Concept for a stepwise approach for an automated verification process of balancing services

Amanda Pleier
FfE GmbH
Munich, Germany
apleier@ffe.de

Patrick Dossow
FfE GmbH
Munich, Germany
pdossow@ffe.de

Michael Hinterstocker
FfE GmbH
Munich, Germany
mhinterstocker@ffe.de

Philipp Thalhofer
Technical University of Munich
Munich, Germany
ph.thalhofer@gmail.com

***Abstract*—To ensure system stability in the power grid, transmission system operators (TSO) are responsible for balancing grid frequency fluctuations by means of balancing services. In many cases, balancing service providers (BSP) aggregate several technical units for the provision of balancing energy. However, beyond the compensation process for the BSP, no monitoring process for the proper provision of required balancing energy by the TSOs exists so far. This paper presents a stepwise concept for a verification process in which the most relevant monitoring requirements of the TSOs are met. These include the exclusive participation of pre-qualified technical units in the balancing service, as well as the correct forwarding of the requested balancing energy from the BSP to its technical units and their proper provision within a tolerated range. The presented concept enables the tamper-resistant storage and retrieval of the required data for verification. In the second stage of the concept, the utilization of a Zero-Knowledge Proof additionally ensures that the verification is performed automatically and in compliance with the BSP's trade secrets. The integration of the monitoring of individual units creates additional value since filtering for faulty units is made possible for both the TSO and the BSP. For a possible implementation of the concept, we discuss and evaluate the usage of the technologies blockchain and public key infrastructure.**

***Keywords*—Balancing service, system stability, digitalization, blockchain, public key infrastructure, asset logging, automation, verification**

I. Introduction

To ensure system stability in the power grid, power generation and consumption have to be balanced at all times. In Germany, the transmission system operators (TSOs) are responsible for balancing grid frequency fluctuations by means of balancing services, when generation or consumption deviate from their respective forecast. In future, it is likely that an increasing number of balancing service providers (BSPs) will aggregate several small scale technical units (TUs) for the provision of balancing service [1], which makes the process more complex and difficult to monitor. Furthermore, the transition of the energy system to renewable energies is likely to raise the overall demand of balancing services so that a proper provision by BSPs is essential for a stable power grid.

Since TSOs currently have no means of monitoring the balancing service provision beyond the compensation process for balancing energy, a verification process for the provision both at aggregation level as well as for the individual TUs is required to prevent intentional or unintentional faulty provision.

The aim of this paper is to create a specific concept for a verification process that meets the demands of both, the TSOs and the BSPs. To do so, first we identified unresolved issues regarding the initial concept based on the findings in [2]. These issues were examined in a bilateral exchange between energy researchers and balancing service experts from a German TSO. In a next step, priorities for the process were identified from the TSO's point of view. The resulting concept was then mirrored to a BSP to identify issues for its role in the process and evolve the concept correspondingly. The final concept is described in the following.

II. Stepwise concept for a verification process

A two-stage solution concept is proposed, which forms the basis of an overall concept for the provision of the three types of balancing services in Germany - automatic frequency restoration reserve (aFRR), manual frequency restoration reserve (mFRR) and frequency containment reserve (FCR) (see also [3]). A summary of the solution stages is shown in Fig. 1.

A. Verification of aFRR provision

In the exchange with stakeholders involved in balancing services provision in Germany, the priority for a verification process is set on the verification of aFRR for the solution stages A1 and A2, since the number of aFRR activations clearly dominates other types of balancing services [4]. To understand

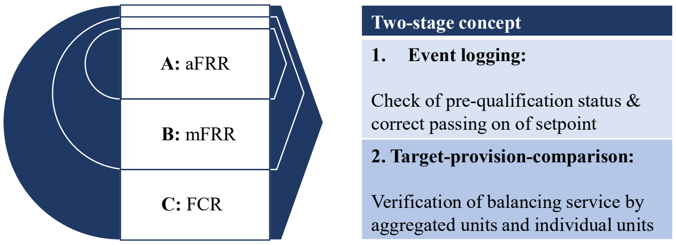
A: aFRR
B: mFRR
C: FCR
Two-stage concept
1. Event logging:
Check of pre-qualification status & correct passing on of setpoint
2. Target-provision-comparison:
Verification of balancing service by aggregated units and individual units

