

Evaluation of Time Synchronization Mechanisms in Legal Metrology

Dr.-Ing. Marko Esche¹, Dipl.-Ing. Felix Reichmuth¹, Dipl.-Inf. Reinhard Meyer¹, Martin Nischwitz¹, M.Sc.

¹ Physikalisch-Technische Bundesanstalt, Fachbereich 8.5 „Metrologische IT“, Abbestraße 2-12, 10587 Berlin

Abstract

To ensure correct billing in case of dynamic tariffs, measuring instruments subject to legal control must be able to correctly obtain legal time from an authenticated source. Typically, each EU member state designates one institution for distributing legal time locally. Several technical implementations for time synchronization are introduced and discussed in this paper. They are evaluated using a harmonized risk assessment approach based on ISO 18045 vulnerability analysis. Results indicate that protection for high-risk scenarios, e.g., critical infrastructure, can be ensured via state-of-the-art cryptographic protocols or by combining different synchronization mechanisms. Based on the results of the assessment, recommendations for the practical usage of the different implementations are made.

Keywords: legal metrology, network time protocol, dynamic tariffs, electric vehicle supply equipment, software risk assessment.

Introduction

In the European Union, certain types of measuring instruments used for commercial transactions are subject to legal control under the Measuring Instruments Directive (MID) [1]. These include widely used instruments such as active electricity meters, gas meters, taximeters, length measuring devices and automatic weighing instruments. The central aim of the MID is to ensure consumer protection through provision of fair and traceable measurements.

Since 2024 the EU legislative bodies have been working towards an amendment of the MID to extend its scope to electric vehicle supply equipment (EVSE) and dispensers for compressed gases [2]. Both are seen as instruments crucial for facilitating the transition from fossil fuels to green energy sources. Given the volatile nature of renewable electrical energy in particular, many EU member states are already experiencing the advent of new and dynamic, i.e., time-dependent, pricing schemes for electrical energy supply, including EVSEs, replacing classical fixed-price schemes known from fuel dispensers. While these pricing schemes will allow users to profit from cheaper energy when solar or wind power are available in abundance, they also pose new challenges for the measuring instruments manufacturer,

with the necessity to create a direct link between measured quantity and applicable price at a given time [3]. Such time-dependent tariffs necessitate that measuring instruments have access to a trustworthy and reliable source of legal time to ensure correct application of varying prices.

Given that MID Annex I requires measuring instruments, including their software, parameters and data, to be adequately secured and protected against manipulation [1], protection means for these assets now have to be extended to cover mechanisms for time synchronization as well. This extension poses new challenges for the legal metrology community since time information is inherently dynamic as opposed to static binary information typically communicated between components of a measuring system.

In this paper, the prevalent time synchronization mechanisms are investigated and assessed regarding their suitability for fulfilling the essential requirements of MID [1]. Based on the outcome of the assessment, recommendations are made to ensure MID-compliant implementation and usage of time synchronization mechanisms for legally regulated measuring instruments.

The remainder of the paper is structured as follows: In the next Section, a short analysis of

the legal requirements for time synchronization in measuring instruments is given. Afterwards, the available time synchronization mechanisms for measuring instruments are introduced and discussed, including several remarks regarding their practical usage and associated security aspects. Subsequently, the risk assessment methodology used in this paper is presented and applied to the different time synchronization mechanisms. Based on the outcome of the analysis, the final Section draws a number of conclusions and makes recommendations regarding the legally relevant usage of time synchronization.

Requirements Overview

As mentioned in the introduction, MID Annex I lays down generic essential requirements applicable to a large range of measuring instruments. By means of the annex, MID aims to establish a common level of consumer protection and trust in measurements conducted for commercial transactions. Amongst the requirements from Annex I, number 8.4 directly addresses IT-related assets, "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." [1] From this essential requirement it can be concluded that measurement data must be secured and protected against attacks, whereas adequacy of the securing and protection means can be demonstrated by means of a mandatory risk assessment, see MID Annex II.

Whenever measurement data are combined with time information, e.g., for assigning different tariffs to measured quantities, the essential requirements need to be extended to the time information, too. This is typically achieved by requiring the measuring instrument's internal clock to have a maximum drift compared to legal time, e.g., 3% of a billing interval, corresponding to 9 seconds for quarter-hourly tariff changes. In addition, setting of the clock must be adequately protected and secured, see clause 6.2.7.1 in [4]. Since time information, as opposed to most other measurement data, must be processed immediately, a bidirectional setup between time source and measuring instrument is typically used, in which all changes to the setup are protected and secured to provide evidence of intervention for later checks by market or user surveillance authorities.

