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

Digital Transformation: Interoperable processes and services based on a cloud native architecture

Alexander Reissert [1], Samuel Eickelberg [1], Petra Tsesmetzi[1], Abdul Rehman[1]

[1]*Physikalisch-Technische Bundesanstalt, Abbestr. 2-12, 10587 Berlin, alexander.reissert@ptb.de*

***Abstract* – In accordance with the Unix philosophy, the implemented software architecture guidelines are designed to prioritise simplicity, modularity and composability. The objective is to develop services that excel in a specific area, with the ability to integrate seamlessly with other services to manage complex tasks.**

In this paper, we address the issues of interoperability and cross-institutional data sharing by proposing a cloud-native software architecture, the Operation Layer. This innovative solution integrates standalone legacy IT systems and paves the way for a comprehensive digital transformation. Furthermore, the revised and extended digital calibration workflow illustrates the potential of interoperable processes.

I. INTRODUCTION

It is an unavoidable fact that all organisations have legacy software and information architectures in place, and that these will continue to grow over time. New information systems will be introduced to solve a further set of problems. However, the exchange of data between these systems is negligible. It is not automated, and nor has it ever been intended. Data sharing within organisations can present certain challenges. Across institutions and other fields, it is not yet a common practice.

It is evident that digital transformation encompasses more than merely the digital support of processes or the digitisation of documents. Rather, it signifies a comprehensive transformation of the organisational structure and working environment, thereby facilitating streamlined and more efficient workflows.

In essence, the implementation of digital transformed and interoperable processes will facilitate the generation of new data and information regarding procedures and systems in real time. This, in turn, will generate new insights and information, which will result in improvements and innovation. This data tier provides a solid foundation for emerging technologies, such as machine learning and artificial intelligence [1].

However, the quality of the data is a key factor in determining the usefulness and outcome of the digitally transformed processes. This is a well-known input-output problem that has become more prominent due to the increased availability of large data sets. The creation of a digital ecosystem is intended to facilitate seamless communication and collaboration among all active participants.

Physikalisch-Technische Bundesanstalt (PTB) is undergoing a progressive digital transformation, encompassing its working groups, laboratories and workflows. This initiative is being implemented to enhance operational efficiency, facilitate seamless data exchange, and ensure the integrity and quality of data. The staff have expressed concerns about the change management process and the individual workflows of the highly specialised working groups, suggesting that these may present an insurmountable challenge.

The Operation-Layer (OP-Layer) is a proposed solution to address the integration problem by bridging the gap between information systems. It achieves this through a highly scalable and distributed architecture consisting of loosely coupled services. The OP-Layer provides highly adaptable services for the horizontal communication flow of working groups, integrating and enabling vertical communication via APIs to other information systems and departments. The OP-Layer is an integration layer that comprises services and APIs. It can also be described as a data tier that lays the foundation for a coherent and consistent digital transformation.

II. INTEROPERABLE PROCESSES

According to Cambridge Dictionary [2], the term "interoperability" is defined as "the degree to which two products, programs, etc. can be used together, or the quality of being able to be used together".

Interoperability can be viewed from four distinct perspectives: technical, syntactical, semantic and organisational. The following descriptions are taken from the ETSI white paper [3] and are intended to facilitate understanding of the complexity.

> **Technical Interoperability** is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to take place. This kind of interoperability is often centred on (communication) protocols and the infrastructure needed for those protocols to operate.
>
> **Syntactical Interoperability** is usually associated with data formats. Certainly, the messages transferred by communication protocols need to

have a well-defined syntax and encoding, even if it is only in the form of bit-tables.

Semantic Interoperability is usually associated with the meaning of content and concerns the human rather than machine interpretation of the content. Thus, interoperability on this level means that there is a common understanding between people of the meaning of the content (information) being exchanged.

Organisational Interoperability, as the name implies, is the ability of organisations to effectively communicate and transfer (meaningful) data (information) even though they may be using a variety of different information systems over widely different infrastructures, possibly across different geographic regions and cultures. Organisational interoperability depends on successful technical, syntactical and semantic interoperability.