Fig. 1. Two-stage concept for a verification process with stepwise adding of different types of balancing service

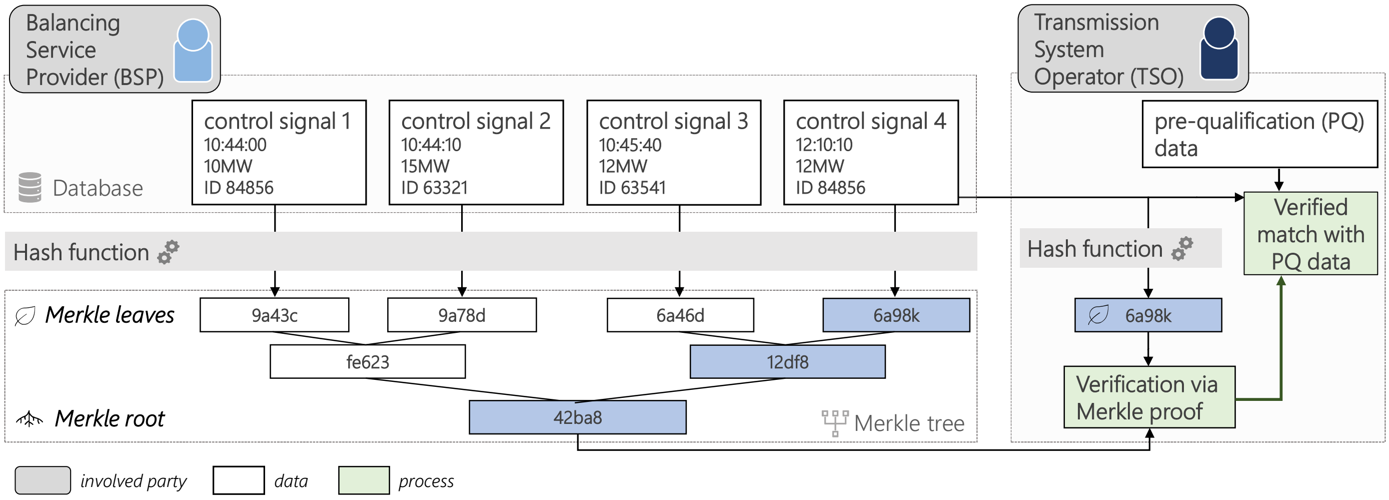

Fig. 2. Illustration of the verification of a control signal by Merkle proof

the developed concept for a verification pf aFRR provision, we first describe the status quo of aFRR provision in Germany.

In most cases, BSPs aggregate several TUs for the provision of balancing services. In order to be admitted to the balancing market, each TU must first undergo a so-called pre-qualification procedure, where each TU must prove that it meets the requirements for a specific type of balancing service. For aFRR, this is the activation within five minutes. After a successful trial activation with the so-called “Doppelhub”, the TUs are stored in the pre-qualification (PQ) platform of the TSOs as pre-qualified for aFRR. The BSP is then allowed to offer the aggregated aFRR capacity on the aFRR balancing capacity market. As soon as the TSO anticipates demand for balancing energy in the timeframe of 5 to 12.5 minutes in the future, the required aFRR setpoint is transmitted to the BSP. The BSP directly activates its TUs in a certain order (merit order) of its choice, so that each TU provides its share of balancing energy. The metering of the TUs is constantly transferred to the BSP, who is required to transfer aggregated metering values of all its TUs to the TSO in a maximum of four second intervals. If the TSO detects incongruities in those data, such as insufficient stabilization of the grid frequency despite the requested balancing service, the metering data for all involved TUs is requested via non-standardized Excel tables [2]. The verification of the data is then done manually by the TSO and therefore requires considerable manpower. Furthermore, the process harbors a high potential for errors and manipulation. The resulting requirements for an improved verification process thus comprise the properties automation and tamper-resistance while still preserving the BSP’s trade secrets. The deduction of those requirements is carried out in [2].

These requirements for a concept primarily add value to the TSO role, whereas adapting the existing process for the BSP role would add implementation workload. However, as TSOs are responsible for system stability, the requirements for an improved verification process are assessed as valid and relevant and form the basis for the solution concept developed. In the following paragraphs, we describe the two-stage concept for a digital verification of aFRR provision with the steps outlined in Fig. 1.

