2025 IMEKO TC-6 International Conference on
Metrology and Digital Transformation - **M4DConf 2025**
Benevento, Italy, September 3-5, 2025

Digitalized Third-Party Validation for Calibration Service: a System Design Example

Hiroshi Watanabe[1], Yoshitaka Shimizu[1], Katsuhiro Shirono[1], Toshiyuki Fujimoto[2]

[1]*National Institute of Advanced Industrial Science and Technology (AIST), National Metrology Institute of Japan (NMIJ), Tsukuba 305-8563, Japan, hiroshi-watanabe@aist.go.jp, y-shimizu@aist.go.jp, k.shirono@aist.go.jp*
[2]*National Institute of Advanced Industrial Science and Technology (AIST), Planning Headquarters, Tsukuba 305-8561, Japan, t.fujimoto@aist.go.jp*

***Abstract* – We present a new case study of digitalized third-party validation for a calibration service of purity. The third-party validation is an add on to the calibration service, conducted by a third party independent from laboratory and customers, aiming at assuring quality of results. The case features frequent validations, and information leakage-free by checking data within the laboratory rather than externally, that have not been addressed in the previous cases. We describe the design and implementation of the system.**

I. INTRODUCTION

Accredited Testing and Calibration services are carried out in accordance with a predetermined procedure in laboratories. The procedure is reviewed by an accreditation body at some regular intervals, such as 3 years. As a result, most customers may assume that the results of the services are sufficiently reliable for their purposes. However, our concern is that the laboratories cannot clearly demonstrate how they implemented the procedures to obtain the individual results. They have no specific means of assuring customers beyond simply reminding them of their accreditation status.

A. Digitalized third-party validation for Calibration service

As a means to complement the system of accreditation, the authors have proposed integrating validation [1, 2, 3] in laboratory calibration processes, meeting the following conditions: conducted by a third party independent of both the customer and the laboratory; performed promptly each time a specific work is executed or data is generated; controlled or automated by software; checks the work log or data to confirm the process is on track, and records proof of the checks or the confirmation in the third party.

In integrating the third-party validation into calibration process, laboratory can convey quality of activities, results, and relevant data to customers by using the result of validation. In addition to the the proposal of the approach [1], we have developed two practical cases that implement the approach as proof of concept: vernier-caliper calibration [2] and calibration of reference photovoltaic devices [3].

These two cases of integrating third-party validation gave clear insight into the approach and showed feasibility of the approach. On the other hand, they revealed remaining two concrete challenges in implementing the approach as follows:

B. Investigation on timing and content of a validation

If a calibration service takes longer period, such as over a few weeks, the more frequent the validations, the more reliance the customer may have in quality of results in laboratory. However, too frequent validations may cause unnecessarily increasing the complexity of the control and cost while decreasing the thruput. In the previous cases, we did not implement frequent validations: one validation in vernier-caliper case [2], and two validations in reference photovoltaic devices case [3]. It is important to design timing and content of a validation to increase reliability as much as possible without increasing costs. To discuss an appropriate frequency, demonstrating cases along with necessity of implementing frequent validations is also indispensable.

C. Laboratory and customer information leakage-free

The data to be checked in a validation may include information of laboratory or customer. If the data is transferred outside of the laboratory and checked at there, any leakage of laboratory or customer information from the transferred data becomes our great concern. In order to decrease the risk of information leakage from the transferred data, we can consider in two directions as follows:

- developing secure and confidential checking system, even in outside, that can handle the transferred data without any information leakage, or
- checking the data within the laboratory rather than externally, and eliminating, originally, any customer or laboratory information from the data transferred outside.

The previous cases [2, 3] addressed the first direction and elaborated the checking system at a third party organization by employing smart contract on a blockchain. The variety of techniques, whether blockchain or not, that realize the first direction needs to be developed further. On the other hand, it has not been addressed yet whether we can develop validation that implements the second direction. In practice, the second direction might be preferred by the laboratories that do not want to be bothered by the transferred data outside.

The present study develops a new case of the third-party validation for calibration service of purity. In developing, we address the above challenges in order to wider the applications of the approach. The main contribution of the present paper is to show a new case of integrating validations with the following both features:

- frequent validations as described in Section IV.B., and
- information leakage-free, following the second direction different from the previous cases, by checking data within the laboratory rather than externally as described in Sections III.D. and IV.C..

