IMEKO TC6 International Conference on Metrology and Digital Transformation
September 19 – September 21, 2022, Berlin, Germany

DESIGN OF THE DIGITALIZED CONFORMITY ASSESSMENT FOR LABORATORY ACTIVITIES IN INDIVIDUAL CERTIFICATIONS

Katsuhiro Shirono [a, *], *Naoki Takegawa* [a], *Mahbuba Moni* [b], *Daniel Peters* [b]

[a]National Institute of Advanced Industrial Science and Technology (AIST)/ National Metrology Institute of Japan (NMIJ), Tsukuba, Japan
[b]Physikalisch Technische Bundesanstalt (PTB), Berlin, Germany
[*]Corresponding author. E-mail address: k.shirono@aist.go.jp

Abstract – Product certifications are conformity assessments for items. In the testing for the product certification, the managerial and technical procedures are validated through another conformity assessment, the accreditation of the testing laboratory. The review for the accreditation is implemented once a few years. The digitalized history of the laboratory activities (e.g. the external and internal reviews, the training, and the calibrations) can be helpful to check the quality of the testing for individual product certifications. In this report, we discuss what data has to be assessed and how security mechanisms can be implemented.

Keywords: conformity assessment, accreditation, digital calibration certificate, blockchain, product certification

1. INTRODUCTION

Product certifications are given to assure the quality of items. For customers, quality of the certification process including the testing is an important issue. Often we establish guidelines for testing laboratories to show the quality of the testing process. In particular when the quality assurance on the certifications is required in a relatively rigour manner, the third-party accreditation is required for the testing laboratories.

In an accreditation process, the competence of a testing laboratory is checked from the managerial and the technical aspects. Since a lot of records must be reviewed in the process, digitalizing the information may be helpful for computer programs to check the appropriateness of the records in an automatic way. The digital techniques seem thus to be helpful to reduce the workload of the reviewers in the present conformity assessment processes. Some ideas have also been suggested elsewhere [1].

The digitalization can bring more value than those provided in ongoing activities. The cheaper cost of running the programs than the reviewers' assessment may accelerate frequent checkings of the laboratory activities. In the present stage, the external review on them is implemented only once a few years. However, customers may have interest only in the performance of the laboratory at the time of the one certification process regarding their items.

We propose the conformity assessment on the laboratory activities on the testing for individual product certifications with using digitalization techniques. This system can relate to the following two conformity assessments; (1) the conformity assessment on the laboratory activities (the accreditation), and (2) that for an item or items (the product certification). We discuss what data to be assessed and how the security of them should be.

2. FLOW OF THE DIGITALIZED CONFORMITY ASSESSMENT

Figure 1 shows the procedural flow of our idea for the conformity assessment. Our idea is that not the whole accreditation procedure but some parts of it are implemented automatically by an assessment program. The residual parts are assessed by qualified reviewers, but the assessment results are given in a digital format. Not only the accreditation body but other institutes like proficiency test providers and calibration laboratories can contribute to this system. Once those types of information is generated, they are given to the testing laboratory. The external review information is hence sent to the testing laboratory only when the review is conducted, i.e. once a few years.

The assessment program is provided as an internet application. On every testing, the testing laboratory complies all the relevant information and sent to the server with the assessment program through the internet. The details will be given in the following sections.

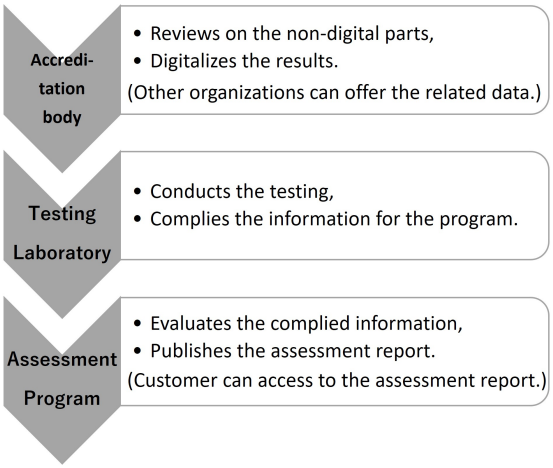

Fig. 1: Flow diagram of the procedure considered for the digitalized conformity assessment in this report.

