ACTA IMEKO
ISSN: 2221-870X
March 2023, Volume 12, Number 1, 1 - 6

Digital transformation: Towards process automation in a cloud native architecture

Alexander Oppermann[1], Samuel Eickelberg[1], Manuel Meiborg[1]

[1] *Physikalisch-Technische Bundesanstalt, Abbestr. 2-12, 10587 Berlin, Germany*

ABSTRACT
Introducing new information systems in organizations often result in information sinks that disrupt people's productivity and prevent a successful change management process. In this paper, the *Operation Layer* is presented, a Cloud Native concept to break up data silos, to streamline workflows and to centralize IT services while maintaining the department's workflows. The feasibility is demonstrated by a complete digital calibration certificate workflow implementation as a service within the Operation Layer. Pursuing this concept consequently will simplify the IT maintenance while flattening the change management curve at the same time.

Section: RESEARCH PAPER

Keywords: digital transformation; universal service hub; metrological processes; digital calibration certificate; DCC

Citation: Alexander Oppermann, Samuel Eickelberg, Manuel Meiborg, Digital transformation: Towards process automation in a cloud native architecture, Acta IMEKO, vol. 12, no. 1, article 17, March 2023, identifier: IMEKO-ACTA-12 (2023)-01-17

Section Editor: Daniel Hutzschenreuter, PTB, Germany

Received November 18, 2022; **In final form** March 19, 2023; **Published** March 2023

Corresponding author: Alexander Oppermann, **e-mail:** alexander.oppermann@ptb.de

1. INTRODUCTION

Digital transformation in public administration is taking place at a different pace and often falls short of the expectations and requirements associated, for example, with the Online Access Act (OZG) in Germany. While the current pandemic situation has accelerated digital transformation measures for mobile work in general and in public administration, it has also highlighted the existing weaknesses. There is an obvious need to support the design and use of digitally supported work methods and appropriately designed process flows. To this end, existing obstacles must be systematically identified and, ideally, eliminated or dissolved by digital technologies and methods. Among other things, these relate to the legal security of digitally transformed processes, billing procedures and models, as well as associated financial and organizational structures, personnel capacities, competencies, and qualifications. In addition, there is now an opportunity to rethink and redesign process workflows to fully exploit the potential of digital transformation - simply transferring existing workflows into the digital domain is not enough.

At the same time, digital quality infrastructures must be established internally and externally, to link previous data silos and to lead to new synergy and efficiency gains (BMWi - Qualitätsinfrastruktur Digital [1]). In addition, suitable concepts are required for designing the transition from analogue to digital processes. Currently, E-Services[1] and E-File[2] are being introduced at PTB, but there is a major obstacle in connecting and digitally transforming the working groups, laboratories, and their workflows. Often, the hurdles for the individual work groups are very high and the upcoming change management processes are overwhelming.

This gap is to be closed by the Operation Layer (OP-Layer), which uses uniform interfaces to connect to the already existing infrastructures at PTB and enables simple data transfer from E-Services and E-File. Through uniform interfaces using REST (Representational State Transfer), the connected internal systems can maintain their previous workflow, while at the same time harmonizing the data. The automatic data transfer drastically increases the confidentiality, integrity and availability of the data and greatly reduces the susceptibility to errors.

The OP-Layer thus makes an enormous contribution to the automation of workflows and can reduce the workload of employees. Automation frees up staff time for research, laborious calibrations, and related tasks.

[1] Web portal for digital services

[2] Document management system for electronic records

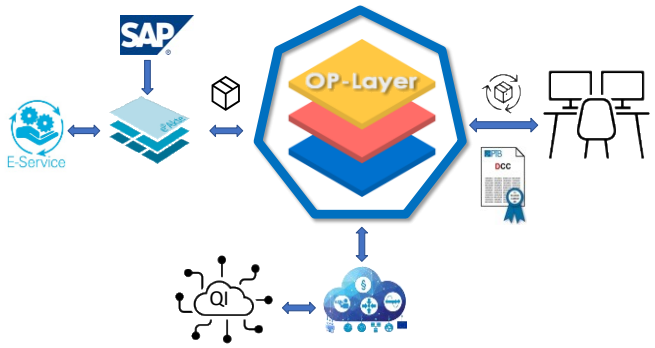

Figure 1. Overview of the workflow with the OP-Layer at heart. The OP-Layer prepares a scalable cloud native infrastructure for special tailored applications.