Time Synchronization Mechanisms

Since 1985 the network time protocol (NTP) [5] has been used to automatically synchronize network-connected devices all around the world. The protocol uses time-stamped UDP messages to allow NTP clients to calculate round-trip times and individual time offsets compared to an NTP server. Because of the reliance on UDP and due to the lack of an authentication mechanism within that protocol, it is potentially susceptible to a man-in-the-middle attack (MITM) which could endanger compliance with the essential requirements from MID. The international organization of legal metrology (OIML) addressed this issue in its latest version of the OIML Document D 31 "General requirements for software-controlled measuring instruments", see clause 6.2.7 in [4]. Notably, the NTP protocol does not provide any proof of identity or authentication mechanism for the time source and relies on a low-latency bidirectional communication channel to ensure proper functioning of the synchronization mechanism.

In 2020, the network time security protocol (NTS) [6] was published, extending NTP with cryptographic security for client-server communication. The protocol consists of two main phases: During the key establishment phase, an encrypted communication channel with a trusted key server is established via TLS and TCP. During this stage, so-called NTS-cookies are shared with the client to ensure that both parties can properly authenticate each other during the second phase by means of the authenticated encryption with associated data (AEAD) mechanism. During the second stage, NTP with a cryptographic extension in the NTS cookie placeholder extension field is used. This field is added to the NTP packets, allowing clients and servers to check each other's identity. At the same time, clients can request new cookies with this extension, whereas servers can monitor the state of the synchronization and issue new NTS cookies when needed. In theory, the NTS key establishment only must be carried out once. It should also be noted that key server and NTP server can be operated separately, putting lower strain on network resources. Practical aspects of the protocol will be discussed during risk assessment and subsequent analysis. When compared to simple NTP, NTS poses additional demands on client devices in particular: For establishment of the TLS connection, cryptographic certificates and keys must be properly handled. Additionally, mechanisms for the correct usage of the

aforementioned NTS cookies have to be implemented in each client.

In Germany, a historical alternative is still the DCF77 transmitter which is physically located in Frankfurt/Main, Germany and continually transmits an analog time signal at a frequency of 77.5 kHz [12]. The base frequency of the signal acts as a frequency normal and is directly fed via a fiber-optical link from the official atomic clocks at the Physikalisch-Technische Bundesanstalt (PTB) Braunschweig, Germany's national metrology institute, which is tasked with distributing legal time in Germany. In addition, phase- and amplitude-modulated information is contained in the signal to enable receivers to decode minute, hour, calendar day, number of the month and year. Given the unidirectional nature of the analog signal, it does not contain any authentication or integrity protection mechanisms. How manipulation of the analog signal can be mitigated nonetheless will be discussed during the following risk assessment.

Risk Assessment

To enable conformity assessment bodies and manufactures of measuring instruments to evaluate the suitability of the implemented securing and protection mechanisms in a measuring instrument, the European Cooperation in Legal Metrology has harmonized a risk assessment methodology in WELMEC Guide 7.6 [8]. The method is based on an original publication by PTB from 2015 [8] and consists of three main stages:

During risk identification potential threats to assets are identified. In the scenario discussed here, such a threat could be formulated in the following manner: An attacker manages to manipulate the internal clock of a measuring instrument without evidence of intervention.

During risk estimation, technical steps needed to realize a threat are investigated and assigned specific point scores making use of ISO 18045 vulnerability analysis [11]. The point scores aim to quantify the resources necessary to implement an attack vector and are divided into the following categories: time required (0 for less than a day to 19 for at least half a year), necessary expertise (0 for a laymen to 9 for an expert in multiple fields), required knowledge of the target of evaluation (0 for public information to 11 for critical data), window of opportunity (between 0 for unlimited or unnecessary access to 10 for severely restricted access) and equipment needed (0 for standard to 9 for multiple bespoke equipment). After having

assigned these scores to an attack vector, a sum score can be calculated which in turn is mapped to a probability score according to Table 1.

Tab. 1: Mapping between sum score, resistance to attacks and probability score. [10]

Sum of point scores	Resistance to attacks	Probability score
0-9	no rating	5
10-13	basic	4
14-19	enhanced basic	3
20-24	moderate	2
>24	high	1

The probability score is then multiplied with the assigned impact ($\frac{1}{3}$ for attacks on single measurements, 1 for attacks on multiple measurements) to yield the final risk score.

Finally, the risk score is put into the context of the instruments usage during risk evaluation.