3. SUGGESTIONS ON THE DATA TO BE ASSESSED IN THE PROGRAM

3.1. Measurement data

The measured data obtained from measurement devices are assessed in the assessment program. For example, in volume measurements with the gravimeteric method, the volumetric apparatus is checked by using pure water in accordance with ISO 8655 Part 6 [2]. The mass of pure water is converted to the volume through its density, which is the function of the water temperature. Moreover, for corrections, the air temperature, the relative humidity, and the air pressure are measured. In this case, we need the values measured by the mass scale, the thermometers for air and water temperatures, the hygrometer, and the pressure gauge.

The volume V is computed as

$$V = m \cdot Z \cdot Y, \tag{1}$$

where Z and Y are the conversion and the correction factors as the functions of the air and water temperatures, the relative humidity, and the air pressure. The measurement of these properties are often repeated. Ten repetitive mass measurements are implemented for a micro-pipette calibration, and the average of the ten repetitive measurements are employed in the computation in ISO 8655 Part 6. It seems preferable that not the testing laboratory but the assessment program conducts the computation of (1) to assure that the computation is implemented properly. Instead of the value of V, the values of all potentially involving data should hence be used as the inputs for the program.

In accordance with ISO 8655 Part 6, the difference between the measured and the nominal volumes is checked. The magnitude is compared with a criteria called the maximum permissible error. If the magnitude is larger than that value, the micropipette is deemed to be non-conforming. The evaluation is implemented in the assessment program.

Reporting all potentially involving data is meaningful not only for the computation of the measured value but also for the checking of the marginal experimental conditions. For example, in ISO 8655 Part 6, it is stipulated that the air temperature should be $15\,^{\circ}\mathrm{C}$ to $30\,^{\circ}\mathrm{C}$. When reporting the measured air temperature, the assessment program checks these conditions. We thus ensure the validity that the measurement results are obtained under the conditions the standard requires.

Although the evaluation on the experimental conditions can be done even without the digitalization techniques, the marginal experimental conditions have been sometimes overlooked in actual processes. Our proposing system prevents testing laboratories from conducting non-conforming practices by mistake. The digital expression may be useful to assure non-tampering on the data by using appropriate techniques as the time stamp and the blockchain system.

3.2. Other data involving laboratory activities

The checking of the measurement data shown in subsection 3.1 has actually also been conducted in present product certification processes, even though it can be done in a more efficient way by digitalization. Our proposal is rather valuable in terms of the use of the digitalized information on the laboratory activities in the testing for individual product certifications. In Listing 1, we show an example of the laboratory activity data. In this data, the registration of the testing laboratory is shown. The data corresponds to the assessment results checked by the qualified reviewers mentioned in Section 2.

In the data under “<dcaLabo:Info>”, we created the elements tagged with “<dcaLabo:Id>”, “<dcaLabo:Data>”, “<dcaLabo:Status>”, “<dcaLabo:RegTime>”, and “<dcaLabo:ChgTime>”. The element tagged with “<dcaLabo:Content>” under the Data element includes the main data for the registration. The main data consists of the laboratory identification in the system, the laboratory name, the event, the scope of the registration, the measurand, the accredited volume range, the event time, and so on. For the volume range, the format proposed in the SmartCom project [3] is employed.

Other than the Content element, there are the elements tagged with “<dcaLabo:CertId>”, “<dcaLabo:Publisher>”, “<dcaLabo:Cert>”, and “<dcaLabo:Sign>” under the Data element. They are for the validation of the authenticity of the provided data. Anyone can make fake data matching the specific data format. To prevent the inappropriate data fabrication, a digital signature is used. We assume that the certificate of the digital signature has been registered so that we can check the authenticity.

Using this accreditation data, the assessment program can check the validity of the accreditation information given by the accreditation body. For example, it checks if the nominal volume of the certified volumetric apparatus is in the accredited range or not. If not, the result is given to be invalid. Moreover, if the validity of the registration has expired or if the authenticity of the registration data cannot be confirmed, the program concludes that the testing process is non-conforming. We can thus check the conformity of the procedures from the managerial point of view regarding the testings of individual product certifications.

The shown format is just an example. We believe that some other information may be required for actual conformity assessments. There are valuable data to be assessed for the testing laboratory activities such as data involving the participation to the proficiency test, the training of the personnel, and the calibrations. The calibration information may be given by the digital calibration certificates [4]. Our idea is that through checking those data, we can show the reliability of the certification procedures in a visible way using the digitalization techniques.

