 Irrespective of the fact that only a recommendation was given here, appointed persons responsible might be mandatory due to applicable laws and regulations.

16 For example, a particularly careful completeness check is required for originally stapled paper documents.

17 This includes all aspects that cannot be decided without doubt by the persons acting on the basis of the process instructions.

demonstrating proof of the time of scanning are mandatory if proof of the time of scanning is crucial."

A.O.2 – Maintenance / repair regulations

In order to ensure secure operations, regulations for the maintenance and repair of the IT systems and applications used for the scanning process SHOULD be made. This includes in particular

(a) the specification of the responsibilities for the assignment, performance and, if necessary, monitoring of maintenance and repair work (see also A.O.1),

(b) procedures for the regular provision and application of security-relevant updates,

(c) regulations on the authentication and proof of the authorization of the maintenance staff,

(d) regulations on the protection of personal data or data otherwise requiring special protection (e.g. trade secrets) on the IT systems to be maintained,

(e) the documentation of security-relevant changes to the IT systems and applications involved as well as

(f) the documentation of the successful implementation of safeguards for quality control and approval (see also A.O.3) prior to the resumption of regular operations.

A.O.3 – Acceptance and approval procedure for hardware and software

In order to prevent the IT systems and applications used for scanning from being manipulated and to document the correctness of the systems, a controlled procedure for the acceptance and approval of the hardware and software used MUST be established. This includes both the scanner and the scanning workstation as well as the scan cache if necessary. In addition to the initial commissioning, this acceptance procedure must also be carried out when resuming operations after maintenance and repair work has been carried out (see also A.O.2).

A.O.4 – Maintaining information security

At adequate time intervals, the effectiveness and completeness of the safeguards provided for information security during replacement scanning SHOULD be checked. In federal agencies, this audit SHOULD be carried out at least every three years (cf. [BSI-IS-Rev]). In these audits, it MUST checked

(a) whether the implemented processes and security safeguards were implemented correctly and are actually effective and

(b) whether the implemented security safeguards provide adequate protection against potential threats or whether additional or corrected security safeguards are required.

In order to avoid conflicts of interests and to allow an impartial audit, the audits SHOULD be performed by independent persons, i.e. persons who are not assigned replacement scanning or the administration of the systems used and who are not bound to the instructions of those persons.

The results of these checks SHOULD be documented in writing. If security gaps or other problems are found, the necessary corrective measures MUST be derived from the audit results. For the implementation of the corrective measures identified, a schedule with responsibilities MUST be defined. The implementation of the safeguards MUST be monitored and reviewed by the persons responsible for this.

A.O.5 – Requirements when outsourcing the scanning process

If the scanning process is performed completely or partially by specialized scanning service providers, the safeguards provided in this requirements catalogue must be implemented accordingly. Furthermore, the following requirements apply[18]:

18 Moreover, [BSI-TR03138-R] examines selected legal aspects which can be relevant when outsourcing the scanning process.

(a) The organisational and technical interfaces between customer and contractor (transmission routes, data storage locations, actors involved, fallback procedures, safeguards to check integrity and completeness etc.) MUST be described explicitly in the process documentation (see A.G.1).

(b) The contractor MUST be obliged to comply with the security safeguards defined by the customer.

(c) An analysis of the additional risks resulting from the division of tasks SHOULD be performed.

(d) In addition to regular auditing (see A.O.4 at the top and A.AM.G.3), unannounced sampling inspections SHOULD be carried out.

4.2.3 Personnel safeguards

In the basic module, the personnel safeguards listed in the following table are provided.

ID	Personnel safeguards	see also
A.P.1	Making staff aware of information security issues	M2.198
A.P.2	Commitment of staff members to compliance with relevant laws, regulations, provisions and process instructions	M3.2
A.P.3	Training on the proper operation of the scanning system	M3.4
A.P.4	Training on security safeguards during the scanning process	M3.5, M3.26
A.P.5	Training of maintenance and administration staff	M2.40

Table 4: Overview of personnel safeguards

A.P.1 – Making staff aware of information security issues

The members of staff SHOULD be made aware with respect to the security safeguards and the security-conscious handling of documents, data and IT systems as well as of the precautions to be taken.

A.P.2 – Commitment of staff members to compliance with relevant laws, regulations, provisions and process instructions

The members of staff involved in the scanning process SHOULD be made aware of the legal framework conditions identified for the field of application concerned as part of the protection requirements analysis (see A.G.2). The members of staff SHOULD, if this has not already been the case, be obliged to comply with the relevant laws, regulations, provisions and the process instructions (see A.G.1).[19]

A.P.3 – Training on the proper operation of the scanning system

The members of staff who perform the scanning process MUST be instructed adequately with regard to the used devices, applications and other workflows. This includes in particular:

(a) the general workflows during the scanning process including the document preparation, scanning, indexing, admissible post-processing and securing of the integrity,

(b) the suitable configuration and use of the scanner and the scanning workstation,

(c) requirements with respect to quality assurance,

(d) the workflows and requirements when creating the transfer note (see A.NB.4),

(e) the configuration and usage of the systems to secure the integrity and

(f) response in the event of an error.

19 This applies irrespective of the legal duties to provide information and notify that exist anyway and will not be described in more detail here.

A.P.4 – Training on security safeguards during the scanning process

The members of staff who perform the scanning process or are responsible for it MUST be trained adequately with respect to the security safeguards to be implemented and those already implemented. If necessary, this includes in particular

(a) generally making staff aware of information security issues

(b) personal security safeguards in the scanning process,

(c) system-related security safeguards in the scanning system,

(d) procedures in the event of malware,

(e) importance of having and generating data backups

(f) handling of personal and other sensitive data and

(g) instruction in emergency measures.

A.P.5 – Training of the maintenance and administration staff

The maintenance and administration staff for the IT systems and applications involved in the scanning process needs detailed knowledge of the IT components used. The organization's own members of staff deployed SHOULD therefore be trained to such an extent that they can

- perform routine administration tasks independently,
- detect and eliminate errors by themselves,
- regularly make data backups by themselves,
- understand the tasks performed by external maintenance personnel and
- detect and quickly eliminate attempts to manipulate the systems or gain unauthorized access to the systems.

4.2.4 Technical measures

ID	Technical measures	see also
A.T.1	Basic security safeguards for IT systems during the scanning process	[BSI-GSK]
A.T.2	Specification of permissible communication connections	M2.42
A.T.3	Protection against malware	B1.6, M2.157, M2.158, M2.159, M6.32
A.T.4	Reliable storage	

Table 5: Overview of technical safeguards

A.T.1 – Basic security safeguards for IT systems during the scanning process

For the IT systems (e.g. client, server and network components) and applications involved in the scanning process, the security safeguards in the IT-Grundschutz Catalogues [BSI-GSK] relevant to the scanning system SHOULD be implemented.

