Theoretical Considerations on Photo-Optical Measurement Data Registration Admissible as Evidence in Legal Metrology

Dr.-Ing. Marko Esche, Physikalisch-Technische Bundesanstalt, Abbestraße 2-12, 10587 Berlin, Germany
Manuel Schmidt, Physikalisch-Technische Bundesanstalt, Abbestraße 2-12, 10587 Berlin, Germany
Martin Nischwitz, Physikalisch-Technische Bundesanstalt, Abbestraße 2-12, 10587 Berlin, Germany
Marco Elfroth, Physikalisch-Technische Bundesanstalt, Bundesallee 100, 38116 Braunschweig, Germany
Stefan Heller, Technische Universität Berlin, Straße des 17. Juni 135, 10623 Berlin, Germany
Dr.-Ing. Markus Beermann, pixolus GmbH, Große Brinkgasse 2b, 50672 Köln
Dr.-Ing. Mark Asbach, pixolus GmbH, Große Brinkgasse 2b, 50672 Köln
Dr. Barbara Krausz, pixolus GmbH, Große Brinkgasse 2b, 50672 Köln
Marco Lierfeld, pixolus GmbH, Große Brinkgasse 2b, 50672 Köln

Abstract

The introduction of smart meters in legal metrology requires a smooth transition from the existing metering system into the digital world. Therefore, connecting legacy meters to the newly created digital backends is desirable to bridge the transitory phase of the rollout. To this end, the legal metrological framework of the European Union is analysed, and the resulting requirements are listed, which need to be fulfilled to allow for a legally valid digital registration of measurement values from legacy meters. Based on these requirements, threats on the process are derived and evaluated. In that framework, a prototypical implementation, utilizing photo-optical means, is presented, showcasing a system that potentially complies with all requirements. A risk analysis on the system illustrates the critical parts of the envisioned implementation and highlights what real-world implementations can improve upon.[1]

1 Introduction

In the European Union, Measuring Instruments Directive (MID) 2014/32/EU and Smart Metering Systems Roll-Out Recommendation 2012/148/EU (mirrored by the German Measures and Verification Ordinance [1] and the Metering Point Operation Act [2]) set out Europe-wide requirements for the operation of smart energy meters. Their main goal is to make energy consumption transparent to the consumer and thus improve energy efficiency. This economic sector of measuring systems subject to legal control, usually referred to as Legal Metrology, is responsible for a sizeable share of Germany's GDP [3]. Even though the rollout of smart meters is ongoing, several years will pass before smart metering replaces all 'classical' utility meters in Germany. Until such time, transitory solutions are needed to connect legacy utility meters to the digital metering infrastructure. These solutions could potentially enable users to retrieve measurement data admissible as evidence from legacy meters without having to resort to manual readouts. Since 'classical' active electrical energy meters for household use are not equipped with respective communication interfaces, there currently exists no trustworthy digital data transmission chain from the meter to the energy provider's backend where billing is performed. Instead, manual readouts by the consumer are widely accepted, although service personnel of the meter operator must manually repeat such readouts when in doubt. To close this gap by digital means, any solution needs to ensure that the remotely examined object is a real meter (instead of a fake), that it is the actual meter in question and that it conforms to legal requirements. In addition, it needs to be proven that the retrieved measurement value is up to date. Since the display is so far the only way to read out the accumulated consumption from legacy meters, only photo-optical solutions (e.g., camera app on a consumer device with image evaluation by a trusted server) offer a viable path to close the communication gap, see Figure 1 for an example. Similar challenges are posed by VideoIdent technology [4] used to authenticate consumers via video chat when validity and actuality of an ID document needs to be proven to sign contracts remotely.

In this paper, an analysis is conducted regarding requirements for measurement data retrieval by photo-optical means. The paper also investigates how conformity with the essential requirements of MID can be demonstrated for such a technology. To this end, a prototypical implementation to securely read a legacy meter's display via a smartphone camera is examined and mapped to the requirements of MID and BSI TR-03147 [4], which lays down requirements for VideoIdent solutions. The paper highlights with the help of an exemplary implementation how such a technology might be practically examined and how open issues (e.g., use of an unsecured smartphone, man-in-the-middle attacks) can be closed by means of a risk assessment [3] if certain prerequisites are fulfilled. It is also addressed how such an assessment may be used for different implementations and how a similar level of information security can be demonstrated. The remainder of the paper is structured as follows: Section 2 illustrates the legal framework for photo-optical measurement data registration and derives applicable security objectives. In the subsequent

[1] This work was financially supported by a grant (Verbundvorhaben eVIDENCE 03EI6025B) of the German Federal Ministry of Economic Affairs and Climate Action (BMWK).