The method was later extended in [9] to allow for the inclusion of attacker motivation in risk assessment. To deal with complex attacks requiring multiple steps, attack probability trees were introduced in [10]. These attack probability trees are graphical representations of an attack and potential subgoals signified by a root node with linked child nodes. A visual example of an attack probability tree with one parent node and two child nodes may be found in Figure 3. In [10] it was proven that any attack probability tree can be represented as a binary tree which enables assessors to assign point scores to the leaf nodes alone. Following rules defined in [10], these point scores can then be propagated up the tree to calculate the risk of the root node and its associated threat.

The results of such a risk assessment can then be used to identify potential countermeasures to said attack vectors. In this paper, a generic architecture of an EVSE and its environment is used to identify potential attack vectors and influence factors for time synchronization, see Figure 1. The EVSE is assumed to contain an EVSE measuring system (EVSE-MS) which is subject to legal control. Typically, the EVSE-MS contains a separately certified active electrical energy meter which calculates measurement data, provides time stamps for beginning and end of a transaction and cryptographically signs the resulting charge data record. Other software

modules or hardware components, both legally relevant or legally non-relevant, may also be part of the EVSE-MS.

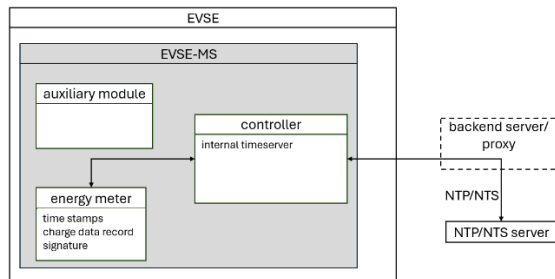


Fig. 1: Generic architecture of an EVSE and its environment. The measuring system of the EVSE (EVSE-MS) creates time-stamped, cryptographically signed charge data records, while the charge point management system (CPMS) acts as a transparent tunnel to the network time security (NTS) server used for distributing legal time.

To obtain valid time information, the EVSE-MS communicates with a pre-established time source, e.g., time servers provided by PTB, and sets the energy meter's internal clock accordingly. If NTP or NTS are used, setting does not occur abruptly but is done in incremental steps to ensure proper functioning of the meter's operating system. In the following, all three time-synchronization mechanisms are examined separately, and the applicable attack vectors are assigned their proper point scores.

DCF77

If the analog DCF77 is used, two potential attack paths appear to be viable: Either an attacker blocks the time signal altogether, which will eventually lead to uncontrollable drift of the internal clock or a sufficiently strong fake signal is provided. Since arbitrary drift of the clock is unlikely to profit a potential attacker, only the latter scenario is examined: Potentially, one could record the time signal and reuse it to artificially increase the duration of a charging session or to assign daytime session to more costly nighttime prices. The equipment needed to capture and retransmit such a signal will have to be specifically built for the purpose (point score of 7) and will require an electronics engineer (point score of 6 for expertise) at least a few days (point score of 2 for time). At the same time, all necessary data can be found readily online, and the attack itself does not require physical access to the EVSE itself.

Instead, the fake time signal generator simply must be put in the vicinity of an EVSE, thus potentially also being able to manipulate multiple instruments and charging sessions simultaneously (impact score of 1). The resulting attack probability tree consisting of a single root node is given in Figure 2.

A01: False time source DCF77	
Ti: 2	WO: 0
Ex: 6	Eq: 7
Kn: 0	Σ : 15

Fig. 2: Attack probability tree consisting of a single root node addressing manipulation of measuring instruments using DCF77 time synchronization. The node is assigned scores for time (Ti), expertise (Ex), knowledge of the device (Kn), needed equipment (Eq) as well as the window of opportunity (WO). Additionally, the sum score (Σ) for the attack is given.

The sum score of 15 results in enhanced basic protection (risk score of 3) for the configuration, see Table 1. To ensure adequate protection against manipulation, a secondary time source like NTP could be used to mitigate the attack and reduce the risk of manipulation even further.

NTP

If the network time protocol is used, a trusted source must be configured during initial installation of the EVSE. Since this process is subject to a separate conformity assessment module, one can assume that the NTP server address is configured correctly at initial startup and that a correct time signal is received at least once. During use of the instrument, however, this will not necessarily hold true. To install a false time source (see Figure 3), an attacker would need to set up a false NTP server (child node A12 in Figure 3) and redirect NTP traffic via a manipulated proxy (child node A13).

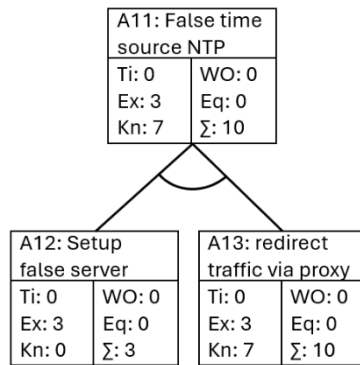


Fig. 3: Attack probability tree for an attack on an NTP-synchronized measuring instrument by setting up a fake time server (A12) and manipulating NTP traffic via a proxy (A13).