Listing 1: Example of the digital information for the laboratory activity; the registration by the accreditation body. The data of the certification for the digital signature in <dcaLabo:Cert> is omitted.

```
<dcaLabo:Info>
    <dcaLabo:Id>Labo1641067237490</dcaLabo:Id>
    <dcaLabo:Data>
        <dcaLabo:Content>
            <dcaLabo:LaboratoryId>Labo12345
                </dcaLabo:LaboratoryId>
            <dcaLabo:LaboratoryName>
                ABC_Testing
            </dcaLabo:LaboratoryName>
            <dcaLabo:Event>
                Registration</dcaLabo:Event>
            <dcaLabo:Personnel>
                ALL</dcaLabo:Personnel>
            <dcaLabo:Scope>ISO_8655
                </dcaLabo:Scope>
            <dcaLabo:Measurand>Volume
                </dcaLabo:Measurand>
            <dcaLabo:RangeMin>
                <si:real>
                    <si:label>volume</si:label>
                    <si:value>1</si:value>
                    <si:unit>\micro\litre
                        </si:unit>
                </si:real>
            </dcaLabo:RangeMin>
            <dcaLabo:RangeMax>
                <si:real>
                    <si:label>volume</si:label>
                    <si:value>10000</si:value>
                    <si:unit>\micro\litre
                        </si:unit>
                </si:real>
            </dcaLabo:RangeMax>
            <dcaLabo:Principle>ISO/IEC_17025
                </dcaLabo:Principle>
            <dcaLabo:EventTime>
                2021-12-01T10:00:00Z
            </dcaLabo:EventTime>
            <dcaLabo:Note>None</dcaLabo:Note>
            <dcaLabo:Salt>@xb</dcaLabo:Salt>
        </dcaLabo:Content>
        <dcaLabo:CertId>
            Cert1635760800000</dcaLabo:CertId>
        <dcaLabo:Publisher>
            LMN_Service</dcaLabo:Publisher>
        <dcaLabo:Cert>
            -----BEGIN CERTIFICATE-----  ...
            -----END CERTIFICATE-----
        </dcaLabo:Cert>
        <dcaLabo:Sign>
            MEYCIQDivQO2i7H1EIOYZIpqiRl0mdSr+7
            hlMQBtsXBmLgmN+wIhAJ/hxC0u1JDVtqNE
            kueBpvCiMEL6VpgcI2O/BLAY7oWC
        </dcaLabo:Sign>
    </dcaLabo:Data>
    <dcaLabo:Status>valid</dcaLabo:Status>
    <dcaLabo:RegTime>
        2022-01-01T20:00:37.490Z
    </dcaLabo:RegTime>
    <dcaLabo:ChgTime>
        2022-01-01T20:00:37.490Z
    </dcaLabo:ChgTime>
</dcaLabo:Info>
```

4. AVAILABILITY AND SECURITY OF THE DATA AND THE ASSESSMENT PROGRAM

4.1. Open database for the digitalized conformity assessment

For the conformity assessment, the validity of the provided data is important. It can happen that the data which have once been published are corrected or nullified. We consider to use an open database to show the validity of the data. However, it may be unrealistic to make the data open to the public because the data involving the product certification can contain highly confidential information. We must consider a good balance between the usage of data and the protection of privacy.

To check the validity of data on an open database, we suggest not to publish the data itself but the hash of it openly through the database. The SHA256 hash of the data under the tag of "<dcaLabo:Data>" in Listing 1 is

ebc36a39ac6543d4c20e8f272f68c3f42
488db78eb26468ad9f88762b3e11c1f.

Even if this hash data is open to the public, no private information is shown. In our idea, with the id of "Labo1641067237490", we can access the data of

```
{
    Id: "Labo1641067237490",
    Hashdata: "ebc36...e11c1f",
    Status: "valid",
    RegTime: "2022-01-01T20:00:37.490Z",
    ChgTime: "2022-01-01T20:00:37.490Z"
}.
```

The Status property shows the validity of the data. We propose a system in which we can change the validity of the information. When serious problematic issues about the information on "Labo1641067237490" are found, the administrator of the system can nullify the validity of the data. The RegTime and ChgTime properties show the time of recording and changing the status, respectively. It is technically possible to delete the data from the database, while deleting impairs the find-ability of the data.