In this paper, the concept of interoperability is constrained to the realms of technical and syntactical interoperability. The primary focus is on harmonised interfaces and data exchange formats. In order to implement interoperable processes successfully, it is essential that the organisational dimension is resolved at a management level. In the absence of interdepartmental interoperability, it is implausible that any technical solution will be capable of overcoming this issue, let alone one that is applicable to different institutions.

Moreover, the term 'interoperability' already suggests the existence of a complex process with multiple subprocesses that must interlock seamlessly. The data are of paramount importance and are invariably intended for a specific purpose. Depending on the initial request, the items are frequently transported and converted during the evaluation process. Nonetheless, it is imperative to ensure the integrity of the data throughout the entire of the process chain. In the context of complex process chains, data is generated from a multitude of sources, employing a variety of methodologies and created by different individuals. These data are subsequently compiled and evaluated in a unified manner. In order to facilitate a successful and harmonised digital transformation of complex processes, it is imperative to undertake a comprehensive analysis of the entire lifecycle of the required and processed data. It is essential that this data is standardised, universally machine-readable, and internationally recognisable as far as possible with regard to future extensions [4].

In consideration of the aforementioned factors, the selection of an appropriate IT infrastructure is imperative that facilitates the management of the data in question, in conjunction with the implementation of suitable interfaces for the purpose of modularisation. It is evident that, with the establishment of a suitably flexible system structure, a multitude of individual processes will be able to be combined in a harmonious manner in the future. The aforementioned interoperability presents a series of opportunities, including the potential for the development of existing infrastructures, the adaptation to novel developments, and the provision of support for the future digital metrology quality infrastructure. [5]

III. CLOUD NATIVE ARCHITECTURE

The Operation Layer (OP-Layer) employs the concept of a central business process middleware or integration layer in a research environment characterised by highly specialised, tailored applications. Rather than using off-the-shelf software, open-source components are employed to address the specific requirements of the research institute and the metrology domain. The OP-Layer constitutes a platform of interconnected, yet loosely coupled services, the purpose of which is to facilitate interaction for a variety of interoperable processes across multiple departments and laboratories within PTB. The following elements are to be considered in order to ensure the effective management of data:

- The harmonisation of data structures and flows through standardised interfaces (REST, JSON),
- Security and traceability are to be ensured by using state-of-the-art single sign-on identification (OpenID [6],
- Direct communication with the electronic file system ("E-Akte") is to be facilitated, and
- High availability and scalability are to be guaranteed through deployment in a managed cluster environment.

All services constituting OP-Layer's interconnected service landscape adhere to the same coding guidelines, module structure, and communication interface design. It is evident that all services are developed in two artefacts: a service and a service-API artefact. The former comprises all the business logic that is required, in addition to a data layer and REST controllers, if these are deemed necessary. The latter consists of the API features that are required in order to communicate with the service. The aforementioned elements comprise data transfer objects (DTOs), client classes that serve as the one-to-one counterparts to the service's REST controllers, controller routes, and other configuration items.

JSON Web Tokens (JWTs) are used to prevent unauthorised access to and among the services. These tokens include the rights and roles of the user initiating the request. Each request header contains such a token. The

service receiving the request will interpret it. PTB operates its own identity provider. This is used to grant federated users specific rights and roles. These are tailored to the services. It also allows PTB to trace each operation back to a user. Use the OpenID-based identity and access management solution Keycloak, which is part of the commonly used resources within OP-Layer. This achieves the required result.