A.T.2 – Specification of permissible communication connections

If the IT systems used for the scanning are connected via a network, the permissible communication connections MUST be protected effectively in this network as well as on the IT systems themselves against access from outside the network (firewall).

A.T.3 – Protection against malware

In order to prevent an infection by malware, the safeguards of the IT-Grundschutz module M 1.6 (Protection against malware) SHOULD be taken into account. The following safeguards in particular MUST be implemented:

(a) Selection of a suitable virus protection program (M2.157)

(b) Reporting infections of malware (M2.158),

(c) Updating the virus protection programs and signatures (M2.159) and

(d) Regular data backup (M6.32).

A.T.4 – Reliable storage

The storage media, processes (e.g. for the backup of data) and configurations used for the storage of the scanned products and metadata with preservation of evidence MUST ensure availability which meets the protection requirements of the data objects for the required retention period or up to the reliable transmission to a suitable long-term memory.

4.2.5 Security safeguards when preparing documents

ID	Technical measures	see also
A.DV.1	Careful preparation of the paper documents	BM2.1[20]
A.DV.2	Preparation of the completeness check	BM2.1

Table 6: Security safeguards when preparing documents

A.DV.1 – Careful preparation of the paper documents

In order to ensure the reliable and complete recording of the paper documents in the next step, paper documents MUST be prepared carefully. This preparation should usually include the following aspects:

(a) if necessary, creating incoming mail stamps, opening the letter carefully, checking whether it is an obviously manipulated document or a copy, assigning the paper document to a specific document class in order to allow corresponding preliminary sorting. In this respect, it MUST be checked in particular whether the documents are generally provided for recording (cf. A.G.1 a)).

(b) if necessary, checking that the documents to be scanned are suitable in such a way that they can be processed with the devices, processes and settings used without errors.

(c) safeguards for preserving the logical context of the documents recorded (e.g. by means of adequate indexing) or for preserving that the scanned pages belong to a document[21] must also be taken into account in particular for “late scanning”.

(d) the correct orientation of the pages to be recorded. If only simplex scanning is performed, it MUST be ensured that the relevant page is recorded. If this is not possible, duplex scanning MUST be performed.

(e) preserving the correct order of pages in the case of documents with several pages.

(f) reliable separation of independent documents.

(g) removing staples, bends and irrelevant sticky notes. If the content of a sticky note is relevant, the sticky note MUST be scanned in a suitable manner (e.g. on a separate page).

20 The references BMx.y given refer to the defined “user-specific safeguards” in [BSI-TR03138-A].

21 Legal considerations and derived recommendations on the handling of documents which have an official seal cord can be found in [BSI-TR03138-R].

(h) other preparing safeguards depending on the written material to be scanned. For example, this can include examining the written material for possibly existing images requiring a specific configuration of the scanner (e.g. with respect to brightness, contrast or colour, cf. A.SC.5). If copying is required as part of the scanning process, it MUST be taken into account that the copy contains all relevant information.

A.DV.2 – Preparation of the completeness check

Suitable[22] safeguards for ensuring completeness MUST be taken. In order to ensure that this completeness check can be carried out as part of the follow-up (see A.NB.3), corresponding preparations SHOULD be taken here if necessary. This CAN for example include the number of pages to be recorded.

4.2.6 Security safeguards during scanning

ID	Technical measures	see also
A.SC.1	Selection and purchasing of suitable scanners	M2.399[23]
A.SC.2	Data and site access controls for scanners	M1.32, M4.80
A.SC.3	Change of preset passwords	M4.7, M2.11
A.SC.4	Careful modifications of configurations	M4.78
A.SC.5	Appropriate usage of the scanner	BM2.5
A.SC.6	Suitable scanning settings	BM2.4
A.SC.7	Suitable collection of meta information	BM2.6
A.SC.8	Quality assurance of the scanned products	BM2.7
A.SC.9	Taking scanners securely out of operation	M2.400
A.SC.10	Information protection and data access restrictions in case of network-compatible scanners	M4.300, S 4.301, M4.303
A.SC.11	Logging during scanning	M4.302
A.SC.12	Selection of suitable image compression processes	

Table 7: Security safeguards during scanning

A.SC.1 – Selection and purchasing of suitable scanners

In order to ensure that suitable scanners are used for the recording process, the following criteria that have to be checked for relevance SHOULD already be taken into account when selecting and purchasing scanners:

- throughput sufficient for the respective application,
- support of suitable data formats,
- support of patch and/or barcodes for document separation and transfer of meta-information,

22 When processing documents with “normal” protection requirements and in an automated process, the completeness check CAN be reduced to regular sampling in order to detect systematic errors (e.g. malfunctions of the scanner). The size of the sample SHOULD be determined depending on the protection requirements of the scanned documents, the reliability of the scanning system and the results of previous samples. Similarly to the quality assurance (cf. A.SC.8), the completeness check CAN be carried out implicitly by the workflow processing downstream of the recording process.

23 The aspects listed in S 2.399 for printers, copiers and all-in-one devices also apply to the same extent to (network-compatible) scanners.

- adequate quality of the scanned products (with respect to resolution, image compression processes, brightness and contrast etc.),
- sufficient flexibility of the configuration,
- adequately reliable and powerful automatic page feed (also for duplex recording and with reliable double-feed control),
- if necessary, possibility to scan bound documents, excess lengths, to scan colour as well as transmitted light documents (e.g. X-ray images),
- suitable interfaces[24] for the transmission of the scanned product in DMS/WS/archives/specialist applications,
- possibility to secure the administration interface (locally and via the network),
- usage of an internal data memory,
- possibility for the secure deletion or encrypted storage of scanned products on the internal data medium and
- sufficient support.

A.SC.2 – Data and site access controls for scanners

In order to avoid malfunctions during the recording process and manipulations at the scanning system, it SHOULD be ensured that unauthorized persons cannot get access to a scanning system. For this purpose, suitable access controls and rules for visitors SHOULD be provided. In order to achieve high protection against manipulations of the scanner or its configurations, or of the documents during the scanning process or against the subsequent reading of scanned products from the internal data medium of the scanner, access to the scanner SHOULD generally (i.e. also beyond the scanning process) be restricted to a minimum.

The administration of the scanner or the configuration of the communication interfaces in the case of network-compatible scanners SHOULD be protected by means of an appropriate authentication procedure (i.e. at least by a suitably chosen password) against unauthorized access. Furthermore, the access to the administration interface SHOULD be restricted to the systems required by means of a suitable network configuration.