Once these scores have been propagated up the tree to the root node A11, a sum score of 10 is obtained, which is equivalent to a probability score of 4. Since the manipulated NTP server would simultaneously affect all measurement results of the attacked EVSE (impact score of 1), the overall risk score has a value 4 as well. Compared with the usage of the analog DCF77 signal, it should be clear that a higher risk of manipulation exists in this scenario.

NTS

To mitigate the shortcomings of NTP, the NTS protocol was introduced by IETF in 2020. With NTS, protection of time information is reliant on two factors: the strength of the cryptographic primitives used for TLS and AEAD in the two protocol phases and the protection of the corresponding cryptographic material used in the measuring instrument. Since TLS uses state-of-the-art RSA or elliptic curve cryptography (ECC) with typical key lengths of 4096 bits for RSA and 256 bits for ECC, attacks on this part of the NTS protocol would realistically take several years on the world's best supercomputers, rendering an attack virtually impossible. According to [6], server and client can negotiate the encryption algorithm used for AEAD, but it is typically AES with a minimum key length of 128 bit. This is again state of the art and extremely difficult to break. Thus, attacks on the protection of the instrument and its cryptographic certificates are much more likely and will be examined here.

To falsify an NTS time source, an attacker would first need to set up an alternative NTS server, see node A22 in Figure 4. Since new certificates would be necessary for such a false

server, these need to be created and introduced into the instrument to be attacked, see node A23. Since setup of NTP and NTS servers are almost identical tasks, typically involving the same open-source Linux package chrony, and redirection of traffic can be realized similarly in both scenarios, the child nodes of A22 are identical to those of node A11 in Figure 3. To introduce false cryptographic certificates into the target measuring instrument, an attacker first needs to generate a false certificate (node 26) and install it in the instrument (node 27). Since certificates are complex configuration files but do not contain any executable code, they are usually interpreted as device-specific parameters of a measuring instrument. This implies that they are protected and secured against exchange and that any modification of the registered certificates is logged in an audit trail.

Since the certificate of the NTS server typically changes on a yearly basis, the corresponding root certificate is usually installed in the measuring instrument instead. This means that for a successful attack, an expert (score of 6) would need to set up their own certificate chain, starting with a fake root, which will take at least a day (time score of 1). Since this does not require any access to the targeted device and can be done with freely available software like OpenSSL, all other scores can be set to 0, see node 26 in Figure 4. The more challenging part for any attacker would be installing the fake certificate on the target device, see node 27. To achieve this on a device with a properly configured operating system, an attacker would likely need to find a loophole in the device's firewall and then use privilege escalation via a vulnerability in one of the operating system's modules. Again, this will require a software expert at least a few days (time score of 1) and will also require sensitive knowledge of the target system (knowledge score of 7). Moreover, the attacker will likely have to develop their own attack tool, making it a bespoke equipment (score of 7) from the point of view of ISO 18045 [11]. Since all parts of the attack on NTS can be done remotely and would affect all future measurements performed by one or more devices, the window of opportunity is unlimited (score of 0) and the impact would be set to 1. Once the scores for the leaf nodes have been propagated up the tree, this results in a sum score of 21 for the root node, an attack probability score of 2 (see Table 1) and an equivalent risk score of 2. This means that the method offers at least moderate protection and

fulfils requirements from WELMEC Guide 7.6 for all risk classes.

Analysis and Conclusions

Based on the results of the risk assessment, recommendations can be made regarding the secure and MID-compliant configuration of time synchronization mechanisms for EVSEs. As can be seen from the total risk scores for the three different synchronization mechanisms, DCF77 offers medium protection against manipulation simply by making the attack itself hardware resource intensive.

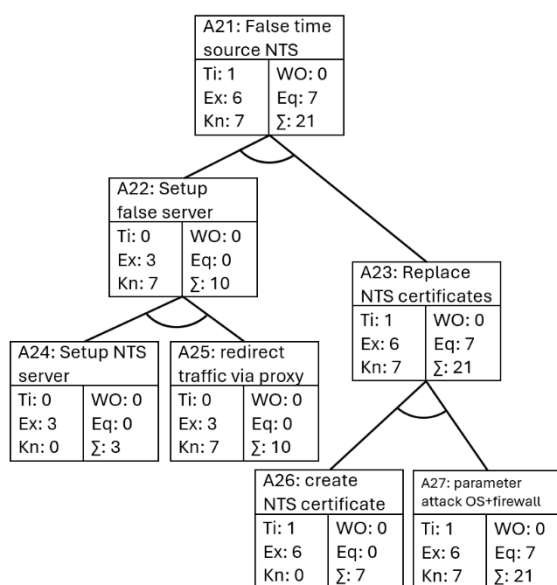


Fig. 4: Attack probability tree for an attack on a NTS-synchronized measuring instrument by setting up a fake time server (A22) and modifying the installed certificates on the device accordingly (A23). Both child nodes are further subdivided.