The case broadens the scope of the approach, since these features have not been addressed in past cases. Today, there are many people in metrology community who are looking for ways to address digital transformation. The system design of the case is of interest to them and offers many valuable insights.

The paper is organized as follows: Section II introduces the procedure of calibration service of purity which we integrate third-party validations. Section III describes a design of third-party validation. Then, Section IV introduces concrete implementation of a few validations. Section V mentions related work. Finally, we discuss and conclude in Section V.

II. CALIBRATION SERVICE OF PURITY

A calibration service of purity used for integration of third-party validation is introduced. The service is part of an accredited calibration service that receives a request with a sample compound from customers, conducts both NMR and GC experiments in parallel, and issues calibration certificate that includes the calibration result (purity). Fig.1 shows a simplified procedure of the calibration service. Any experiment comprises three activities: sample preparation, measurement, and data analysis. Of these, the activities measurement and sample preparation are repeated until sufficient measurement data is available for the data analysis. Once both experiments are completed and both results of data analysis are obtained, a calibration result is determined and a calibration record file is compiled from these results. The calibration certificate is issued based on the calibration record file. There are multiple personnel in charge of the service, with roles divided as

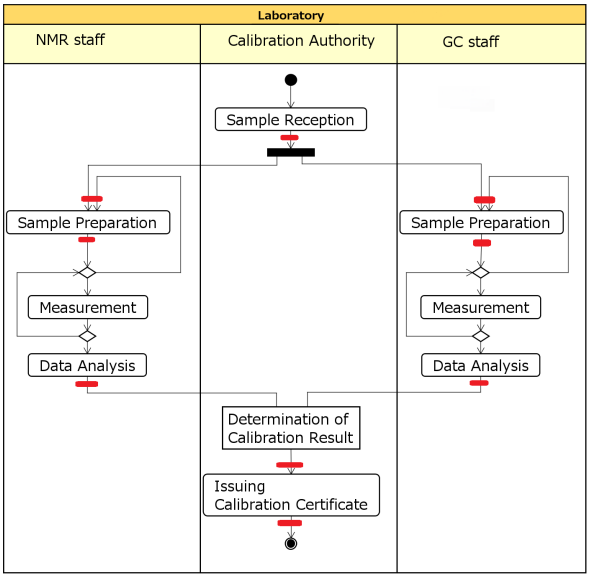

Fig. 1. Procedure of calibration service of purity, and timings of validations. The small red signs indicate the timings for validations described in Sections iii. and iv.

follows: Calibration Authority, NMR staff, and GC staff. The entire service, from receiving a request to issuing certificates, takes 2 weeks to 2 months, at most.

Keeping environment (temperature and humidity) in the laboratory stable during the activities of sample preparation is crucial for later valid calibration results. Some sample compounds absorb moisture from the air, altering their weight and purity. Therefore, acceptable ranges of environment is specified in a quality manual as environmental conditions for each sample compound. We ensure that the laboratory environment meets the environmental conditions during the activities.

III. DESIGNING VALIDATIONS

A. Basic Design of Validations

Table 1 shows a list of validations we considered, whose timings are also indicated on the procedure in Fig. 1. We integrate validations after each of the following activities: sample reception, sample preparation, data analysis, and issuing calibration certificates. Among these activities, before each of the following activities, we also integrate validations: sample preparation and issuing calibration certificate. We call the validation before issuing calibration certificate ConformityAssessment, since, in this validation, we check the calibration record file with the calibration result that is to be transcribed to the certificate.

Table 1. List of Integrated Validations

Name	Timing	Operator	Data to be checked and compiled into data package	Log
SampleReception	after **SR**	CA	reception information sample information	Y
pre-SamplePreparation	before **SP**	MS	environment (temperature and humidity), personnel and equipment	N
post-SamplePreparation	after **SP**	MS	sample preparation record file for NMR or GC, environment (temperature and humidity), personnel and equipment	Y
DataAnalysis	after **DA**	MS	summary report for NMR or GC, measurement data, sample information	Y
ConformityAssessment	before **ICC**	CA	calibration record file	Y
RegistrationOfCertificates	after **ICC**	CA	calibration certificates and their IDs	Y

SR= Sample Reception, **SP**= Sample Preparation, **DA**= Data Analysis, **ICC**= Issuing Calibration Certificate, CA=Calibration Authority, MS=NMR staff or GC staff

B. Local Application and Local Storage

Let us introduce some terms before we explain concrete design. A *local application* is software that is designed and developed by the third party but is deployed and operated in the laboratory. A *local storage* is a storage installed in laboratory to allow sharing information between local applications. A *data package* for activity is a text data in JSON format generated by local applications, which stores a collection of data produced or generated during the activity. A *completion log* of an activity is a text message generated and sent by local applications that indicates the completion of the activity. It consists of a control ID (which identifies the activity within a series of activities in a calibration service), a hash of the activity's data package and a time stamp.