Section 3, existing methods for photo-optical data registration are described and evaluated regarding their applicability for the examined scenario. Section 4 describes the theoretical application of one such method (namely VideoIdent following BSI TR-03147) and demonstrates how remaining open technical and organizational aspects of providing evidence of a measurement result can be closed. A prototypical implementation of the identified requirements is presented and evaluated in Section 5. Section 6 summarizes the paper and outlines further work.

2 Legal framework

In principle, all usage of measurement data for commercial or official transactions is subject to legal metrology legislation in Germany. This implies that the user of such measurement data must prove that the data can be traced back to a verified and correctly operated measurement instrument, see §33 in [5]. In case a measurement result is read by an untrusted third party e.g., the consumer, from a cumulative utility meter, proof of a correct readout can only be provided by spot checks of the actual accumulated measurement result on site. An alternative to this procedure is offered by so-called smart meters, where remote retrieval of the protected measurement result via a communication interface is enabled. For these results, which are transmitted via communication networks to the energy provider's backend for billing purposes, essential requirement 8.4 from Annex 2 in [1] applies, "Measurement data, software that is critical for measurement characteristics and metrologically important parameters stored or transmitted shall be adequately protected against accidental or intentional corruption." It follows that protection against accidental or intentional modification of the communicated data i.e., the measurement result, shall be ensured along the entire chain of communication. This implies that modifications shall either be impossible or at least detectable.
Although requirements from [2] will allow for cryptographic protection of data transmission in the long run, a transitory solution based on photo-optical digital measurement data registration shall be discussed here. The paper will highlight how a comparable level of protection can be demonstrated for such an alternative.

3 Overview of existing methods

In the following subsections, different technological solutions to the problem of measurement data retrieval from utility meters are described. These cover both solutions that require additional capabilities of the meter (see 3.2) and those that do not (see 3.1 and 3.3).

3.1 OCR-based measurement data registration

Optical character recognition (OCR) has been used in different fields of application for many years. A specific application to measurement data registration from legacy meters has been described in [6]. As detailed in Section 1, a consumer smartphone is used to register photo-optical data from a utility meter. The solution given by Harmon and Barker does not, however, focus on the admissibility as evidence of any registered data. Instead, they focus on the retrieval process regarding information for identifying instrument and measurement itself. In addition, the user of the smartphone is actively asked to confirm the accuracy of registered results which opens up the possibility of manipulation.

3.2 Measurement data retrieval via DLMS/COSEM

A description of an alternative method only applicable to smart meters equipped with compatible communication interfaces may be found in [7]. The DLMS (device language message specification) and COSEM (companion specification for energy metering) lay out a set of protocols for digital communication with utility meters and ancillary devices. Data exchange in DLMS/COSEM is modelled according to the well-known open system interconnection (OSI) model and divided into application, intermediate and physical layers. Any entity implementing the model must be realized as a physical device that supports one or more communication profiles such as HDLC or TCP/IP and is consequently uniquely identified by a physical address dependent upon the used profile. Compliant devices use a client-server model to realize connection-oriented communication, where meters act as servers, whereas the querying party acts as a client. Since legacy meters would need to be fitted with additional hardware, such as a communication adapter turning displayed values to digital information, to be able to communicate via DLMS/COSEM this does not represent a viable alternative for connecting legacy meters to digital backend systems quickly.

3.3 BSI TR-03147

In a different field of ensuring admissibility as evidence of registered photo-optical data, a method for remote identity validation of human individuals (VideoIdent) already exists and is frequently used to digitally agree to contractual obligations e.g., when signing purchase contracts online [8]. Specific requirements for implementations of this method in Germany were established by the German Federal Financial Supervisory Authority (BaFin) in 2017 [9]. These requirements were supplemented by a generalized technical requirement document for any kind of identity checking technology by the German Federal Office for Information Security (BSI) [4].