Event logging (A1): In the first stage, the control signals for an aFRR activation are stored locally by the BSP as shown in Fig. 2. The control signals including the timestamps are added as leaves to a so-called Merkle tree after applying a hash function. By a pairwise combination of the leaves, a single top hash is created. [5] This so-called root of the Merkle tree is thus a "digital fingerprint" of all control signals in the pool. If necessary, the TSO can request the raw data of the control signals stored by the BSP and apply the same hash function. If the raw data is unchanged, the resulting hash again corresponds to the original leaf in the Merkle tree. Therefore, the TSO can use a so-called Merkle proof to verify the integrity of the raw data, as long as the immutability of the Merkle root is guaranteed [6]. The verified IDs of the controlled TUs can then be matched with the list of pre-qualified units from the PQ-platform of the TSOs. The verified control signals also allow the BSP to prove that he has correctly passed on the TSO's setpoint to its TUs. If the TSO detects deviations between the required balancing energy and the sum of the transmitted control signals, the real metering data of the individual TUs can be requested, analogous to the status quo, and the provision of the balancing energy can be checked at TU level. In contrast to the current process, however, this ex-post query of the metering data should ideally be standardized. To ensure the integrity of the control signals, the Merkle root must be stored tamper-resistant until the execution of the Merkle proof. The transaction of the raw data must be done via a communication channel where the integrity is guaranteed. Options for a technical implementation which meet these requirements are discussed in section 3.

Target-provision-comparison (A2): In the second stage, the verification of aFRR provision is done automatically at both aggregation level and TU level, without disclosing confidential information of the BSP. Therefore, the concept of Zero-Knowledge Proof (ZKP) is utilized. Here, one party wants to prove a certain fact, while the opposite party learns nothing except the truth of this proof. The result of the proof can be trusted by both parties since they have jointly set up the rules for

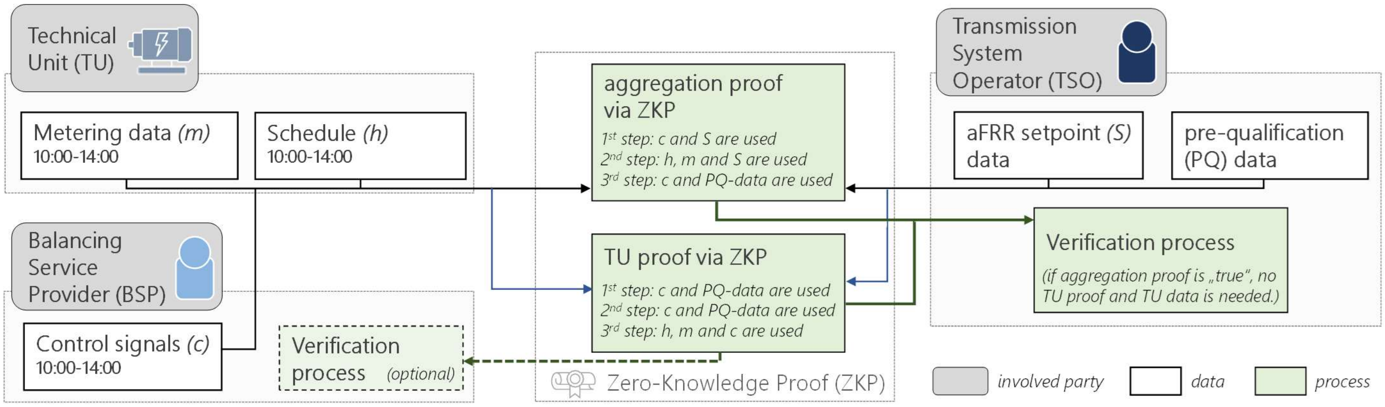
Technical Unit (TU)
Metering data (m)
10:00-14:00
Schedule (h)
10:00-14:00
Balancing Service Provider (BSP)
Control signals (c)
10:00-14:00
Verification process (optional)
aggregation proof via ZKP
1st step: c and S are used
2nd step: h, m and S are used
3rd step: c and PQ-data are used
TU proof via ZKP
1st step: c and PQ-data are used
2nd step: c and PQ-data are used
3rd step: h, m and c are used
Zero-Knowledge Proof (ZKP)
Transmission System Operator (TSO)
aFRR setpoint (S) data
pre-qualification (PQ) data
Verification process
(if aggregation proof is „true", no TU proof and TU data is needed.)
involved party
data
process