A.SC.3 – Change of preset passwords

If the administration of the scanner or the configuration of the communication interfaces in the case of network-compatible scanners is secured with a password, such a password MUST be set or changed after the scanner has been installed. The basis for the assignment of the passwords SHOULD be explicitly formulated internal security policies by taking into account the recommendations in [BSI-GSK] (S 2.11).

A.SC.4 – Careful modifications of configurations

Performing configuration modifications to an IT system during regular operations, such as a scanner and the corresponding software components, must always be classified as critical, which is why appropriate caution MUST be exercised in this respect. Prior to changing the configuration, the old configuration SHOULD be backed up. Moreover, all changes which have been performed SHOULD be examined by a colleague before being incorporated into regular operations.

A.SC.5 – Appropriate usage of the scanner

In order to ensure the reliable and complete recording of paper documents, a scanner maintained according to the manufacturer's specifications MUST be used. The documents MUST be transferred to the scanner in accordance with specifications in the product manuals and according to the physical structure of the

24 For example, this can include the mutually authenticated and encrypted as well as asynchronous and, if necessary, time-controlled transmission.

documents. For documents which are not suitable for automatic feed (e.g. unsuitable paper grades, damaged pages, bound documents), suitable methods[25] must be described in the process documentation.

A.SC.6 – Suitable scanning settings

The scanning settings (e.g. simplex or duplex scan, format, resolution, image compression processes, contrast, brightness, colour depth, automatic document separation, detection of empty pages, blind colour filter) MUST be suitably chosen for the respective documents. Here, suitable profiles SHOULD be defined, tested, approved and used according to the document types to be processed. The profile to be used CAN already be defined during the document preparation (see also A.DV.1). Otherwise, it SHOULD be checked during scanning at the latest that suitable scanning settings are used.

A.SC.7 – Suitable collection of meta information

In order to ensure that it is possible to subsequently assign the scanned products to a business transaction, index data and metadata SHOULD be transmitted in a suitable manner. In the case of a high scanning throughput and if complex contexts (e.g. envelope context) have to be observed, corresponding, automatically recordable cover sheets for the separation of documents and specification of other meta-information such as page number, scanning settings, document context, index information, CAN be used. In this case, the scanning system CAN evaluate this information automatically if necessary, adjust the settings, summaries scanned products accordingly and add the metadata to the scanned product. Solutions for the automatic reading of index information CAN also be used. However, the application SHOULD then be configured reliably with respect to the detection and validity of the read values and careful manual quality assurance and post-processing.

A.SC.8 – Quality assurance of scanned products

In order to avoid faulty scanning processes (e.g. missing pages, lack of readability, missing document interrelation, damaged files), suitable quality control and, if necessary, new recording and an adjustment of the scanning settings MUST be performed. The detailed design of the quality assurance step SHOULD be based on the scan throughput as well as on the protection requirements of the processed documents.

When processing documents with “normal” protection requirements and a high throughput, the visual inspection CAN be reduced to regular sampling in order to detect systematic errors (e.g. unsuitable scanning settings, malfunctions of the scanner). The size of the sample SHOULD be determined depending on the protection requirements of the scanned documents and the reliability of the scanning system and specified in the process documentation. In addition, automatic mechanisms for quality control CAN be used, such as an automatic detection of empty pages or of an inadequate image quality or the checking of the page number (e.g. by comparing it to the metadata provided on the cover sheet). Since, however, automatic quality controls are generally prone to error (e.g. it might be difficult to distinguish between pages with hand-written notes only, such as initials, and empty pages), the automatically identified problems SHOULD be examined manually. Quality assurance CAN also be performed implicitly by the workflow processing downstream of the recording process.[26]

The original documents MUST NOT be destroyed before the quality control has been completed.

A.SC.9 – Taking scanners securely out of operation

When taking scanners out of operation, all security-relevant information as well as information stored in the meantime in the scan cache MUST be deleted reliably from the devices. This also applies particularly to authentication information (e.g. passwords, private keys). This applies especially when the components will be disposed of or given to third parties. Furthermore, specific configuration information (e.g. IP addresses) which can provide conclusion to internal network structures SHOULD be deleted.

25 For example, it can be prescribed for those documents that they have to be placed manually on the scanner or copied according to a defined process.

26 See also A.O.1 k).

A.SC.10 – Information protection and data access restrictions in case of network-compatible scanners

For scanners which can be addressed via a network, suitable safeguards to restrict access and to protect the information transmitted via the network SHOULD be provided. This includes securing the data transmission between the scanner and scanning workstation or scan cache as well as the secure storage and deletion of data on an internal data medium of the scanner. If network drives for the storage of intermediate results or scanned products are used, access to these network drives MUST be restricted to the minimum extent required. When all-in-one devices that support a scan-to-mail or scan-to-fax function, the scanned products MUST be prevented from being sent to undesired groups of recipients by means of a suitable configuration of the servers used for the transmission.

A.SC.11 – Logging during scanning

In order to ensure a reliable operational management and comprehensibility of the scanning process, suitable[27] logging that is specified in more detail in the process instructions and includes the following aspects in particular SHOULD be carried out:

- the change of critical configuration parameters as well as authentication and authorization information,
- the information who has used the scanning system when and how,
- the information whether manual post-processing of the scanned product has been performed and
- failed authentication processes and other occurred errors.

The logged data MUST be processed according to the applicable data protection provisions and protected against unauthorized access in particular.

A.SC.12 – Selection of suitable image compression processes

For scanning, the selection of suitable image compression processes MUST be taken into account. Both lossless and lossy processes are considered suitable.

Processes which use the so-called “Symbol Coding”[28] for image compression MUST NOT be used.[29]

27 On the one hand, logging aims at making a reliable operational management possible during the scanning process and, on the other, at comprehensively documenting the relevant aspects of the scanning process for as comprehensive a preservation of the evidential value of a scanned product as possible unless these already result from the transfer notes according to A.NB.4.

28 The basic principle of “Symbol Coding” is explained in the so-called “JBIG2” standard (see Section 0.2.1 in [ISO14492] or [ITU-T.88]). More detailed information in this respect can be found under the term “Pattern Matching & Substitution” or “Soft Pattern Matching” in Section D of [HKM+98].

29 In the case of imprecise or improperly implemented “Symbol Coding”, there is the risk that the scan result differs semantically (e.g. by changing the places of characters) from the original. Even if implemented correctly, the required legal certainty cannot be ensured because it cannot be determined securely that the content and the picture conform to each other.