The rest of the paper is structured as follows, section 2 describes the concept and infrastructure of the OP-Layer. Section 3 outlines the use cases, their implications, as well as interoperability scenarios resulting from them. A summary and outlook are given in section 4.

2. CONCEPT & INFRASTRUCTURE

In the last years, a distributed microservice architecture has been built and designed explicitly in the domain of legal metrology with a focus on interconnecting external stakeholders [2], [3], [4], [5]. While the generic IT architectural design approach has proven to be successful, a similar approach will be pursued to digitally transform the internal process flow.

This time, the focus of the IT architecture will be extended to be cross-domain and linking internal stakeholders. Further targets are the stakeholders' isolated workflows as well as internal and external IT infrastructure. The foundation of the IT infrastructure will be more sophisticated in terms of scalability, availability, portability, and security (see section 2.1). Furthermore, the Infrastructure as Code (IaC) paradigm will be put at the heart of the OP-Layer.

Figure 1 gives an overview of the digitally transformed workflow [6] with the E-Service web portal as a contact point for a range of services. Once the order has been placed, an electronic file will be created in the E-file service. The E-File service stores all information centrally. The necessary administrative data is maintained independently by the customer while the required metrological data is stored as machine-readable document [7].

This is where the OP-Layer comes into place and links seamlessly the laboratories' workflows and internal departments' use-cases (see section 3) with the E-File service via an API. Moreover, the OP-Layer will feature a microservice architecture and host specific tailored applications and services that will harmonize the service infrastructure within PTB. While centralizing the service infrastructure, the individual and adapted workflows of each department will be protected. This will reduce the maintenance costs for IT-services and increases efficiency of digitally supported services.

In the preparation phase of the OP-Layer project it became obvious that companies and research institutes face the same challenges while digitally transforming their processes and infrastructures. The following list describes common challenges of organizational transformation that have to be comprised, addressed and reflected in the architectural concept of the OP-Layer:

- isolated (research / IT) infrastructures within organization
- no centralized or harmonized workflow
- no streamlined process chain across departments
- interfaces are programmed several times within one organization
- no IT management on executive level
- IT management without qualified technical experience
- no IT security awareness and organizational structure
- area of conflict between centralization and decentralization within organization
- isolated responsibilities and knowledge in each organizational unit
- lack of transparency of process flows and chains

2.1. Distributed Cloud Native Infrastructure

A distributed IT architecture (see Figure 2) that is able to support a microservice approach has to map the requirements such as high availability, (auto-) scaling, portability and security. The Kubernetes[4] design principles fulfil most of the mentioned requirements for a modern distributed infrastructure approach. The following paragraphs give a short overview of the requirements:

Scalability - Avoiding technical bottlenecks in a distributed infrastructure is vital because those can lead quickly to points of failure. Being able to scale applications horizontally, that means starting the same application several times, will redistribute the