For each validation in Table 1, we design a local application. Fig.2 shows a basic design for local applications prepared to align the designs for individual applications. The applications generally behaves as follows: when the operator uploads data, the local application retrieves from the local storage the relevant past data packages, called "context"; it checks the data by using the context; after the check, it compiles the data with the check results into a new data package; this new data package is then saved back to the local storage; finally, the application sends a completion log to the third party.

Note that the local storage must be properly access controlled, since it affects the later validation results. So, we encrypt the local storage using a third-party key. The third party ensures that only local applications have access to the storage using the key, making the contents directly inaccessible to laboratory members.

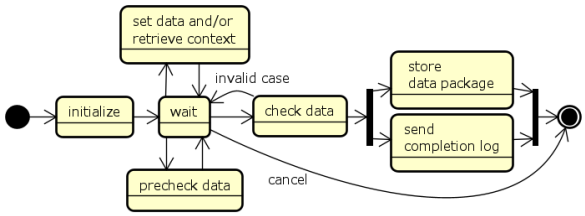

Fig. 2. Basic design for local applications

C. Certifier Server in third-party organization

In the third party, we prepare a certifier server with the following two functions: logging completion and integrity checking. The function logging completion stores the completion logs sent from local applications. The function integrity checking returns the result of comparing the incoming list of pairs of control ID and hash from ConformityAssessment and stored completion logs in the server.

D. Data Transfer from Local applications to Certifier Server

A general data flow diagram for a local application is illustrated in Fig.3. The message from local application to certifier server does not contain any laboratory or customer information. The application does not send data packages to the server, but sends messages such as completion logs, lists of pairs of control ID and completion log, or signals of beginning or ending calibration, at most. These messages do not contain any laboratory or customer information, except control IDs.

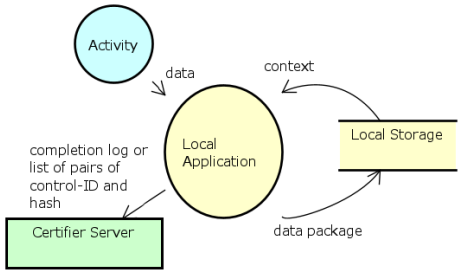

Fig. 3. Dataflow for local application

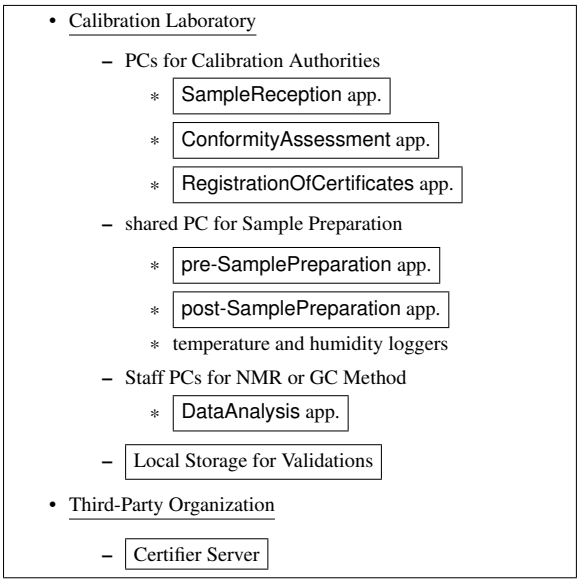

Fig. 4. System Configuration of entire system.

IV. IMPLEMENTING VALIDATIONS

We developed a system for validations based on the design described in the previous Section. Here, we describe an overview of the entire system, and a few concrete validations implemented as local applications, as shown in Fig.2.

A. System Configuration

Fig 4 shows the configuration of the entire system. In the laboratory, the local applications are installed in dedicated PCs for personnels or a shared PC for sample preparation with connected temperature and humidity loggers; the local storage is also prepared inside the laboratory. In the thrid-party organization, a certifier server is prepared.