4.2.7 Security safeguards during post-processing

ID	Security safeguards during post-processing	see also
A.NB.1	Adequate and traceable post-processing	Bm4.1
A.NB.2	Quality assurance of post-processed scanned products	BM3.4
A.NB.3	Implementation of the completeness check	BM2.1, A.DV.2
A.NB.4	Transfer note	[BSI-TR03138-R] for further legal explanations

Table 8: Security safeguards during post-processing

A.NB.1 – Adequate and traceable post-processing

The scanned product MUST NOT be post-processed (e.g. change in the contrast/brightness, colour quantization, cutting, noise reduction) except in order to increase readability. If the scanned product is post-processed, this MUST be carried out carefully and logged so that it is not possible that potentially relevant information is destroyed or contents are manipulated without this being noticed. What form of post-processing is permissible in which cases SHOULD be regulated in the process instructions (see A.G.1).

A.NB.2 – Quality assurance of post-processed scanned products

If the scanned products are post-processed, quality assurance MUST in any case be performed as part of the operations carried out so that it is ensured that no relevant information has been lost due to the post-processing. The original scanned products MUST NOT be deleted before the quality control has been completed.

A.NB.3 – Implementation of the completeness check

Suitable safeguards for ensuring completeness MUST be taken. For this purpose, for example the number of the pages recorded by the scanner CAN be compared to the number determined during the document preparation (see A.DV.2). By means of a suitable double-feed control at the scanner (see A.SC.1) the simultaneous feed of several pages CAN avoided or at least detected. The completeness check CAN also be carried out as part of the subsequent processing.

When processing documents with “normal” protection requirements and in a largely automated process, the completeness check CAN be reduced to regular sampling in order to detect systematic errors (e.g. malfunctions of the scanner). The size of the sample SHOULD be determined depending on the protection requirements of the scanned documents, the reliability of the scanning system and the results of previous samples.

A.NB.4 – Transfer note

For each scanned product, a related transfer note documenting the following aspects in particular SHOULD be created:

(a) creator[30] of the scanned product,

(b) technical and organisational environment of the recording process,

(c) any abnormalities during the scanning process[31],

30 “Creator” refers to the natural person responsible for the creation of the scanned product who can be identified if necessary (e.g. in case of dispute). For data economy reasons, using suitable mechanisms for pseudonymisation is recommended.

31 For example, it can be noted that the original paper document was incomplete or has already been available as a copy.

(d) time of recording[32],

(e) quality assurance result and

(f) the fact that it is a scanned product which conforms to the paper document both pictorially and as regards content.

The transfer note or the equivalent information MUST logically be linked with the scanned product or integrated into the scanned product. The integrity of the transfer note MUST be protected according to the protection requirements of the processed documents (cf. A.IS.1, A.AM.IN.H.1 and A.AM.IN.SH.2). For the documentation of the technical and organisational environment, the transfer note CAN refer to the process documentation valid at that time. The transfer note CAN be omitted as an independent document or information embedded in the scanned product if the information above can easily be proven in another a way, such as based on the corresponding logged information[33].

4.2.8 Security safeguards when securing the integrity

ID	Security safeguards when securing the integrity	see also
A.IS.1	Use of adequate services and systems for the protection of the integrity	BM4.3

Table 9: Security safeguards when securing the integrity

A.IS.1 – Use of adequate services and systems for the protection of the integrity

In order to prevent the data objects (scanned product, transfer note, index data and metadata, log data etc.) which originate from the scanning process from being manipulated without this being noticed, adequate mechanisms for the protection of the integrity of these data objects MUST be used. For the suitability of a mechanism for the protection of the integrity, the resistance to targeted attacks is crucial, which MUST be based on the protection requirements of the data objects to be processed with regard to integrity. Pursuant to this, any backup data or system-related security safeguards CAN generally be used provided that the mechanism used is adequately[34] resistant. When processing documents with "normal" protection requirements with respect to integrity, it is not necessary to use cryptography. In order to protect the data objects against accidental changes or changes due to system errors, however, they SHOULD be secured using a suitable data backup method. If data objects are processed which have "high" or "very high" protection requirements regarding integrity, the additional safeguards from the "advanced module integrity" MUST be taken into consideration (see Section 4.3.2).

4.3 Advanced modules

In order to be able to provide adequate packages of safeguards for the respective use case, specific safeguards are required in addition to the basic module in the case of higher protection requirements (cf. Figure 3).

In this respect, general safeguards (A.AM.G.x) are provided in Section 4.3.1 which MUST be implemented if the protection requirements of the processed documents regarding at least one of the considered basic values of integrity, confidentiality and availability are at least "high".

32 See also A.O.1 k).

33 If the logged information partially or completely replace the transfer note, the integrity of the latter must be protected accordingly.

34 With respect to the decision whether a security mechanism used has adequate resistance, the potential for attack of an attacker formalised as part of the Common Criteria (cf. [CC-P3-v3.1], Section 16 and Section B.4) can be used if necessary. For example, an appropriate level of security is achieved in the case of "very high" protection requirements if attackers can be warded off successfully with a "high" potential for attack.

Moreover, the specific safeguards in the Sections 4.3.2 - 4.3.7 MUST be implemented when the protection requirements regarding the corresponding basic value (integrity (gw=IN), confidentiality (gw=VT) or availability (gw=VF)) is "high" (A.AM.gw.H.x) or "very high".

4.3.1 General safeguards in case of increased security requirements

The following safeguards MUST be implemented provided that documents are processed whose protection requirements with respect to at least one of the considered basic values of integrity, confidentiality or availability are at least classified "high".

ID	General safeguards in case of increased security requirements	see also
A.AM.G.1	Restricting access to sensitive paper documents	BM2.3
A.AM.G.2	Mandatory logging during scanning	M4.302
A.AM.G.3	Mandatory regular auditing	

Table 10: Additional safeguards in the event of increased protection requirements

A.AM.G.1 – Restricting access to sensitive paper documents

When processing documents with protection requirements of at least "high" regarding integrity, confidentiality or availability, NO unauthorized persons SHOULD gain access to the paper documents during preparation and during the scanning process. In this case, suitable safeguards for restricting access to sensitive paper documents SHOULD therefore be taken. These safeguards include:

(a) suitable restrictions of access to the premises in which the documents are processed,

(b) storage that provides protection against unauthorized access, inspection or damage as well as

(c) the commitment of staff members to the careful handling of the documents (e.g. no leaving documents unattended, no forwarding without verifying authorization).

Unless there are already general regulations for the access to sensitive paper documents, corresponding regulations MUST be established as part of replacement scanning.

A.AM.G.2 – Mandatory logging during scanning

When processing documents with protection requirements of at least "high" regarding integrity, confidentiality or availability, the logging recommended in A.SC.11 (see Section 4.2.6) MUST be performed.

A.AM.G.3 – Mandatory regular auditing

When processing documents with protection requirements of at least "high" regarding integrity, confidentiality or availability, the auditing of the effectiveness and completeness of the safeguards provided for information security during replacement scanning that are recommended in A.O.4 (see Section 4.2.2) MUST be carried out at least every three years (cf. [BSI-IS-Rev]).