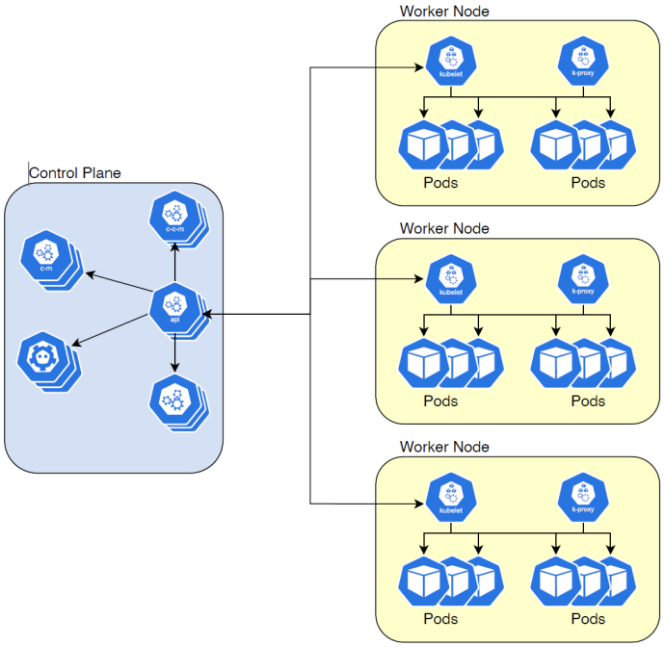

Figure 2. Overview of a generic Kubernetes architecture with a control plane on the left side, which consists of API-Module, Cloud-Controller-Module, Contoller-Manager and the Scheduler. The control plane provides the global operations for the Kubernetes architecture, like scheduling, scaling and steering pods. On the right side are three worker nodes that consists of a Kubelet[3] and a Proxy module. These provide functionality and network capabilities to the pods that hold the containerized application. A worker node can handle several pods a time. A pod can host several containers.

[3] https://kubernetes.io/docs/reference/command-line-tools-reference/kubelet/

[4] https://kubernetes.io/

request load on several "shoulders" to cope with peak in demand. Kubernetes provides load balancing and horizontal scaling capabilities out of the box.

High Availability - Backups and replicas address the high availability requirement. While backups focus on data restoration on a specific time point, replicas support business continuity. Often replicas ensure access to critical data and application infrastructure from a secondary location. Kubernetes addresses high availability both at application and infrastructure level.

Portability - Software development and deployment changed drastically. With container and pods, applications can run on any platform and cluster. Kubernetes provides many container runtimes that enable application portability and easy deployment for an agile development approach. This concept facilitates workloads across private and public cloud environments and supports availability fault tolerance zones within the infrastructure design.

Security - Security has to be addressed on multiple layer such as cluster, application and network. API endpoints are secured via TLS (Transport Layer Security). Furthermore, strict role and rights management (see section 2.2.2) has to be enforced for each user, so that only authorized operations can be executed on the cluster. Finally, network communication flows for pods have to be defined, so that only wanted communication behaviour is feasible. In a highly distributed architecture, a session-less authorization and authentication approach using tokens, which are placed in each HTTP REST request, has proven itself to be state of the art. This way, each operation can be traced back to the user (see section 2.2.2) initiating any defined process in the use cases.

2.2. Distributed Software Architecture

The envisioned distributed microservice software architecture borrows heavily from the concepts designed and developed in [2], [3], [4], [5] and adds the following requirements:

- No-configuration debugging: The same image runs in test and production.
- Containerization: All the code runs in a container plus shared resources.
- Blue/green deployment: Sending traffic only after the server exists. That means no downtime and simplified rollbacks.
- Application composition: Individual pieces of functionality can be composed in separate images, while being technology agnostic.
- Load balancing: Scaling stateless containers is a stark requirement for architecture performance.
- Service registry and discovery: Microservices have to automatically register in a registry service to enable auto-discovery of dependent microservices.

Once-Only principle: Harmonizing processes and software development by parameterizable services that fit all internal stakeholders.

2.2.1. Functional and Security Requirements

The OP-Layer can provide a variety of exchange formats such as JSON, XML and CSV. For the internal communication JSON is used to exchange data from one service to another. The interfaces will be implemented as harmonized REST interfaces. The data will be signed, validated, and archived. While the data is at rest or at transport, it will be encrypted and secured against unauthorized access. The OP-Layer supports an Open ID Connect access management solution with single sign on capabilities. A session-less and tokenized access management solution is intended, to increase security and avoid session handling in a highly distributed environment. Further the CIA triad attributes (confidentiality, integrity, and availability) are deeply incorporated in the basic infrastructure design.