B. Validations for Sample Preparation

In the calibration service (Fig.1), the activity of sample preparation is repeated during both NMR and GC experiments. For each sample preparation, the NMR or GC staff uses local applications to initiate validation pre-SamplePreparation before the activity and validation post-SamplePreparation after the activity.

The pre-SamplePreparation verifies specific environmental conditions of the sample compound before moving on to the sample preparation. In the "check data" state shown in Fig.2, the local application checks both

- the qualifications of personnel and equipment, and
- the environmental conditions by using the latest temperature and humidity data directly extracted from the logger connected to the shared PC.

If both succeed, the application displays with the message "Move on to Sample Preparation"; otherwise, the application halts the operation and prevents the staff from beginning the activity with deviations from quality manual; in this case, some corrective action is required to continue. We omit implementing "send completion log" in the local application.

The post-SamplePreparation leaves completion log in the third party immediately after completing the sample preparation. The completion-log sent by the local application includes the hash of the data package, which contains both the sample preparation record noted by the staff and data from the previous pre-SamplePreparation.

The completion logs stored in the certifier server in the third party cannot be falsified later by the laboratory member. So, they provide evidence to show integrity for the data packages stored in the laboratory, which we show in Section IV.C..

For every sample preparation, the present case repeats the pair of validations above. The combination of validations not only prevents deviations from quality manual at real time but also promptly leaves completion logs in third party.

C. ConformityAssessment

The calibration certificate with calibration result is issued based on the calibration record file in the activity "Issuing Calibration Certificate" shown in Fig.1. Just before the activity, the calibration authority uses the local application to start the validation ConformityAssessment.

The ConformityAssessment, conducted through the collaboration of the local application and the certifier server, verifies the calibration record file as follows. In the "set data and/or retrieve context" state shown in Fig.2, the calibration authority uploads calibration record file, then the local application retrieves all relevant data packages from the local storage, including sample reception, data analysis, and sample preparation. In the "check data" state, the application checks that the calibration record file does not contain any of the following errors:

- data omissions or inconsistencies, such as inconsistency of data between sheets inside Excel file,
- copying errors from data packages, and
- miscalculations, such as for calibration result, uncertainty and compensation.

Meanwhile, the certifier server checks the integrity of the retrieved data packages as follows: The local application recalculates hashes from the data packages, pairs the hashes with control IDs, creates a list of pairs of control ID and hash, and sends this list to the certifier server. The server then uses the integrity checking function (stated in Section III.C.) to compare the received list with the stored logs.

If both succeed, the local application indicates that the result is valid. If either check fails, it indicates that the result is invalid and displays the errors found.

Note that the validation provides a conformity assessment of calibration record file by combining the local application and the certifier server, including a consistency check with data from past data packages. Also, note that the local application does not send laboratory or customer information outside the laboratory, except for control IDs used to manage the service.

V. RELATED WORK

The present work follows the previous works [1, 2, 3] that explored integrating (third-party) validation in laboratory calibration processes. Specifically, these studies addressed micropipette calibration [1], vernier-caliper calibration [2], and reference photovoltaic devices calibration [3]. These focus on the third-party validation for calibration services more strongly than other related studies in the rest of this section. A key aspect of these works is implementation using smart contracts in blockchain technology. In contrast, the present study addressed a design that does not assume blockchain technology. Further details on the differences between the present study and the previous works are elaborated in the Introduction.

In addition, the line of work was heavily influenced by research on blockchain technology applications in metrology, especially in conformity assessment. This includes blockchain applications for legal metrology [4], measuring system implementation to enhance security and simplify regulatory management [5], and PKI implementation for smart meters [6].

In the digitalization of calibration services, Digital Calibration Certificates (DCC) [7] is currently a hot topic in the metrology research community. Beyond DCC, there are also studies on lab data management studies, such as [8], which utilize semantic web technologies and ontologies to enhance data interoperability and reusability in accordance with FAIR principles [9]. Both DCC and FAIR principles do not directly relate to the present topic of third-party validation.

The challenge of frequent validations (in Section I.B.) is inseparable from a principle of 'contemporaneous data' that means the data should be recorded at the time it is generated. The principle is known as the C of ALCOA principles, which gives a set of guidelines to ensure Data integrity (see [10, 11, 12]) in GxP practices, such as GMP, GLP, and GCP. Although the challenges are similar, we have not found any relevant studies in the field of data integrity that correspond to our third-party validation. Still, we have seen similar system development. For instance, a blockchain-based monitoring system for pharmaceutical manufacturing lines [13] performs integrity inspections of reports from various parts of the lines in real-time and conducts monitoring to reduce risks.