4.3.2 Additional safeguards in case of high integrity requirements

The safeguards provided in this Section MUST be taken into account when processing documents with protection requirements of at least "high" regarding integrity.

ID	Additional safeguards in case of high integrity requirements	see also
A.AM.IN.H.1	Use of cryptographic mechanisms for the protection of the integrity	BM4.2
A.AM.IN.H.2	Appropriate key management	M2.46
A.AM.IN.H.3	Selection of a suitable cryptographic procedure	M2.164
A.AM.IN.H.4	Selection of a suitable cryptographic product	M2.165
A.AM.IN.H.5	Long-term data backup when using cryptographic methods	M6.56
A.AM.IN.H.6	Prevention of insecure network access	M2.204, M5.146

Table 11: Additional safeguards in case of high integrity requirements

A.AM.IN.H.1 – Use of cryptographic mechanisms for the protection of the integrity

When processing data objects with protection requirements of at least "high" regarding integrity, suitable cryptographic mechanisms (e.g. digital signatures and time stamps) SHOULD be used. Otherwise, written proof MUST be furnished that the mechanism used for the protection of the integrity is adequately[35] resistant within the meaning of the definition above.

With an advanced electronic signature according to § 2 No. 2 SigG [German Signature Act] or an electronic seal according to Art. 3 No. 25 of the Regulation (EU) No. 910/2014, both the integrity and the authenticity of the corresponding data objects (e.g. scanned product, transfer note) can be ensured. In order to also ensure the negotiability of the data objects and backup data, using standardized formats (e.g. [CAdES], [PAdES] , [XAdES] and [ASiC]) is RECOMMENDED.

A special form of the advanced electronic signature, for which the requirements A.AM.IN.H.2, A.AM.IN.H.3 and A.AM.IN.H.4 are complied with automatically, is the qualified electronic signature according to § 2 No. 3 SigG [German Signature Act], which is additionally based on a qualified certificate and was created using a secure signature creation device.

For the protection of the integrity of the documented time of the scanning process (as metadata item), time stamps SHOULD[36] be used according to [ISO18014-1] or [RFC3161].[37]

A.AM.IN.H.2 – Appropriate key management

If key-based cryptographic mechanisms are used, suitable methods for the key management MUST be provided.

Throughout the provided retention period of the scanned products, it MUST be ensured that

- the confidentiality, integrity and authenticity of the keys are maintained,
- private or secret keys cannot be used in an unauthorized manner,
- the keys and certificates required for the check of the integrity protection remain available.

35 See footnote 34.

36 See also A.O.1 k).

37 It must be taken into account, however, that such a time stamp only proves that the document (e.g. scanned product, transfer note) equipped with the time stamp has been available at that time, i.e. that the document is not newer than the time indicated in the time stamp. In order to also prove that a document is not older than a time indicated in a time stamp, the time stamp can be equipped with an advanced electronic signature first and another time stamp can then be created for this electronic signature (see [HüKo06], Section 4.7). In order to protect several data objects with a time stamp, hash trees can be created, as it is explained in more detail in [RFC4998], and only the root of the hash tree can be equipped with a time stamp. The evidential value related to a time stamp with regard to the time of signing depends not least on the security safeguards implemented at the issuer of the time stamp. Qualified time stamps according to § 2 No. 14 SigG [German Signature Act] that are equipped with a qualified electronic signature have a particularly high evidential value, since they also benefit from the prima facie evidence in accordance with § 371a ZPO [German Code of Civil Procedure].

In this respect, the relevant recommendations in [BSI-M 2.46], [NIST-800-57-1], [NIST-800-57-2] and [NIST-800-133] SHOULD be taken into consideration when managing the key material or trustworthy services providers (e.g. accredited certification service providers) used for the key management.

A.AM.IN.H.3 – Selection of a suitable cryptographic method

If cryptographic methods are used, suitable cryptographic methods MUST be used. In this respect, methods according to [BSI-TR02102] or [BSI-TR03116] SHOULD be used. Otherwise, written proof MUST be furnished that the mechanism used is adequately[38] resistant within the meaning of the definition above.

A.AM.IN.H.4 – Selection of a suitable cryptographic product

In order to secure the integrity, suitable products regarding functionality and trustworthiness MUST be used. In terms of functionality, adequate[39] strength and resistance of the security mechanisms used must be taken into account. With respect to the trustworthiness, using published and jointly analysed algorithms (see A.AM.IN.H.3, at the top) and sources as well as tests carried out according to a recognized security standard, such as FIPS-140, Common Criteria or ITSEC must be rated positively and should therefore be used primarily.

For the creation of qualified electronic signatures, secure signature creation devices according to § 2 No. 10 SigG [German Signature Act] MUST be used. Furthermore, suitable signature application components according to § 2 No. 11 SigG that have a manufacturer declaration or confirmation according to the German Signature Act SHOULD be used. The Federal Network Agency (BNetzA) provides lists with confirmations and manufacturer declarations for products for qualified electronic signatures. Since the suitability of the cryptographic algorithms as security measures may change, it SHOULD be taken into consideration that the corresponding components can easily be exchanged.

In order to ensure that the cryptographic products are used securely, the necessary operating conditions and other recommendations of the manufacturer MUST be taken into consideration.

A.AM.IN.H.5 – Long-term data backup when using cryptographic methods

For the cryptographic methods used, the suitable of the algorithms and parameters used SHOULD be evaluated at regular intervals. For digital signatures, the suitability of the methods is defined in the algorithm catalogue which is published by the Federal Network Agency (BNetzA) in coordination with the BSI each year. If the evidential value of qualified signed data is to be preserved over longer periods of time, re-signing MUST be carried out in a timely manner before the suitability of the cryptographic methods expires. For the preservation of the evidential value of cryptographically signed data, using the methods and formats specified in [BSI-TR03125] is RECOMMENDED.

A.AM.IN.H.6 – Prevention of insecure network access

If the IT systems used for the scanning are connected via a network, insecure access to this network segment MUST be avoided. This network segment MUST NOT be accessed from the Internet unless the communication is provided by means of a proxy or a gateway and the connection is established from inside.

4.3.3 Additional safeguards in case of very high integrity requirements

The safeguards provided in this Section MUST be taken into account when processing documents with “very high” protection requirements regarding integrity.