Fig. 3. Target-provision-comparison via Zero-Knowledge Proof

proof generation in the context of a multi-party computation. More information about ZKPs and their application in the energy sector are available in [7] and [8]. In the context of proving the correct provision of aFRR, this means that the actual metering data as well as the TU schedules including the timestamp directly serve as input to the ZKP program. Another input is the aFRR setpoint and the TSO's list of all pre-qualified TUs as well as the BSP's control signals to its TUs, as depicted in Fig. 3. Since the creation of a ZKP requires a considerable amount of computational power, we propose to check a timeframe of four hours. First, the aggregation ZKP is used to prove whether the aggregated balancing energy was provided correctly at aggregation level without revealing any information about the sensitive input data for the considered timeframe. In the following, the individual steps in the ZKP for an aggregation proof are described.

The first step is to verify whether the sum of all control signals c_i corresponds to the aFRR setpoint S. Therefore, it is checked if the BSP has correctly passed on the required setpoint to its i units within a given tolerance range tol:

$$\sum_i c_{i,t} - S_t \leq tol \tag{1}$$

Hereby, the index t describes the value for each second in the considered timeframe of four hours. In the event logging solution stage A1, this check was carried out by the TSO who had to proactively request the control signals in order to check the correct forwarding of the setpoint. In this solution stage, the check is now carried out automatically in the ZKP. The interface between the ZKP and the input data of TSO and BSP must be set up in advance to ensure automated input. The tolerance for a deviation between aggregated control signals and the setpoint is determined based on the settlement method for aFRR provision in [9]. An acceptance range is defined depending on a dynamic gradient that itself depends on the course of the setpoint. An additional tolerance range is placed around this accepted range to allow for fluctuations in the provision. For the evaluated timeframe in (1), we suggest to allow for 10% of the values to be in the tolerance range and 3% of the values to be outside of the tolerance range. Since the tolerance range is dependent on the setpoint, there needs to be a minimum range for small setpoints. Here, it is suggested to use a range of 10% of the reserved balancing capacity. The tolerance range is also used in the next step in the ZKP, where it is checked whether the aggregated balancing energy was provided correctly. Thereby, the aggregated balancing energy of all TUs is compared with the TSO's setpoint. The balancing energy provided by the individual units is calculated from the difference between the TU schedule h and its metering data m:

$$\sum_i (h_{i,t} - m_{i,t}) - S_t \leq tol \tag{2}$$

If the deviations are within the tolerance range, the test step is positive. As a third step, it has to be checked whether all activated TU are pre-qualified for aFRR. For this purpose, an interface to the TSO's PQ-platform to the ZKP must be created, which imports the current list of all pre-qualified unit IDs. The IDs in the control signals of the activated units can then be matched with those in the PQ list. The check is only positive if all the activated units in the aggregation are found in the PQ list.

When all three steps for the check on aggregation level are met, the ZKP outputs a "true" for the investigated timeframe. The TSO can thus be sure that the balancing energy was correctly provided at an aggregation level and that only pre-qualified units were involved. If one of the three check steps fell through, the ZKP outputs a "false".

In the following, the checking steps for a proof on TU level are explained. First, analogous to the third step of the aggregation proof, the ID of the activated unit is compared with the list of pre-qualified TUs. If there is a match, the check step is passed. As a next step, it is checked whether the activation value in the control signal is less than or equal to its prequalified capacity. In a final step, the balancing energy provision is checked at TU level. Here, the difference between the TU schedule h and its metering data m is compared with its control signal c:

$$(h_{i,t} - m_{i,t}) - c_{i,t} \leq tol \tag{3}$$

If the deviations are within the same tolerances as in the aggregation proof, the test is passed. If all three steps passed, the ZKP outputs a “true” and the unit ID is stored in the TSOs database with its proof for the examined timeframe. As soon as one of the three steps has been checked negative, the TU proof is negative and is stored together with its ID as "false".