3.3.1 Security objectives of BSI TR-031047

In this context, the task of proving the admissibility of optically registered measurement data as evidence shows many similarities with the scenario addressed in [4]: Both in the case of natural persons and for legacy utility meters, the central challenge consists of authentication by means of optical characteristics alone. In this context, biometric data e.g., fingerprints, are also interpreted as optical characteristics.
In this context, BSI's technical guidance [4] formalizes the following generic security objectives:

- "S1.Existence: Existence of an entity (natural person) to which all claimed ID attributes apply."
- "S2.Legitimacy: All stated ID attributes apply to the natural person claiming them (implies S1. Existence)."
- "S3.Uniqueness: No two persons have identical values for all captured ID attributes."

For photo-optical retrieval, S1 translates to the existence of one measuring instrument to which the defined ID attributes e.g., metrological markings, serial number, physical seals and potentially the installation environment, apply. Due to the requirements laid down in [1], it is ensured that for a given valid ensemble of ID attributes, there exists one real instrument.
When applied to legacy utility meters, S2 implies that if verification markings, serial number and installation environment all match, the correct instrument has been identified. Regarding S3, the requirements of [1] (see §13 1) and §14) ensure that no two devices may have identical ID attributes as metrological markings must be clear, unique and not transferable to a different device. It follows that all three security objectives (see interpretation above) can be applied to the conditions provided by photo-optical measurement data registration. Moreover, all three objectives should be fulfilled by default by any verified utility meter.

3.3.2 Threats formalized to ID attributes

From the mentioned security objectives, [4] derives four distinct threats to the ID attributes themselves that need to be countered by any VideoIdent technology:

- "B1. Claimed ID attributes apply neither to the person claiming them nor to a different person."
- "B2. Successfully and correctly checked ID attributes become invalid […]."
- "B3. A person illegitimately uses the ID attributes of another person […]."
- "B4. Claimed ID attributes are valid for more than one person."

In the case of photo-optical measurement registration from a legacy utility meter, B1 translates to the threat posed by a fake meter whose markings etc. do not match any real measuring instrument. B2 can be specifically mapped to the validity checking of both the visually observed ID information and the actual measurement data. Threat B3 would correspond to moving ID information from the correct meter to another one, whereas threat B4 would describe an ID dataset fitting two different physical measuring instruments.

3.3.3 Additional threats

In addition to threats to the ID attributes, [4] specifies threats to the trustworthiness of ID documents, to the security of transmission channels and to the checking procedure of ID documents. Since ID attributes of measuring instruments are issued by accredited Notified Bodies, their trustworthiness should be ensured. If state-of-the-art signature and encryption algorithms are used, the security of transmission channels should also be much more difficult to breach than e.g., manipulating visual data prior to capturing. Therefore, the focus of the remainder of the paper shall be on the checking procedure of the ID attributes and on the threats for said attributes themselves, see Section 4. Regarding the checking procedure, [4] specifies the following threats:

- "B1. An ID document reported as stolen, lost or revoked is used."
- "B2. An expired ID document is used."
- "B3.A counterfeited ID document is used."
- "B4.A document with manipulated ID attributes is used."

Additional sections in [4] address the comparison process between ID document and natural person, the correct registration of ID attributes and safeguarding procedures for process integrity by the VideoIdent service provider. As visual ID markings of measuring instruments are physically attached to the individual device, a comparison process is not needed. The registration of ID attributes and retrieved measurement data in a backend system are beyond the scope of this paper and are already covered by existing certification for such systems if needed. Regarding safeguarding procedures for process integrity, [4] already states that these may be "ensured through technical measures, organisational measures or a combination of both." Since the objective of this paper is to describe and evaluate a purely technical solution that does not require modifications over time, process integrity assurance shall not be examined in the remainder of the paper. Section 4 will, therefore, focus on assessing threats B1 to B4 for ID attributes (henceforth referred to as BID1 – BID4) and threats B1 to B4 for the checking procedures (BCK1 – BCK4).