38 See footnote 34.
39 See footnote 34.

ID	Additional safeguards in case of very high integrity requirements	see also
A.AM.IN.SH.1	Two-person rule	A.O.1 (item c in particular), page 15
A.AM.IN.SH.2	Use of qualified electronic signatures and time stamps	BM4.2 [BSI-TR03138-R]
A.AM.IN.SH.3	Separate network segment	M2.204, M5.146
A.AM.IN.SH.4	Labelling of the documents regarding sensitivity	BM2.2

Table 12: Additional safeguards in case of very high integrity requirements

A.AM.IN.SH.1 – Two-person rule

In the case of "very high" protection requirements regarding integrity, a two-person rule MUST be implemented as part of the division of tasks (see A.O.1). In this respect, it MUST be ensured in particular that the generation and quality assurance of the scanned product is carried out by different people.

A.AM.IN.SH.2 – Use of qualified electronic signatures and time stamps

If data objects

(a) with "very high" protection requirements regarding integrity are processed,

(b) negotiability is required and

(c) the data objects (scanned product, transfer note, index data and metadata, logged data) resulting as part of the scanning process are probably to be used as evidence,

qualified time stamps SHOULD be used for securing the integrity of the scanned product or the transfer note qualified electronic signatures and for securing the integrity of the documented time of the scanning process (cf. A.AM.IN.H.1). Otherwise, written proof MUST be furnished that the mechanism used for the protection of the integrity is adequately[40] resistant.

A.AM.IN.SH.3 – Separate network segment

In the case of "very high" protection requirements of the data objects regarding confidentiality or integrity, the IT systems used for the scanning MUST be integrated into a separate network segment. This network segment MUST NOT be accessed from other network segments unless the communication is provided by means of a proxy or a gateway and the connection is established from inside.

A.AM.IN.SH.4 – Labelling of the documents regarding sensitivity

Documents which have "very high" protection requirements regarding integrity SHOULD be labelled as such. The labelling SHOULD be displayed clearly visibly so that people processing the document pay attention to the sensitive nature of the document and handle it adequately.

4.3.4 Additional safeguards in case of high confidentiality requirements

The safeguards provided in this Section MUST be taken into account when processing documents with protection requirements of at least "high" regarding confidentiality.

40 See footnote 34,.

ID	Additional safeguards in case of high confidentiality requirements	see also
A.AM.VT.H.1	Awareness-raising and training of the staff members	A.P.1, A.P.2
A.AM.VT.H.2	Prevention of insecure network access	A.AM.IN.SH.3, Section 4.3.2
A.AM.VT.H.3	Deletion of intermediate results	[BSI-B1.15]

Table 13: Additional safeguards in case of high confidentiality requirements

A.AM.VT.H.1 – Raising the staff members' awareness and commitment of staff members

When processing documents with protection requirements regarding confidentiality of at least "high", the staff members MUST be made aware of the security safeguards and the security-conscious handling of documents, data and IT systems and the precautions to be taken and trained in this respect. Moreover, the staff members MUST be obliged by means of explicit process instructions to comply with the relevant laws, regulations and provisions.

A.AM.VT.H.2 – Prevention of insecure network access

See A.AM.IN.SH.3, Section 4.3.2.

A.AM.VT.H.3 – Deletion of intermediate results

When processing documents with protection requirements regarding confidentiality of at least "high", the intermediate results resulting from processing (e.g. raw scanned products, data in the scan cache, swap files) MUST be deleted in a reliable manner.

4.3.5 Additional safeguards in case of very high confidentiality requirements

The safeguards provided in this Section MUST be taken into account when processing documents with "very high" protection requirements regarding confidentiality. In addition to or instead of the safeguards listed here, the corresponding requirements of the instructions for classified information must be taken into consideration when processing classified information.

ID	Additional safeguards in case of very high confidentiality requirements	see also
A.AM.VT.SH.1	Labelling of the documents regarding sensitivity	BM2.2
A.AM.VT.SH.2	Correct disposal of resources requiring protection	M2.13
A.AM.VT.SH.3	Special reliability and trustworthiness of staff members	M3.33
A.AM.VT.SH.4	Encrypted data transmission within the scanning system	BM4.2

Table 14: Additional safeguards in case of very high confidentiality requirements

A.AM.VT.SH.1 – Labelling of the documents regarding sensitivity

Documents which have "very high" protection requirements regarding confidentiality SHOULD be labelled as such. The labelling SHOULD be displayed clearly visibly so that people processing the document pay attention to the sensitive nature of the document and handle it adequately.

A.AM.VT.SH.2 – Correct disposal of resources requiring protection

If the scanner is equipped with an internal data medium and documents with "very high" protection requirements regarding confidentiality are scanned, the data medium MUST be reliably deleted before the scanner is disposed of. If possible, the data medium SHOULD be removed from the scanner and deleted by

means of a suitable method or destroyed if necessary. Moreover, cryptographic keys which are stored in software in the scanner to be disposed of MUST be reliably deleted or otherwise deactivated (e.g. by means of corresponding safeguards in the infrastructure provided for key management). In any contracts concluded with service providers, it must be ensured that a reliable deletion and disposal method that is transparent for the organisation is established.

A.AM.VT.SH.3 – Special reliability and trustworthiness of staff members

If documents are scanned whose protection requirements are "very high" regarding confidentiality, it SHOULD be ensured that the staff members who are responsible for the scanning process and perform the process are particularly reliable and trustworthy.

A.AM.VT.SH.4 – Encrypted data transmission within the scanning system

When processing data objects with "very high" protection requirements regarding confidentiality, the data transmission between scanner, scan workstation, scan cache and other related systems SHOULD be carried out by means of suitable encryption methods according to [BSI-TR02102] or [BSI-TR03116]. Otherwise, adequate proof MUST be furnished that the communication connections are protected adequately by means of alternative safeguards.

4.3.6 Additional safeguards in case of high availability requirements

The safeguards provided in this Section MUST be taken into account when processing documents with protection requirements of at least "high" regarding availability.

ID	Additional safeguards in case of high availability requirements	see also
A.AM.VF.H.1	Extended quality assurance of the scanned products	A.SC.8
A.AM.VF.H.2	Error-tolerant protocols and redundant data storage	

Table 15: Additional safeguards in case of high availability requirements

A.AM.VF.H.1 – Extended quality assurance of the scanned products

In the case of "high" protection requirements of the data objects regarding availability, particularly careful[41] quality control of the scanned products (see A.SC.8, page 23) SHOULD be performed.

A.AM.VF.H.2 – Error-tolerant protocols and redundant data storage

In the case of "high" protection requirements regarding availability, using an error-tolerant transmission protocol as well as redundant data storage are RECOMMENDED.

4.3.7 Additional safeguards in case of very high availability requirements

The safeguards provided in this Section MUST be taken into account when processing documents with "very high" protection requirements regarding availability.