The TU proof is performed independently of the aggregation proof. So even if a deviation of the aFRR setpoint from the control signals passed on to the TU has already been detected in (1) of the aggregation proof, the TU proofs can still be "true", since only the correct behavior of the individual unit at the control of the aggregating BSP is checked. Both the aggregation proof and the TU proof are stored in a database. However, since deviations from individual units can cancel each other out at aggregation level, a "true" aggregation proof is crucial for the TSO. The TSO as well as the BSP have a verification key and can thus only verify a proof, if the proof has been carried out with the rules defined in advance. This allows both parties to trust the proof. If the aggregation proof is "false", the TSO receives information about which TUs were operated incorrectly. This way the units to be examined are pre-filtered and the TSO has the option of requesting only the metering data of individual TUs with negative TU proof. The TSO can transfer the TU proofs to the BSP, so that it can specifically investigate the faulty units. This means a significant reduction in the workload for both parties.

B. *Verification of aFRR and mFRR provision*

In the first section, we considered the simplified case of a homogeneous pool with only TUs for the provision of aFRR. In reality, pools usually consist of TUs pre-qualified for different types of balancing service. Individual units can also be pre-qualified for several types of balancing service at the same time, as long as they meet all their requirements. In this section, the solution concept for the verification of the correct provision of aFRR and mFRR is explained.

Event logging (B1): In the first solution stage, the control signals of the activated TU including time stamp and unit ID are logged and hashed and the resulting Merkle root is stored. In case of demand, the TSO can request the control signals from the BSP and verify them by using a Merkle proof. However, in the case of an activation of aFRR as well as of mFRR, the TSO is so far not able to verify for which type of balancing service the controlled units are pre-qualified since it has only received the information for the activation of a specific TU. Therefore, in this solution stage, it is necessary to log the associated type of balancing service in addition to the control signal. Since only the BSP can provide the information for which type of balancing service a TU is activated, there is a theoretical risk of manipulation. If necessary, however, the TSO compares the sum of all control signals per type with the target value for this type of balancing service, so that an incorrect assignment of individual control signals would quickly become apparent. The TSO can then compare the verified TU IDs with the prequalified unit IDs from its PQ-platform for the respective type of balancing service and can also compare the aggregated control signals per type of balancing service with the corresponding setpoint.

Target-provision-comparison (B2): In the second solution stage, the ZKP for an activation of both aFRR and mFRR is carried out. In case of a simultaneous provision of aFRR and mFRR of one unit, the TU's metering data are available without distinction between aFRR provision and mFRR provision. Additional inputs for the ZKP to the ones shown in Fig. 3. are the setpoints for aFRR and mFRR provision as well as the control signals forwarded by the BSP to its TUs, broken down to the desired control reserve type.

As a first step for an aggregation proof, the sum of all control signals per control reserve type are compared with the corresponding setpoint analogous to (1). In the following step, it is checked whether the correct amount of balancing energy was provided at aggregation level. Therefore, the balancing energy provided at aggregation level is calculated from the difference between the sum of all TU schedules and its metering data and is compared with the sum of aFRR setpoint and mFRR setpoint analogous to (2). In the third step, it is checked if all activated TUs are pre-qualified for the corresponding type of balancing service analogous to A2. The aggregation proof is "true" as soon as all three check steps have passed.

The TU proofs are performed analogously to the ZKP for aFRR provision, but individually for each type of balancing energy. In the third step, where the balancing energy provision has to be checked for each unit, the check is performed cumulatively for both types of balancing energy, since the metering data is available without distinction between aFRR provision and mFRR provision. The difference between metering data and TU schedule is compared with the sum of both control signals for the unit in case of a simultaneous provision of aFRR and mFRR in the considered timeframe. If all three test steps are passed, the TU proof is "true". The TU proof is stored in the TSO's database.