4 Application of BSI TR-03147

An advantage of photo-optical measurement data registration compared to VideoIdent technology lies in the availability of all necessary reference information (data on type label, verification markings, physical protection and securing measures) to the checking/receiving party prior to measurement data registration. BSI TR-03147 provides assessment guidelines for each requirement used to cover the previously introduced threats. The goal of such an assessment is to demonstrate that a certain level of assurance has been achieved. A similar method applicable for different IT solutions in legal metrology has been described in [3]. Following the logic of [4] the introduced threats will now be analysed to yield verifiable and assessable requirements which should enable assessment of arbitrary real implementations.

4.1 Analysis of threats to ID attributes

If ID attributes match no real utility meter (BID1), this does not cause any problems, since no false measurement data will be registered. Therefore, the threat does not require further investigation.
In legal metrology, already verified attributes may indeed become invalid (BID2) before they can be used. Since the time window between registering a measurement result with associated ID information and usage of the result i.e.,

writing it to a trusted database, is extremely short compared to the window one might have for capturing an image and submitting it for verification, this threat will be dealt with under the threat for usage of fully expired ID information, see BCK2 below.
Threat BID3 implies usage of another person's ID without authorization. When mapped to legal metrology, usage of a valid set of ID attributes together with the actual accumulated measurement value would not cause harm since the actual dataset would not be modified. Instead, one consumer would be submitting correct measurement data for a different consumer which might be problematic from a privacy standpoint but does not affect legal metrological requirements. Therefore, the threat does not require further examination.
With respect to cumulative utility meters, BID4 (attributes match more than one person) only applies to the ID attributes themselves since the measurement value can be identical across several meters without violating any requirements. Since conformity assessment of measuring instruments prior to their usage ensures that no two meters can have the same markings, matching attributes for more than one meter would always also imply manipulated ID information, which will be dealt with under threat BCK3 (see below).

4.2 Analysis of threats to checking procedures

Regarding threat BCK1 (lost/stolen ID used), it should be noted that verification markings are generally physically attached to the instrument. Loss is impossible, therefore. Moreover, forceful removal of verification markings with the intention of adding them to a different instrument would destroy the physical mark.
Threat BCK2 addresses usage of an expired ID. Since photo-optical data registration theoretically enables capturing of all ID attributes of a measuring instrument, it should always be feasible to also verify their temporal validity either through plausibility checks or by matching them with respective databases of verification bodies. However, since the current measurement value must also be communicated, there is no guarantee that no outdated value is transmitted. Therefore, the threat shall be examined here.
Similarly, threat BCK3 addresses counterfeited IDs. In principle, verification markings on an instrument and the legally relevant indication of the measurement result should be extremely difficult to manipulate since this threat pertains to all measuring instruments regardless of the manner of measurement data retrieval. However, since image capturing and processing open up additional possibilities for manipulation, the threat shall be investigated here.
With respect to BCK4 (manipulated ID used), the same argument holds as for BCK3. Specifically, BCK4 should also apply to the case of a manipulated measurement value together with a true set of ID attributes since assignment of false measurement values to real ID attributes can also be seen as manipulation. Therefore, threats BCK2, BCK3 and BCK4 shall be examined together in Section 5.

5 Prototypical implementation

Based on the identified applicable threats from [4], Section 5.1 will derive a set of technical prerequisites that any implementation will have to realize. These are then used in Section 5.2 to construct a generic implementation that is close enough to an actual product description for evaluation without being overly restrictive in its applicability to different use cases. As indicated in Section 4, [4] already implies the possibility of proving fulfilment of its requirements by means of a risk assessment, which yields a certain assurance level. A brief except from such an assessment for the prototypical implementation will be shown in Section 5.3

5.1 Requirements derived from applicable threats

Usage of an expired ID (BCK2) can only be detected if some sort of trustworthy time reference is used. This could either be generated by a trusted source or provided by the (trusted) checking entity itself. To enable detection of counterfeited ID markings or manipulated measurement results (BCK3) two different preconditions need to be met: Firstly, a known reference for the markings themselves must be available to the checking entity. Regarding the checking procedure for the measured value itself, there must either be a detection process in place to detect forgeries or forging a correct result must be made too difficult for the anticipated attacker to realize. Both mechanisms would also automatically mitigate threats posed by a manipulated ID (BCK4).