The Kubernetes design principles[1] fulfil the majority of the aforementioned requirements for a modern distributed infrastructure approach [7]. The subsequent bullet points delineate the requisite criteria:

- **Scalability** - is defined as the ability to expand or grow in size or capacity. In the context of applications, scalability refers to the capability of a system to handle increasing demand or workload. Horizontal scaling, a method of enhancing scalability, involves the execution of the same application multiple times. This approach ensures that the application's request load is distributed across multiple instances, thereby mitigating the impact of high demand. It is evident that Kubernetes is equipped with the inherent functionality of load balancing and horizontal scaling capabilities, which are available without the necessity for additional configuration or customisation.
- **Portability** - Deployment operations have undergone significant changes. Containers and pods enable applications to run on any platform and cluster. Kubernetes provides a range of container runtimes, facilitating application portability and straightforward deployment for an agile development approach.
- **High Availability** - It should be noted that backups and replicas address the high availability requirement. Whilst backups concentrate on data restoration at a specific point in time, replicas support business continuity. Kubernetes is designed to ensure high availability at both the application and infrastructure level.
- **Security** - It is essential that security be addressed at the cluster, application and network levels. Furthermore, it is imperative to implement stringent rights and role management for each user, thereby ensuring that only authorised operations are executed by applications in the cluster. In a distributed architecture with loosely-coupled services, a session-less authentication and authorisation approach using tokens, which are placed in each HTTP REST request, has proven itself to be state-of-the-art. This approach ensures that each operation can be traced back to the user initiating any defined process in any use case. Moreover, the API endpoints are secured via Transport Layer Security (TLS).

[1] https://kubernetes.io/docs/concepts/overview/

IV. SERVICE INFRASTRUCTURE

This section outlines the most significant services that have been implemented to date and those that are scheduled for completion within the current year. During implementation, great care was taken to ensure that these were implemented as generically as possible so that the code base can be reused in other use cases.

A. *E-File*

The E-File is an integrated service for electronic file management. It is based on a structured filing system for secure, revision-safe file management. In addition, the E-File provides functionalities for collaboration and support for case processing and special procedures.[2]

The interoperability of processes is best shown when using E-File, as it is the center piece of numerous procedures within PTB. So whenever documents and attached meta data are part of a procedure, there will be interoperability between E-File service and other services within OP-Layer. Every described use case described in this paper interoperates with E-File.

B. *DigiSeal*

Establishing a digital workflow by interconnecting different information systems with a central electronic sealing capability is the key design aim for a formal process. Currently, two file types are supported: PDF files allow embedding electronic seals from the PDF/A-1 standard onward. Digital Calibration Certificate (see section v.) XML files can also take an embedded electronic seal according to the W3C XML Signature[3] recommendation.

The Digital Seal Service within OP-Layer [8] interacts with E-File Service in the following way. Digital Seal Service is job-controlled, meaning that it checks periodically via E-File Service for circulars containing documents to seal. The interoperability between E-File and DigiSeal through OP-Layer occurs as follows:

1. The service receives circulars directed at the organizational unit (OU) "Siegelstelle" (sealing authority), and extracts documents in these circulars.
2. The service opens the documents, extracting any records, as actual physical files, such as PDF or XML, from them.
3. Digital Seal Service sends theses files to *digiSeal server* through its proprietary SOAP interface. The *digiSeal server* is a third-party product developed by secrypt GmbH[4]. PTB runs a server instance, as part

[2] https://www.bva.bund.de/DE/Services/Behoerden/Verwaltungsdienstleistungen/E-Akte/e-akte_node.html