C. *Verification of aFRR, mFRR and FCR provision*

For a concept including the possible provision of FCR in the BSP's aggregation of TUs, several features of the balancing service type have to be considered. First of all, the activation of FCR is automatically controlled by the locally measured system frequency. There is no setpoint sent by the TSO and no control signal sent by the BSP. However, the balancing energy to be provided is proportional to the deviation of the system frequency from its target value, so that the "control signal" can be calculated from the frequency measurement at the unit. The calculated "control signal" can then be logged with the TU ID together with the logging of aFRR and mFRR control signals in the solution stage **event logging (C1)**. This can be done regardless of a simultaneous activation of aFRR or mFRR for the same TU, since their activation is controlled independently of a possible additional FCR provision.

For the second solution stage **target-provision-comparison (C2)**, the calculation is integrated in the ZKP program. Since a schedule for units providing FCR also exists, the provided balancing energy can be calculated using (2). The unit's pre-qualification for FCR can be checked analogous to aFRR and mFRR provision.

The consideration of FCR in the concept increases the complexity for an implementation but also adds value by verifying a realistic provision of all types of balancing service.

III. Options for technical implementation

In the previous sections, a stepwise concept for the verification of balancing service was described. In the event logging stage, a tamper-resistant storage of the Merkle root and verified control signals is required. In the second solution stage, the transmission of input data to the ZKP program must take place via a secure channel to ensure computation with verified data. Finally, in both stages the ex-post query of metering data must be tamper-resistant. To meet these requirements in a technical implementation, different options are discussed. A summary including an evaluation for the verification of balancing services can be found in Table 1 and is described in the following.

One option for the tamper-resistant storage of data is **blockchain technology**. Here, any modifications to data in the chain are detected and must be agreed on by all nodes which makes the blockchain a tamper-resistant database [11]. Therefore, the updated Merkle root in the event logging stage can be stored on a blockchain, so that the information of all control signals can be verified using a Merkle proof. However, blockchains have many features, which are summarized in Table 1. Because of the implementation effort and the demand of energy for the technology, the implementation of a blockchain-based platform is primarily useful if it benefits from several features mentioned in Table 1. For the described concept, not many blockchain-features are used.

One major advantage for the use of blockchain technology is the easy integration in the existing process and the possible creation of synergies for other use cases, where logging and tamper-resistant storing of data become necessary. A detailed description of data logging for assets in the energy sector and its implementation on a blockchain-based data platform can be found in [12].

Since tamper-resistance on a blockchain is only given from the moment data is put on the blockchain, but data integrity is required along the entire process, a secure communication channel for the transmission of data is needed. For this channel the following requirements have to be met:

1. The metering data have not been subsequently modified.
2. The metering data can only be read by the recipient.
3. The metering data actually originates from the requested TU.
4. The receiving market participant is actually authorized to receive the metering data.

TABLE I. FEATURES OF IMPLEMENTATION OPTIONS EVALUATED FOR THE VERIFICATION OF BALANCING SERVICES

Technical implementation	**Features**	**Feature evaluation regarding the use case “verification of balancing services**
Blockchain	Tamper-resistance	Beneficial, but only as of the deposit on the blockchain. Before that, the risk of tampering is given.
	Transparency through publicly viewable database	Not required, as only two parties have access to the data: the BSP and the TSO.
	Available and distributed data platform	Not required, as only TSO has an interest to obtain hashes from the blockchain. Other accesses are not intended.
	No single point of failure	Beneficial, but only as of the deposit on the blockchain. Before that, the potential of error is given.
	High degree of automation	Beneficial, but adds little value since the only transaction is the deposit and retrieval of the Merkle root from the blockchain.
Public-key-infrastructure (PKI)	Confidentiality through digital certificates*	Beneficial, as data, such as generated proofs or requested metering data, can thus only be read by the recipient.
	Integrity through digital signatures*	Beneficial, as input data for the ZKP and metering data for an ex-post query cannot be subsequently modified.
	Authenticity through digital certificates issued by a certificate authority*	Beneficial, as input data for the ZKP and metering data for an ex-post query actually originate from the requested TU.
Smart metering public-key-infrastructure (SM-PKI)	Tamper-resistant metering device	Beneficial, as the recording of provided energy cannot be tampered with.
	Access restricted to authorized market participants	Beneficial, as metering data of TUs can only be accessed by authorized market participants.