5.2 Implementation description

The following generic implementation for a photo-optical measurement data retrieval system admissible as evidence is based on the assumption that a trustworthy backend exists which provides a time reference and is able to perform necessary checks on submitted data/images. A description of all components that are part of the implementation is given below. For each component, the basic assumptions regarding their capabilities are also detailed.

5.2.1 Component description

As described in Section 1, a smartphone shall act as the optical sensor to capture digital photos of legacy meters. Since the phone will usually be a standard consumer device, it is assumed that the device will not necessarily reply correctly to external commands and that it may even maliciously insert wrong data into the communication channel. Regarding said channel as an intermediary between smartphone and backend, it is again assumed that it cannot be relied upon to behave correctly. This includes the capability to inject false or duplicate data packets and to delete data packets or delay them arbitrarily.
The backend as the third party, however, is assumed to be properly certified according to legal requirements (see [5]) and to be operated in a verified state that is regularly subject to market and user surveillance. Therefore, the

ISBN 978-3-8007-5835-7

backend can act as a trust anchor both for providing a reliable time reference for the actions of all other parties and for performing necessary checking procedures for received data packets/images.

5.2.2 Component interaction

All communication described below shall be signed using state-of-the-art cryptographic signatures to ensure that no other parties besides the ones introduced in Section 5.2.1 can practically influence transmitted data packets. It is assumed that the corresponding cryptographic certificates have been exchanged between smartphone and backend prior to initiation of the following steps. To address the requirements derived for the prototypical implementation in Section 5.1, the following protocol (see **Figure 1** for an abstract UML representation) shall be observed regarding correct component interaction:

Whenever a consumer wishes to register her current meter reading with the energy company's backend, she triggers a cryptographically signed request from her smartphone. The signed request is sent via the communication channel to the backend which checks the signature and creates a (random) one-time token. This token and a current timestamp are again cryptographically signed by the backend and sent back to the smartphone via the communication channel.

Upon reception of this data packet, the smartphone takes a picture/video of the utility meter and embeds the data of the token in the picture as a watermark. This (random) watermark serves the dual purpose of ensuring that the phone cannot prerecord the image and that the obtained image shows a real utility meter. The actual implementation of adding the watermark is not the subject of this paper, but several options such as a zooming sequence (in/out) controlled by the one-time token to check that the captured object has three dimensions, activation of the smartphone's flashlight according to the one-time token or even camera movements controlled by the token (up/down) seem feasible. Although the latter would require additional user interaction. Afterwards, the watermarked picture/video is transmitted to the backend for checking and registration.

The backend then checks whether the smartphone's response was within preassigned time limits and whether the correct watermark corresponding to the one-time token has been embedded in the captured image. In addition, a check is performed on the recognized verification markings of the meter, which are matched against an internal trusted database, and the cumulative measurement value is finally extracted from the image and registered with the backend. The registered measurement result is then sent back to the smartphone for information purposes and to indicate completion of the protocol to the consumer.

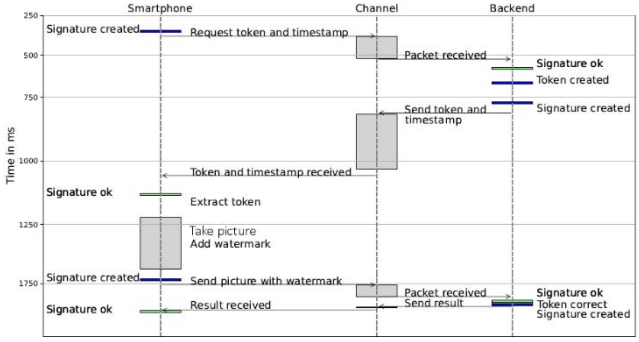

Figure 1 UML flowchart for adding a secure watermark to captured pictures

5.3 Risk analysis

To demonstrate that the applicable threats BCK2, BCK3 and BCK4 from Sections 4.1 and 4.2 are adequately addressed by the implementation, a brief exemplary risk analysis following the method from [3] shall now be performed.

5.3.1 Method description

To this end, attack vectors are identified which can be used to implement one or more threats. Depending on whether an attack vector affects one or more registered measurement results, it is assigned an impact value of 1/3 or 1. The attack vectors are then rated according to a point scoring system with respect to the estimated time and expertise required to implement an attack, the necessary knowledge regarding the target of evaluation (TOE), the needed window of opportunity (if any) and the necessary equipment. Since the scoring part of the method from [3] is based on the vulnerability analysis from ISO/IEC 18045 [10], a more detailed description of the point scores and examples regarding their assignment may be found there.