[3] https://www.w3.org/TR/xmldsig-core/

[4] See https://www.secrypt.de/en/homepage/

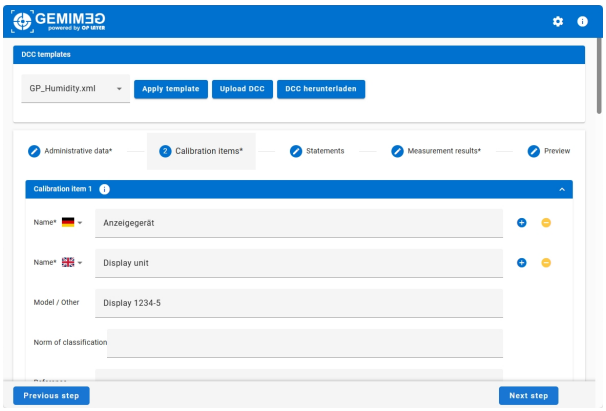

Fig. 1. GEMIMEG 2.0 Tool Editing Mode

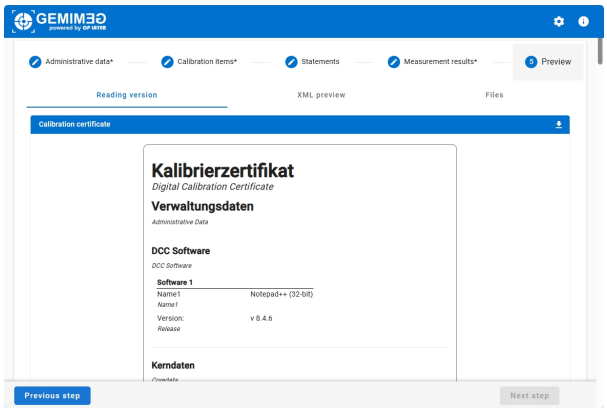

Fig. 2. GEMIMEG 2.0 Tool Preview Mode

of the central OU "Siegelstelle".

4. The sealed files are placed in the documents, which were received though steps one and two. The E-File Service then redirects the circular(s) to the respective initiator(s) of the original procedure(s).

C. Certificates and ID generation

Every report, certificate, conformity declaration and other such documents have unique identifiers, which follow specific patterns, depending on the type of document, and the issuing department. The identifier generation patterns have been implemented in a backend service within OP-Layer, which not only generates new document identifiers, but also stores already generated ones in order to keep them unique. This service, called *Document ID generator*, can interoperate with E-File, when a document, which is to be a result of e. g. a calibration procedure. The resulting calibration certificate will then receive a unique document identifier from Document ID generator, and, if required, an electronic seal from Digital Seal Service (see section iv.-B.).

For measurement instruments, calibration and conformity certificates are issued by PTB. They are stored in a central database called the *MICert* database. The OP-Layer service to manage certificates in this database is currently under development. It will automatically, and periodically pull any new certificates from E-File and store them in the MICert database. The database has a publicly available web interface for customers and other authorities, so keeping it up-to-date is another aspect of how interoperability advances digital transformation.

V. DIGITAL CALIBRATION CERTIFICATE WORKFLOW

As part of the digital transformation strategy and propagation, the Digital Calibration Certificate (DCC [9]) serves as the cornerstone to provide a digital document format for official calibration certification. As it is XML-based, DCC allows for machine-readable, interoperable data exchange. The first showcase implementation of DCC within OP-Layer was concerned with calibration applications submitted via the E-Service Portal, forwarding its data via E-File to the calibration laboratory and providing a valid DCC [7], [10].

At the current stage of development, the use of DCCs is integrated into several processes already in place within OP-Layer. The following sections describe the usage and integration of DCCs in different use cases.

A. Embedded electronic seal

For processing DCC XML files, a document in E-File must contain a DCC XML file which is to be sealed. The Digital Seal Service will check though the DCC Service, if the provided XML is a valid DCC according to the DCC schema. If this is the case, Digital Seal Service will process it further according to steps three and four, as described in section iv.-B..

B. Gemimeg Tool 2.0

The GEMIMEG Tool 2.0[5] is a stand-alone version of two components: A frontend and a backend service. The frontend contains everything required to run the DCC display and editing components as an Angular[6] service. The backend contains the DCC Service and in addition the Cache Service as well as several common components, integrated within one backend instance. OP-Layer's security components are not part of this version, because its main goal is to be able to run independently even on client computers, which don't need to be connected to the internet. Figure 1 shows the editing of a DCC conveniently in a browser window. It currently supports five languages: English, German, French, Spanish and Portuguese, in order

[5] https://gemimeg-tool.ptb.de
[6] https://angular.dev/

to address different NMIs and related institutions around the globe.

The GEMIMEG Tool also has a preview mode, so that the currently edited DCC can be previewed in a human-readable form. This preview can also be downloaded as PDF. The preview mode is white-labeled, so that an institution wishing to use the tool to generate DCCs can place their own logo in the resulting documents. Figure 2 shows the white-labeled preview mode in a browser window.