*Feature also valid for SM-PKI

The first requirement can be guaranteed by using digital signatures. In this case, a TU has an asymmetric key pair: a secret key for encrypting data (private key) and a public key for decrypting data (public key). The public key is calculated by a cryptographic one-way function from the private key, so that it is not possible to deduce the secret private key from the publicly accessible public key. In the digital signature, data is first converted to a fixed-length character string (hash) using a hash function. A digitally signed data set is created by encrypting the hash of the metering data with the private key of the unit [13]. This digital signature can now be sent with the clear data and the public key of the unit. The recipient uses the public key to decrypt the digitally signed data record and thus receives the hash of the original data record, since this hash was encrypted with the corresponding private key. In order to now check the integrity of the sent clear data, the same hash function is applied to the clear data as in the digital signature and the resulting hash is compared with the hash from the digitally signed data set. If they match, this is proof that the plain data has not been altered. By successfully decrypting the digitally signed data set with the public key, the recipient can also verify that the message originated from a sender with the corresponding private key. This rules out the possibility of an attacker sending forged data with the unit’s public key. However, since the metering data in this scenario is sent as clear data, it can also be intercepted and read by unauthorized third parties. Therefore, the second point in the above requirements for secure transmission of metering data is not guaranteed by the mere use of a digital signature.

The second requirement can be met by encrypting the data with the recipient's public key so that only the recipient can decrypt it with their private key. However, this option still does not cover requirements three and four, since the sender's public key cannot be assigned to a specific unit as well as the recipient's public key does not necessarily belong to an authorized market participant. For this reason, digital certificates are used to ensure the authenticity of a public key and its permissible scope of application and validity. A trusted third party, the Certification Authority (CA), checks the identity of the owner and other properties of the public key and issues a certificate if the information is correct. If the public keys of both parties involved in a communication are deposited with the CA and certified, the authenticity and identity of both, the sender and the recipient, can be ensured. The digital certificate itself is in turn protected by a digital signature of the issuer, so that the authenticity of the certificate can be verified with its public key. The authenticity of this public key can in turn be confirmed by another certificate from a higher authority. This hierarchy of certificates and their management forms a **public key infrastructure (PKI)**. By using a PKI, data can be retrieved and sent via an encrypted channel where data integrity is guaranteed. This ensures a tamper-resistant transmission of the Merkle root in the first solution stage and of the input data for the ZKP program in the second solution stage, as well as a secure transmission of metering data in the ex-post query in both stages. Since PKI is a reliable technology with less implementation effort than a blockchain, this option is preferred to the implementation of a blockchain.

However, for this option, the metering itself is carried out by uncertified meters. which could be manipulated. Therefore, a certified intelligent metering system is needed which can communicate only with authorized market participants on a secure channel. The **smart metering (SM-) PKI**, developed in Germany, meets these requirements [10]. Hereby, the German Federal Office for Information Security (BSI) acts as the highest CA. It issues certificates for subordinate certification authorities. The role of these so-called sub-CAs is taken by audited and monitored organizational units and is authorized to issue certificates for end users such as external market participants as well as the smart meter gateway (SMGW) administrator of an installation. Only holders of such certificates are technically able to read data from SMGWs, if they also have the required approvals [10]. Therefore, SM-PKI is a secure infrastructure for the metering and logging of control signals and the data transmission to authorized market participants such as the BSP and TSO in the described concept for the verification of balancing service.

For this purpose, a so-called “tariff application case” (German: Tarifanwendungsfall, TAF in short) must be formulated, that defines the transmission of high-resolution metering data for a specific time period. [10]. The transaction data is then transmitted to the BSP via the SM-PKI and temporarily stored there. In case of an ex-post query of the metering the TSO can request the stored data from the BSP. The origin of the data from a specific TU can be clearly verified by the digital certificate of the sender. In addition, the hash comparison of the digital signature described above enables the TSO to detect whether the values have been manipulated on their way from the TU via BSP. Since the storage of the transaction data by the digital certificates requires a lot of storage space, a rule could also be defined in a TAF that filters and stores only the relevant data from the header of the digital signature.

A disadvantage for the use of SM-PKI is the large storage space of the data, which can be considerable even if the data headers are filtered by a TAF. In addition, the rollout of smart meters in Germany is not yet far enough advanced to expect availability at all units of BSPs. Although the obligatory rollout for smart meters is scheduled for 2032 in Germany, it continues to be delayed [10] which prolongs the utilization of proprietary systems.