The sum score is then turned into a probability score by means of the mapping provided in **Table 1**.

Table 1 Mapping of sum score to TOE resistance and probability score [3]

Sum of Points	TOE Resistance	Probability Score
0-9	No rating	5
10-13	Basic	4
14-19	Enhanced Basic	3
20-24	Moderate	2
>24	High	1

Multiplying impact and probability finally yields the risk score [3]. For real-world implementations, a full risk analysis based on the attack probability trees from [3] would be needed to identify as many ways of realizing the applicable threats as possible. Since the analysis here is only focused on a generic prototypical solution, only a limited number of attack vectors shall be examined for illustration purposes.

ISBN 978-3-8007-5835-7

5.3.2 Attack vector description

Potentially, all three threats (BCK2, BCK3 and BCK4) could be realized by attacks that need to be repeated for each measurement value. This would result in a reduced impact score of 1/3. In order to also cover attacks targeted at implementing a solution that works automatically for all future measurement values to be registered, two versions of each threat shall be investigated here i.e., one with full and one with reduced impact each. These are represented as 'BCKx all' and 'BCKx one' in **Table 2**.

In the following, a limited number of exemplary attack vectors is described. In a full risk assessment, this list would be much more extensive, see Section 5.3.1. Nevertheless, the exemplary attack vectors should suffice to illustrate how coverage of the applicable threats from BSI TR-03104 [4] can be illustrated:

- AV_STI: A sticker showing a fake measurement value is individually printed and glued over the display of the meter.
- AV_REP: An attacker manually replaces the displayed measurement value in the captured image within the timeframe allowed by the backend.
- AV_FOR: An attacker manually forges ID attributes and adds them to a photo of an unverified manipulated meter.
- AV_ALT: An attacker writes a software that digitally alters an outdated photo of a real meter to comply with the token data transmitted by the backend.
- AV_FAK: An attacker writes software that generates a photo of a fake meter that complies with the token data transmitted by the backend.

5.3.3 Risk estimation and evaluation

In **Table 2** these attack vectors are now assigned to the identified threats which they implement. Each realized threat is finally assigned point scores according to the categories introduced in Section 5.3.1.

Threat 'BCK2 all', for example, may be realized by writing a software that automatically alters outdated photos according to the transmitted token data. Depending on the complexity of imprinting the token in the image, this will require around half a year (score of 17 for elapsed time), whereas only a programming expert can write such a software (score of 6 for expertise). Since the knowledge regarding token and watermark should be well protected, the information would be considered sensitive (score of 7 for knowledge of the TOE). As the attack can be realized without physical access to any verified components i.e., the backend, the window of opportunity is unlimited (score of 0). Finally, the software development environment used would count as standard equipment (score of 0). According to **Table 1**, the resulting sum score of 30 translates to a probability score of 1. Once multiplied with the assigned impact of 1 this produces a risk score of 1.

Threat 'BCK4 one', as another example, requires printing of a sticker label that mimics the real display. Such a printout can be generated within minutes (score of 0 for elapsed time) by a layman (score of 0 for expertise). No special knowledge regarding the TOE is required since images of utility meters can be publicly downloaded from the internet or simply obtained on site (score of 0 for knowledge). Since a printer can be considered standard equipment, the last score is 0, too. From **Table 1**, a probability score of 5 follows, which is only reduced to a risk of 2 since the product of impact and probability score is rounded to the next integer number.

Table 2 Each attack vector (AV) is evaluated based on estimated time (ET), Expertise (Ex), Knowledge of the TOE (KT), the window of opportunity (WO), needed equipment (Eq). The resulting sum score is turned into a probability score (PS), which is then multiplied with the impact (I) to calculate the risk.