If combined with a second unauthenticated synchronization mechanism for plausibility checking, DCF77 will likely remain an adequate technical means for the foreseeable future for all WELMEC risk classes. However, compared to the other two network-based solutions, it does require the manufacturer to realize a specific hardware configuration in their device (temperature-controlled real time clock, analog

radio receiver). These are likely to stop most parties from pursuing this solution.

NTP, by comparison, is already available in most common embedded devices via their operating system. It does not require an expensive RTC on the client side, if synchronizations with the server occur sufficiently often. However, it does not offer sufficient protection against manipulation and attacks could potentially affect many devices and measurements.

NTS should be an acceptable alternative for most use cases. While the cryptographic strength of the protocol and its different phases is well known, this has to be supported by proper configuration of the client's operating system to ensure adequate protection of the associated cryptographic material.

In this regard, OIML D 31 and other requirement documents still appear to provide insufficient guidance on the handling of cryptographic material needed for usage of time synchronization mechanisms, specifically in the context of MID requirements for prevention of inadmissible modifications.

It is anticipated that the evaluated time synchronization mechanisms should cover a significant portion of EVSE models currently in use. For other types of measuring instruments that use legal time, e.g., smart utility meters for electrical energy, gas, water, or thermal energy, requirements are typically less strict since the supplied customer does not change frequently, and billing does not need to be done in real time. Subsequently, a combination of DCF77 and NTP as a standalone mechanism should be acceptable in this scenario. In Germany, the Federal Office for Information Security (BSI) prescribes the usage of NTS for such meters. How to safely commission NTS client devices without the need for manual checks of the installed certificates remains a task for future work.

References

- [1] EC, "Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments," European Union, Council of the European Union; European Parliament, Directive, February 2014

- [2] EC, "Measuring instruments", [Online]. Available: "https://single-market-economy.ec.europa.eu/single-market/goods/building-blocks/legal-metrology/measuring-instruments_en" [Accessed 21 November 2025].
- [3] "OIML G22 Electric Vehicle Supply Equipment (EVSE)," International Organization of Legal Metrology, Paris, France, Tech. Rep., 2022
- [5] D. Mills, U. Delaware, E. J. Martin, J. Burbank and W. Kasch, "RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithm Specification", [Online]. Available: <https://tools.ietf.org/html/rfc5905>. [Accessed 4 May 2020].
- [4] "OIML D31 General requirements for software-controlled measuring instruments," International Organization of Legal Metrology, Paris, France, Tech. Rep., 2023.
- [6] D. Franke, D. Sibold, K. Teichel, M. Dansarie and R. Sundblad, "RFC 8915 - Network Time Security for the Network Time Protocol", [Online]. Available: <https://tools.ietf.org/html/rfc8915>. [Accessed 13 February 2025].
- [8] "WELMEC Guide 7.6: Software Risk Assessment for Measuring Instruments", WELMEC, 2021.
- [8] M. Esche and F. Thiel, "Software risk assessment for measuring instruments in legal metrology," in Proceedings of the Federated Conference on Computer Science and Information Systems, Lodz, Poland, September 2015, pp. 1113–1123
- [9] M. Esche, F. Thiel „Incorporating a Measure for Attacker Motivation into Software Risk Assessment for Measuring Instruments in Legal Metrology“, 18. GMA/ITG-Fachtagung Sensoren und Messsysteme, Nuremberg, Germany, May 2016, doi: 10.5162/sensoren2016/P7.4
- [10] M. Esche, F. Grasso Toro, and F. Thiel, "Representation of attacker motivation in software risk assessment using attack probability trees," in Proceedings of the Federated Conference on Computer Science and Information Systems, Prague, Czech Republic, September 2017. doi: 10.15439/2017F112 pp. 763–771.
- [11] "ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation", ISO, Geneva, August 2022
- [12] D. Piester, "DCF77", [Online]. Available: <https://www.ptb.de/cms/en/ptb/fachabteilungen/abt4/fb-44/ag-442/dissemination-of-legal-time/dcf77.html> [Accessed 10 February 2026]