It can be concluded that the implementation of a PKI in combination with conventional metering is the best option for an early realization of the concept. However, this option leaves the possibility for manipulated metering data. Therefore, as soon as the rollout of smart meters in Germany is completed, the SM-PKI should be used as metering infrastructure for the provision of data.

IV. Conclusion and Outlook

The bilateral exchange with balancing service experts from a German TSO showed high demand for a monitoring and verification process of balancing services. To meet this demand, a concept was developed which step-by-step meets the most relevant requirements of the TSO. In this concept, the first stage can be implemented with little effort but already adds value to the status quo by checking the PQ status of TUs and the correct forwarding of the setpoint. In the second stage, a ZKP is used to additionally ensure that the verification of balancing service provision is performed automatically and in compliance with the BSP’s trade secrets. The concept also includes a proposal for how to gradually integrate the three different balancing services.

For the technical implementation with the requirement of integrity-proof transmission of metering data, the technical options blockchain, PKI and SM-PKI were discussed. Hereby, a PKI was evaluated as the best solution for a shortterm implementation of the described concept.

A realization of the concept will incite the correct provision of balancing services by BSPs and will thereby help the TSOs to balance the power grid. Furthermore, the automation of the verification process will reduce the workload of TSOs and BSPs. In future, the TU proofs of the ZKP could also be used for the repetition of pre-qualification. Thereby, the faulty provision of balancing services by one TU can serve as a red flag so that the repetition of pre-qualification of that TU will be monitored more thoroughly. If a TU only produces positive proofs, the repetition of pre-qualification can be skipped reducing the workload for both, the BSP and the TSO.

References

[1] Poplavskaya, K., de Vries, L.: Chapter 5 - Aggregators today and tomorrow: from intermediaries to local orchestrators? In: Sioshansi (ed.), F. Behind and Beyond the Meter, pp. 105-135, Academic Press (2020).

[2] Djamali, A., Dossow, P., Hinterstocker, M., Enzenhöfer, R., Beitsch, D., Bogensperger, A., Anforderungen an einen automatisierten Nachweis von Regelreserve. In: 12. Internationale Energiewirtschaftstagung an der TU Wien, Wien (2021).

[3] „regelleistung.net“, https://www.regelleistung.net/ext/, last accessed 2022

[4] Bundesnetzagentur, Bundeskartellamt, Monitoringbericht 2022, (2022).

[5] J. Chapweske, G. Mohr: Tree Hash EXchange format (THEX). San Francisco (2008).

[6] Merkle, R., A Digital Signature Based on a Conventional Encryption Function. In: Pomerance, C. (ed.), CRYPTO 1987, LNCS, volume 293, pp. 369-378, Springer, Berlin (1988).

[7] Goldwasser, S., Micali, S., Rackoff, C., The knowledge complexity of interactive proof-systems. In: Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing, pp. 291-304, Association for Computing Machinery, Rhode Island (1985).

[8] Sedlmeir, J., Völter, F. Strüker, J., The next stage of green electricity labeling: using zero-knowledge proofs for blockchain-based certificates of origin and use. In: SIGENERGY Energy Inform, Association for Computing Machinery, New York (2021).

[9] 50Hertz, Amprion, Tennet TSO, TransnetBW, Abrechnung der aFRR-Arbeit ab 01.10.2021, (2021).

[10] Bogensperger, A., Estermann, T., Samweber, F., Köppl, S., Müller, M., Zeiselmair, A., Wohlschlager, D., Smart Meter - Umfeld, Technik, Mehrwert, (2018)

[11] Beck, R., Stenum Czepluch, J. S., Lollike, N., Malone, S., Blockchain – The Gateway to Trust-Free Cryptographic Transactions. In: Twenty-Fourth European Conference on Information Systems (ECIS), Springer Publishing Company, Istanbul (2016)

[12] Djamali, A., Dossow, P., Hinterstocker, M. et al. Asset logging in the energy sector: a scalable blockchain-based data platform. In: Energy Informatics 4, (2021)

[13] Johnson, D., Menezes, A., Vanstone, S., The Elliptic Curve Digital Signature Algorithm (ECDSA). In: International Journal of Information Security, Mississauga (2001)