VI. DISCUSSION AND CONCLUSION

We add some remarks and future works, and then conclude.

1. The design choice of implementing local application on PCs was made to connect additional equipment and extract data from them, not just from temperature and humidity loggers.

2. We recall a point of validation that the third party implements checks in the validation based on the information gathered from the laboratory. We also remind the laboratory to consider and decide on corrective actions regarding the validation results in advance when implementing the system.

3. The development of the case is completed, but it has not been deployed and put into actual operation with the calibration service. The actual operation will be our future works.

4. The present case was provided with minimal security measures since we did not anticipate the presence of malicious members in the laboratory, such as those who report false activities or falsify results. Security measures for them will be future works too.

5. For an application of the third-party validation results, another futuer work will be to design a service of the third-party organization to endorse the calibration results to the customer.

In the present study, we have developed a new case of integrating third-party validation into calibration service for purity. The case addressed the identified challenges of both frequent validations and information leakage-free. The information leakage-free was instantiated by checking the data inside the laboratory and eliminating, originally,

customer and laboratory information from the data transferred to outside. The case broadens the applications of our developing approach.

REFERENCES

[1] K.Shirono, N.Takegawa, M.Moni, D.Peters, “DESIGN OF THE DIGITALIZED CONFORMITY ASSESSMENT FOR LABORATORY ACTIVITIES IN INDIVIDUAL CERTIFICATIONS”, Proc. of M4Dconf2022., September 2022, doi:10.21014/tc6-2022.009.

[2] K.Shirono, A.Hirai, G.Matsui, O.Sato, H.Watanabe, T.Takatsuji, T.Fujimoto, “Proof of concept for the digitalized certification of measurement data: An example of vernier-caliper calibration”, AMCTM XIII, World Scientific, 2025, pp. 260-267, doi:10.1142/9789819800674_0024.

[3] S.Igari, H.Watanabe, T.Fujimoto, K.Shirono, “Quality-compliance validation system for individual calibration and testing events: case study of primary calibration of reference photovoltaic devices”, Meas. Sci. Technol., vol. 36, March 2025, doi:10.1088/1361-6501/adb643.

[4] D. Peters, J. Wetzlich, F. Thiel and J. -P. Seifert, "Blockchain applications for legal metrology," 2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Houston, TX, USA, 2018, pp. 1-6, doi:10.1109/I2MTC.2018.8409668.

[5] W. S. Melo, A. Bessani, N. Neves, A. O. Santin and L. F. R. C. Carmo, "Using Blockchains to Implement Distributed Measuring Systems," in IEEE Transactions on Instrumentation and Measurement, vol. 68, no. 5, pp. 1503-1514, May 2019, doi:10.1109/TIM.2019.2898013.

[6] W. Melo, R. C. S. Machado, D. Peters and M. Moni, "Public-Key Infrastructure for Smart Meters using Blockchains," 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, Roma, Italy, 2020, pp. 429-434, doi:10.1109/MetroInd4.0IoT48571.2020.9138246.

[7] The Physikalisch-Technische Bundesanstalt, Digital Calibration Certificate (DCC) - Wiki, https://wiki.dcc.ptb.de/.

[8] Schilling, M., Bruns, S., Bayerlein, B., Kryeziu, J., Schaarschmidt, J., Waitelonis, J., Dolabella Portella, P. and Durst, K. (2025), Seamless Science: Lifting Experimental Mechanical Testing Lab Data to an Interoperable Semantic Representation. Adv. Eng. Mater., 27: 2401527. doi:10.1002/adem.202401527.

[9] Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3, 160018 (2016). doi:10.1038/sdata.2016.18.

[10] U.S. Department of Health and Human Services Food and Drug Administration, Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry, 2018, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers.

[11] Medicines and Healthcare products Regulatory Agency, Guidance on GxP data integrity, 2018, https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity.

[12] World Health Organization, TRS 1033 - Annex 4: WHO Guideline on data integrity, 2021 https://www.who.int/publications/m/item/annex-4-trs-1033/.

[13] Durá, M., Leal, F., Sánchez-GarcÃa, Á. et al. Blockchain for Data Originality in Pharma Manufacturing. J Pharm Innov 18, 1745-1763 (2023). doi:10.1007/s12247-023-09748-z.