41 When scanning personnel files in the Federal Administration, Federal Commissioner for Data Protection and Freedom of Information (BfDI) generally requires complete visual inspection and the use of qualified electronic signature according to the German Signature Act (cf. [BfDI-TB-23] (Sections 5.5 and 12.3) and [BfDI-TB-24] (Section 13.3)).

ID	Additional safeguards in case of very high availability requirements	see also
A.AM.VF.SH.1	Complete visual inspection for assuring the quality of the scanned products	A.SC.8
A.AM.VF.SH.2	Test of the devices and settings with similar documents	

Table 16: Additional safeguards in case of very high availability requirements

A.AM.VF.SH.1 – Complete visual inspection for assuring the quality of the scanned products

In the case of "very high" protection requirements of the data objects regarding availability, quality control of the scanned products SHOULD be carried out by means of complete visual inspection.

A.AM.VF.SH.2 – Test of the devices and settings with similar documents

In the case of data objects with "very high" protection requirements regarding availability, the suitability of the devices, processes and settings used MUST be tested in advance with physically similar documents that do not have high protection requirements regarding availability and the test result documented.

Table of abbreviations

AO	(German) General Tax Code
Ax	Application
A.x.y	Requirement
M x.y	Module in the BSI's IT-Grundschutz Catalogues
BBG	(German) Federal Civil Service Act
BDSG	(German) Federal Data Protection Act
BGBl	(German) Federal Law Gazette
BGH	Federal Supreme Court
US x.y	User-defined security safeguard
BNetzA	Federal Network Agency; (German) Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
BSI	Federal Office for Information Security
CC	Common Criteria for Information Technology Security Evaluation
Dx	Data object
DMS	Document Management System
ECM	Enterprise Content Management
ETSI	European Telecommunications Standards Institute
GDPdU	Principles of Data Access and Auditability of Digital Documents (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
GoBS	Principles of Orderly IT-Supported Bookkeeping Systems (Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme)
HGB	(German) Commercial Code
IT	Information technology
ITSEC	Information Technology Security Evaluation Criteria
Cx	Communication relation
S x.y	Security safeguard in the BSI's IT-Grundschutz Catalogues
PDF	Portable Document Format
RFC	Request for Comments
Sx	IT System
SigG	(German) Signature Act
SigV	(German) Signature Ordinance
TLS	Transport Layer Security
TR	Technical Guideline
TSP	Time Stamp Protocol
USB	Universal Serial Bus

WS	Workflow system
VSA	Instructions for classified information
XML	eXtensible Markup Language
ZDA	Certification Service Provider
ZPO	(German) Code of Civil Procedure

Glossary

Authentication

The term “authentication” refers to a “claim” concerning an electronic identity. Here, a “claim” consists at least of one identity attribute (e.g. the name of the communication partner).

Authentication

In the case of “authentication”, a “claim” concerning an electronic identity is made.

Authenticity

The term “authenticity” of data means that the source of the data can clearly be determined.

Pictorial Conformity

“Pictorial conformity” between a scanned product and an original is given if the scanned product is an identical copy of the original within the framework of the resolution chosen.

Supplementary Scanning

If the paper-bound original is still kept after “scanning”, “supplementary scanning” is referred to.

Replacement Scanning

If the paper-bound original is destroyed after “scanning”, “replacement scanning” is referred to.

Informative

An “informative” part of a document does not contain any binding specifications and requirements and is intended to only provide the reader with information.

Content-Related Conformity

“Content-related conformity” between a scanned product and an original is given if the scanned product and the original conform to each other in the essential content data, but not necessarily in the visual representation.

Integrity

“Integrity” means that the data or systems were not modified. In the case of the effective protection of the integrity, at least changes are also identified.

IT System

The term “IT system” describes an information processing system consisting of hardware and software.

Readability

Readability means that the information contained in the data can be recognised.[42]

Deletability

Deletion of data means that the data stored is made illegible (§ 3 (4) No. 5 BDSG) [German Federal Data Protection Act]. This is the case if the data has been treated irrevocably in

42 It should be noted that the negotiability of cryptographically secured data can only be ensured if generally recognised (e.g. international) standards and interoperable systems are used.

such a way that one's own information cannot be obtained from the data stored, i.e. if it is no longer possible to access this data [ScWi12, § 3 Rn. 75], [Dammann in Simi11, § 3 recital 180].

Comprehensibility

The term "comprehensibility" of a process refers to the fact that all important steps of the process can be reproduced by an independent body.

Normative

A "normative" part of a document contains binding specifications and recommendations the implementation of which is also subject of an audit and certification process.

Patch Code

This is a specific bar code used for the automation of scanning processes which consists of differently wide, parallel bars and gaps.

Scanning

"Scanning" refers to the electronic recording of paper documents with the aim of electronic further processing and storage of the resulting electronic copy (scanned product).

Backup Data

"Backup data" is data objects which is used to protect the integrity and, if necessary, the authenticity of other data objects. In particular, this includes electronic signatures, time stamps, certificates, revocation information and evidence records (cf. "Credential" in [BSI-TR03125]).

Securing Measures

In this Technical Guideline, the term "securing measures" refers to backup data or security systems.

Security systems

"Security systems" are IT systems and/or applications which are used to protect the integrity and, if necessary, the authenticity of other data objects.

Availability

The "availability" of data, services, IT systems, IT applications or IT networks is given if they are available to the users in the required form within acceptable waiting times.

Confidentiality

"Confidentiality" means that information or data is prevented from being accessed and read in an unauthorised manner.

Negotiability

"Negotiability" refers to the possibility of being able to transmit documents and files from one system to another, in which the "quality" of the document as well as its integrity and authenticity remain verifiable.2

Completeness

"Completeness" means that the mutual reference of several data objects that are related due to an inner linkage is ensured.

References

[ASiC] ETSI: Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (AsiC); EN 319 162

[BfDI-TB-23] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [Federal Commissioner for Data Protection and Freedom of Information]: Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010 (23. Tätigkeitsbericht) [Activity report on data protection for 2009 and 2010 (23rd activity report)], 2011, http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23TB_09_10.pdf?__blob=publicationFile&v=6

[BfDI-TB-24] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [Federal Commissioner for Data Protection and Freedom of Information]: Tätigkeitsbericht zum Datenschutz für die Jahre 2011 und 2012 (24. Tätigkeitsbericht) [Activity report on data protection for 2011 and 2012 (24th activity report)], 2013, http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23TB_09_10.pdf?__blob=publicationFile&v=7

[BSI-100-2] Federal Office for Information Security (BSI): BSI-Standard 100-2: IT-Grundschutz Methodology, https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30758/standard_1002.pdf

[BSI-B 1.15] Federal Office for Information Security (BSI): IT-Grundschutz module M 1.15 – Deleting and destroying data, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01015.html