Needless to say, we can control which data is open to the public. The disclosure of some parts of the data may motivate people to develop new valuable applications. The proposed system can realize the minimum functionality for the conformity assessment, with which we can check the latest status of the data.

Furthermore, when we run the database with the time provided by a time assessment authority, the time of the data on the database can ensure the status of the data at the shown time. It is an option to use a blockchain system instead of the time assessment authority.

4.2. *Assessment program for the digitalized conformity assessment*

Although we propose that only the hash is recorded in the open database, the data itself should be sent to the server with the assessment program. We assume the assessment program is run by servers of a highly reliable organizations in terms of security. However, some additional approach to enhance the security may be preferable.

First we must protect the integrity of the assessment program. If the program is changeable without leaving the history, the assessment results are no longer reliable. For this purpose, the blockchain technique may be a solution. In blockchain systems, the programs are usually deployed before running, and the deployment leaves the history. A participant organization cannot therefore change the program by their own.

When the integrity of the assessment program can be established, we can enhance the protection of the data to be inappropriately intercepted by the participants in the blockchain system. The details are shown in the Japanese patent which one of the authors submitted [5]. The points are follows:

1. An intermediate organization between a testing laboratory and the servers with the assessment program is set,
2. The encrypted data set to be decrypted only in the assessment program is sent from a testing laboratory to the intermediate organization,
3. The intermediate organization invokes the assessment program without sending the data at this stage,
4. A private and public key pair is randomly generated in the assessment program for the connection between the intermediate organization and the server,
5. The assessment is implemented after the intermediate organization's sending the data set (doubly) encrypted with the public key, and
6. The data set is deleted at the end of the assessment program from the servers.

Thus, we can achieve the conformity assessment without showing the data set.

In fact, the fully homomorphic encryption, the zero knowledge proof technique, and other relevant techniques are available for this purpose. They may be more preferable than the method we propose. We however believe that the cost including the computation time of these techniques is unrealistically large at the present stage. Thus, we propose the above, just as a tentative technique.

5. DEMONSTRATION

We have developed the prototype system using the blockchain technique to realize the concept proposed in this paper as shown in Fig. 2. We use Hyperledger fabric [6] for this purpose, which is one of popular blockchain platforms.

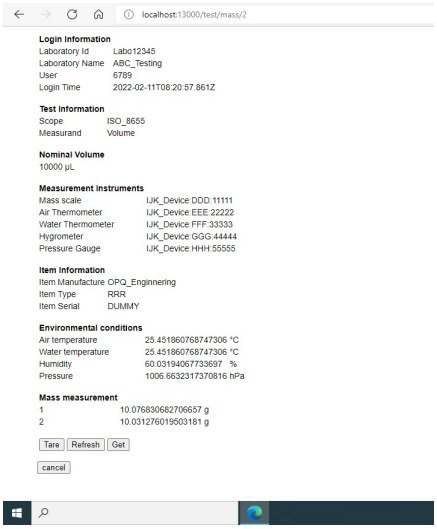

Fig. 2: Screenshot of the prototype system.

ACKNOWLEDGEMENTS

This work was supported by JSPS KAKENHI Grant Number JP20K04997.

REFERENCES

[1] Pysikalisch-Technishe Bundesanstalt, Into the Future with Metrology - The Challenges of Digital Transformation, https://www.ptb.de/cms/en/research-development/into-the-future-with-metrology/the-challenges-of-digital-transformation.html (accessed 15 Feb 2022).

[2] International Organization for Standardization (ISO), *ISO 8655-6:2002 Piston-operated volumetric apparatus - Part 6: Gravimetric methods for the determination of measurement error*, ISO, Geneva, 2002.

[3] The European Association of National Metrology Institutes, Communication and validation of smart data in IoT-networks, https://www.euramet.org/research-innovation/search-research-projects/details/project/communication-and-validation-of-smart-data-in-iot-networks/ (accessed 15 Feb 2022).

[4] G. Hackel, F. Härtig, J. Hornig, and T. Wiedenhöfer, "The Digital Calibration Certificate", *PTB-Mitteilungen*, vol. 127, pp.75-81, 2017.

[5] Katsuhiro Shirono, Information processing system (Toku-gan 2021-052208), 2021.

[6] Hyperledger foundation, Hyperledger Fabric - Hyperledger Foundation, https://www.hyperledger.org/use/fabric (accessed 15 Feb 2022).