Carving out the backend DCC and Cache Services from OP-Layer's backend service ecosystem is comparably easy, as they are already loosely coupled and communicate via open and harmonized RESTful interfaces. The only integration that was made is integrating both Cache and DCC services into one GEMIMEG Backend service. As mentioned above, the security features comprising of JWT-based authentication and IAM (Identity Access Management) integration (e.g. Keycloak) have been entirely removed from the code base.

The frontend separation required to first create a library of re-usable components for Angular, and make it available for NPM[7] so that it can be integrated within OP-Layer's frontend as well as GEMIMEG frontend from the same code base. This way, and feature development and maintenance done for one of them automatically finds their way into the other.

C. SI Digital Framework

The DCC schema uses the D-SI schema to include dimensions. By doing this, the DCC service interoperates with another OP-Layer backend service, the D-SI service. It validates SI units, assures correct conversions and verifies number formats [11].

VI. CONCLUSIONS AND FUTURE WORK

In this paper, the concept of interoperability is introduced and defined in terms of technical and syntactical interoperability. To ensure the profitable implementation of interoperable processes, the primary focus should be on harmonised interfaces and data exchange formats. Furthermore, to implement interoperable processes successfully, it is essential that the organisational dimension is resolved at a management level. In the absence of interdepartmental interoperability, it is implausible that any technical solution will be capable of overcoming this issue, let alone one that is applicable to different institutions.

If a process management system is in place that ensures linear and concise processes with clearly defined responsibilities, then the proposed business process middleware Operation Layer can unfold its full potential in a cross-institutional data sharing infrastructure. This paves the way for a holistic digital transformation of a highly automated infrastructure, with data sharing at its core. Enabling future projects such as predictive and automated calibration of measuring instruments.

[7]Node Package Manager is the recommended package manager for Node.js, which Angular is built on.

REFERENCES

[1] Christoph Jacob. Designing innovative ecosystems and introducing digital smart services using examples of the value chain from building investor to facility management. *Creating Innovation Spaces: Impulses for Start-ups and Established Companies in Global Competition*, pages 99–117, 2021.

[2] Cambridge English Dictionary. Meanings & definitions, 2025. https://dictionary.cambridge.org/dictionary/english/interoperability?q=Interoperability [Accessed: (2025-04-28)].

[3] Hans Van Der Veer and Anthony Wiles. Achieving technical interoperability. *European telecommunications standards institute*, 2008.

[4] C Kulka-Peschke, S Eickelberg, A Keidel, M Meiborg, and A Oppermann. A1. 3-digital transformation of processing metrological services. *Lectures*, pages 33–34, 2023.

[5] Anke Keidel and Sascha Eichstädt. Interoperable processes and infrastructure for the digital transformation of the quality infrastructure. In *2021 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0 & IoT)*, pages 347–351, 2021.

[6] Alexander Oppermann and Samuel Eickelberg. Digitale Transformation in der Metrologie: Harmonisierung digitaler Identitäten mittels OpenID. *Werkwandel - Zeitschrift für angewandte Arbeitswissenschaft - Ausgabe #1 - Februar,2022*, pages 26–30, 2022.

[7] Alexander Oppermann, Samuel Eickelberg, and Manuel Meiborg. Digital transformation: Towards process automation in a cloud native architecture. *Acta IMEKO*, 12(1):1–6, 2023.

[8] Alexander Reissert, Anke Keidel, and Samuel Eickelberg. Digital transformation: Building an event driven electronic seal service within a cloud native metrological ecosystem. *Measurement: Sensors*, page 101489, 2024.

[9] Siegfried Gustav Hackel, Frank Härtig, Julia Hornig, and Thomas Wiedenhöfer. The digital calibration certifcate. *PTB-Mitteilungen*, 127(4):75–81, dec 2017.

[10] Samuel Eickelberg, Thomas Bock, Matthias Bernien, and Alexander Oppermann. Integrating a calibration labaratory worflow into a metrological digital ecosystem: A case study. *Acta IMEKO*, 12(1):1–6, 2022.

[11] Richard JC Brown, Jan-Theodoor Janssen, and Louise Wright. Why a digital framework for the si? *Measurement*, 187:110309, 2022.