[BSI-GSK] Federal Office for Information Security (BSI): IT-Grundschutz Catalogues, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[BSI-IS-Rev] Federal Office for Information Security (BSI): Informationssicherheitsrevision, Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz [Information security revision, a guide for the IS revision based on IT-Grundschutz], https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v2_pdf.pdf

[BSI-M 2.46] Federal Office for Information Security (BSI): IT-Grundschutz safeguard S 2.46 – Appropriate key management, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02046.html

[BSI-TR02102] Federal Office for Information Security (BSI): Cryptographic Mechanisms: Recommendations and Key Lengths, BSI TR-02102, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[BSI-TR03116] Federal Office for Information Security (BSI): eCard-Projekte der Bundesregierung [eCard Projects of the German Federal Government], Technical Guideline (TR) of the BSI No. 03116, Part 1-2 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html

[BSI-TR03125] Federal Office for Information Security (BSI): Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR) [Preservation of Evidence of Cryptographically Signed Documents (TR-ESOR)], Technical Guideline (TR) of the BSI No. 03125, Version 1.1, 2011,

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

[BSI-TR03138-A] Federal Office for Information Security (BSI): Ersetzendes Scannen [Replacement Scanning] – Anlage A [Annex A]: Ergebnis der Risikoanalyse [Result of the Risk Analysis], Technical Guideline (TR) of the BSI No. 03138 (TR RESISCAN), Version 1.0, 2013

[BSI-TR03138-P] Federal Office for Information Security (BSI): Ersetzendes Scannen [Replacement Scanning] – Anlage P [Annex P]: Prüfspezifikation [Audit Specification], Technical Guideline (TR) of the BSI No. 03138 (TR RESISCAN), Version 1.0, 2013

[BSI-TR03138-R] A. Roßnagel, M. Nebel, O. Grigorjew, S. Jandt: Unverbindliche rechtliche Hinweise zur Anwendung der TR-RESISCAN [Non-Binding Legal Information in the Application of TR-RESISCAN], Version 1.1, 2013

[BSI-TR03138-V] Federal Office for Information Security (BSI): Ersetzendes Scannen [Replacement Scanning] – Anlage V [Annex V]: Exemplarische Verfahrensanweisung [Exemplary Process Instructions], Technical Guideline (TR) of the BSI No. 03138 (TR RESISCAN), Version 1.1, 2015

[CAdES] ETSI: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures, EN 319 122

[CC-P3-v3.1] Common Criteria: Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1, Revision 3, Final, http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf

[EGovG-MK] Bundesministerium des Innern (Referat O2) [German Federal Ministry of the Interior, department O2]: Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften [Mini Commentary on the Act to promote electronic government (E-Government Act - EGovG) as well as on the Amendment of other Regulations], http://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Artikel/Minikomment a_EGov_Gesetz.pdf

[HKM+98] P. G. Howard, F. Kossentini, B. Martins, S. Forchhammer, W. J. Rucklidge: The emerging JBIG2 standard, IEEE Transactions on Circuits and Systems for Video Technology, vol.8, no.7, pp. 838-848, 1998

[HüKo06] D. Hühnlein, U. Korte: Grundlagen der elektronischen Signatur [Basics of the electronic signature], Federal Office for Information Security (BSI) and SecuMedia Verlag, Bonn / Ingelheim, 2006, https://www.bsi.bund.de/DE/Themen/ElektrSignatur/esiggrundlagen.html

[ISO14492] ISO/IEC ISO/IEC 14492: Information technology - Lossy/lossless coding of bi-level images, International Standard, 2001

[ISO18014-1] ISO/IEC 18014-1: Information technology - Security techniques - Time stamping services - Part 1: Framework, 2008

[ITU-T.88] ITU-T T.88: Information technology - Lossy/lossless coding of bi-level images, 02/2000, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-T.88-200002-I!!PDF-E&type=items

[JaWi09] S. Jandt, D. Wilke: Gesetzliche Anforderungen an das ersetzende Scannen von Papierdokumenten [Legal requirements for replacement scanning of paper documents], K&R 2/2009

[NIST-800-57-1] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid: Recommendation for Key Management – Part 1: General (Revised), NIST Special Publication 800-57, 2007,

http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

[NIST-800-57-2] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid: Recommendation for Key Management – Part 2: Best Practices for Key Management Organization, NIST Special Publication 800-57, 2007, http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf

[NIST-800-133] E. Barker, A. Roginsky: Recommendation for Cryptographic Key Generation, NIST Special Publication 800-133, July 2011, http://csrc.nist.gov/publications/drafts/800-133/Draft-SP-800-133_Key-Generation.pdf

[PAdES] ETSI: Electronic Signatures and Infrastructures (ESI), PAdES digital signatures; EN 319 142

[RFC2119] S. Bradner: Key words for use in RFCs to Indicate Requirement Levels, IETF RFC 2119, via http://www.ietf.org/rfc/rfc2119.txt

[RFC3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF RFC 3161, via http://www.ietf.org/rfc/rfc3161.txt

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: Evidence Record Syntax (ERS), IETF RFC 4998, via http://www.ietf.org/rfc/rfc4998.txt

[RFJW08] A. Roßnagel, S. Fischer-Dieskau, S. Jandt, D. Wilke: Scannen von Papierdokumenten – Anforderungen, Trends und Empfehlungen [Scanning of Paper Documents - Requirements, Trends and Recommendations], “Der elektronische Rechtsverkehr” [Electronic Legal Transactions] Volume 18, Nomos 2008, ISBN 978-3-8329-3195-7

[RoNe14a] A. Roßnagel, M. Nebel: Simulationsstudie Ersetzendes Scannen, Ergebnisse [Simulation Study Replacement Scanning, Results], 30 January 2014, http://www.datev.de/portal/ShowContent.do?pid=dpi&cid=226590

[RoNe14b] A. Roßnagel, M. Nebel: Beweisführung mittels ersetzend gescannter Dokumente [Evidence using replacement-scanned Documents], Neue Juristische Wochenschrift (NJW) journal, 2014, p. 886 et seq. ISSN 0341-1915

[SGHJ12] A. Schumacher, O. Grigorjew, D. Hühnlein, S. Jandt: Die Entwicklung der BSI-Richtlinie für das rechtssichere ersetzende Scannen [The Development of the BSI Guideline for legally viable Replacement Scanning], Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) [Joint Symposium of Administrative Informatics] and Fachtagung Rechtsinformatik (FTRI) [Symposium of Legal Informatics] 2012, LNI 197, 2012, https://www.ecsec.de/fileadmin/Ecsec-files/pub//2012_FTVI.pdf

[XAdES] ETSI: Electronic Signatures and Infrastructures (ESI); XadES digital signatures; EN 319 132