T	Description	I	AV	ET	Ex	KT	WO	Eq	Σ	PS	Risk
BCK 2 one	An attacker manages to register an expired set of measurement value and valid ID attributes.	1/3	AV_REP	0	6	7	10	0	23	2	1
BCK 2 all	An attacker registers an unlimited number of sets of expired measurement values and valid ID attributes.	1	AV_ALT	17	6	7	0	0	30	1	1
BCK 3 one	An attacker manages to register a measurement value together with fake ID attributes.	1/3	AV_FOR	0	6	3	0	0	9	5	2
BCK 3 all	An attacker registers an unlimited number of measurement values together with fake ID attributes.	1	AV_FAK	19	6	0	0	4	29	1	1
BCK 4 one	An attacker manages to register a measurement value together with manipulated ID attributes.	1/3	AV_STI	0	0	0	0	0	0	5	2
BCK 4 all	An attacker registers an unlimited number of measurement values together with manipulated ID attributes.	1	AV_ALT	17	6	7	0	0	30	1	1

Similarly, scores in the individual categories for the remaining threats can be assigned. The resulting risk scores

ISBN 978-3-8007-5835-7

between 1 and 2 would all be acceptable for legal metrology, where countermeasures are only required if a risk score of 4 or higher is obtained. However, the pivotal role of elapsed time for all automated attacks (see threats marked as 'BCKx all' in **Table 2)** must be stressed here. The time scores for AV_ALT and AV_FAK are based on the assumption that it is extremely difficult and time-consuming to write a software that either manipulates an existing photo according to the token data or to fake a photo altogether. If the algorithm of embedding the token data is very simple, however, the time scores could, for instance, be reduced to 1 (less than a week) which would increase the resulting risk score to 4 in both cases. It follows that during evaluation of any real implementation, particular care must be given to analyzing as many potential attack vectors as possible and designing relevant countermeasures where necessary. Overall, the risk assessment method offers the possibility of comparing the protection level realized by different photo-optical capturing solutions.

6 Summary and further work

In this paper, the challenges posed by connecting legacy utility meters to the smart metering infrastructure have been outlined. Based on an overview of technologies that could act as transitory solutions before the widespread roll out of smart meters, the requirements for the VideoIdent technology were examined in more detail and it was investigated how they could be used to demonstrate compliance with legal metrological requirements. It has also been shown which threats need to be addressed by any photo-optical capturing solution to be used for registration of measurement data admissible as evidence. The risk assessment methodology from [3] was applied to the identified threats to illustrate how a comparability of the protection level achieved by different implementations could be demonstrated. Currently, no certified solution to the investigated problem exists, nevertheless the combination of requirements from BSI TR-03147 [4] and methodology from software risk assessment [3] will likely provide the tools necessary for examination and evaluation of such a technology. Further work will, therefore, focus on generating a more extensive list of feasible attack vectors to be considered during evaluation of the technology and on integrating the risk assessment process into the overall conformity assessment procedure required by the legal framework [1].

7 Literature

[1] Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung (MessEV), Federal Law Gazette, Volume 2014 Part 1 No. 58, December 2014, last modified on May 12, 2021

[2] Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (MsbG), Federal Law Gazette, Volume 2016 Part 1 No. 43, August 2016, last modified on July 16, 2021

[3] M. Esche, F. Grasso Toro and F. Thiel, Representation of attacker motivation in software risk assessment using attack probability trees, 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), 2017, pp. 763-771, doi: 10.15439/2017F112

[4] Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons, Federal Office for Information Security, Bonn, Version 1.0.4, December 2018

[5] Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (MessEG), Federal Law Gazette, Volume 2013 Part 1 No. 43, July 2013, last modified on June 9, 2021

[6] B. Harmon, T. Barker, Optical character recognition (OCR) and coded data for legacy instrument data transfer (US Patent No. 20170116493) U.S. Patent and Trademark Office, 2017

[7] DLMS/COSEM Architecture and Protocols, DLMS User Association, Edition 8.3, June 2017

[8] N. Pohlmann, J.-H. Frintrop, R. Widdermann, T. Ziegler, Wenn der Softbot menschliche Identität bestätigt. Videoident-Verfahren II: Die Technik, Die Bank, No. 6, 2018, pp. 66-70,

[9] Bundesanstalt für Finanzdienstleistungsaufsicht (Hg.) (2017): Rundschreiben 3/2017 (GW) – Videoidentifizierungsverfahren

[10] ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation, International Organization for Standardization, Geneva, CH, Standard, August 2008