2.2.2. Identity and Access Management

The following requirements for an Identity Access Management (IAM) solution are described in [8] and are adapted to meet the criteria for the proposed distributed microservice software architecture:

- Separation of concerns: Users and roles must be isolated within the platform but differentiated and centrally managed across the entire process.
- Single Sign-On: A user should log on only once and should have access to the functions assigned to him by means of roles in the frontend and in the backend services.
- Identity Federation: It should be possible to authorize additional identity servers of third-party organizations (federated ID), so that their users can log on directly to the proposed platform with their organizational ID and use its services.
- Audibility and Traceability: Due to the highly decoupled and decentralized approach of the architecture, user-based sessions are not used. A token-based approach is implemented to login. The token will contain further information about the user, such as roles and the validity period of the token, in encrypted form. This means that every request to a backend service and every processing step in the respective processes can be traced back to the initiating user.
- Harmonized Login Procedure: In addition to users, measuring devices and external services should also be authenticated and authorized by the IAM system on the platform in the future.
- Harmonized Authentication Protocols: By using a standard-compliant OpenID Connect IAM solution which also supports SAML2, developers can focus on the business requirements and their implementation, as there is no longer any need to develop IAM mechanisms. This also simplifies the maintainability of the platform and makes it comparatively easy to exchange the IAM solution used.

3. USE CASES

Each use case is implemented as a separate containerized back-end service. They all provide REST API endpoints for communication, such as triggering actions, or providing information. The following subsections describe the three use-cases of the proposed OP-Layer platform.

3.1. E-File Connector

The E-File Connector service will have no graphical user interface. Instead, this service bridges the gap between the automated data access from the laboratory workflow, in order to import data. As a first step, only administrative data will be converted and exported. Later this restriction will be lifted, and all necessary data will be available to support the automation of workflows.

The use-case consists of five steps. Finding the electronic file and filtering the administrative data. Then the export in a

preselected exchange format, such as JSON, XML or CSV, is triggered. The laboratory can start their workflow and create for example a digital calibration certificate with the exported data. This XML certificate can now be uploaded and will be validated. If the validation is successful, it will be put into the electronic file in the E-File-Service.

3.2. Digital Calibration Certificate Process

Reference implementations of services with a high impact factor are provided, to facilitate the adoption of the OP-Layer within PTB. As a prominent example serves the Digital Calibration Certificate (DCC [9]) process. It has been entirely digitally transformed and implemented [6] as a service within the OP-Layer.

The digital calibration process starts with the E-Service Portal. A customer portal, which offers a calibration certificate application. After applying for a calibration certificate for a measuring instrument, the process continues with an automatically created file in the E-File System. All data is automatically transferred and archived in a file. The responsible department checks the validity of the application. At this point in the process, the OP-Layer offers a convenient way to automatically transfer all necessary data to the calibration laboratory via unified REST interfaces. Moreover, the aforementioned service is built to automatically import administrative data from the E-File System, in order to create a proper DCC. The resulting DCC can be automatically uploaded via the OP-Layer into an existing file within the E-File System. From there, the file handler submits the DCC to the E-Service Portal.

The entire use case is depicted in Figure 3. In step 1, the customer applies for a Digital Calibration Certificate for a supported measuring instrument within the E-Service portal. A notification is sent to the responsible organizational unit.

In step 2, the responsible case worker creates a new procedure within E-File and transfers the administrative data from the application into the new file.

The OP-Layer pulls incoming E-Service procedures from E-File at the beginning of step 3. The lab technician sees the new application within the OP-Layer web frontend, and initiates DCC creation. The OP-Layer transfers the administrative data from E-File automatically into the DCC service. The lab technician can provide the measurement results via web frontend.

Figure 3 is a simplification of the digitally transformed process. Hence, E-File is actually two instances. The E-File system itself, and an OP-Layer specific E-File connector, which serves as communication interface for the other OP-Layer components.

When all required data is provided in the DCC input form (see Figure 4) in the OP-Layer, the lab technician can review the data and submit it to the DCC service to create a valid DCC as XML. The XML file is attached as a record to the calibration document in the procedure within E-File.

The case worker provides the DCC XML record to the E-Service application, to make it available to the customer in step 4. The customer can view and download the given DCC XML file from the E-Service portal in step 5.

3.3. Digital Calibration Certificate Service

The digital calibration certificate service (DCC Service) is a centralized service that harmonizes the creation of a DCC-XML-certificate. Depending on the laboratory, the object of the calibration and its measurement might differ. However, the

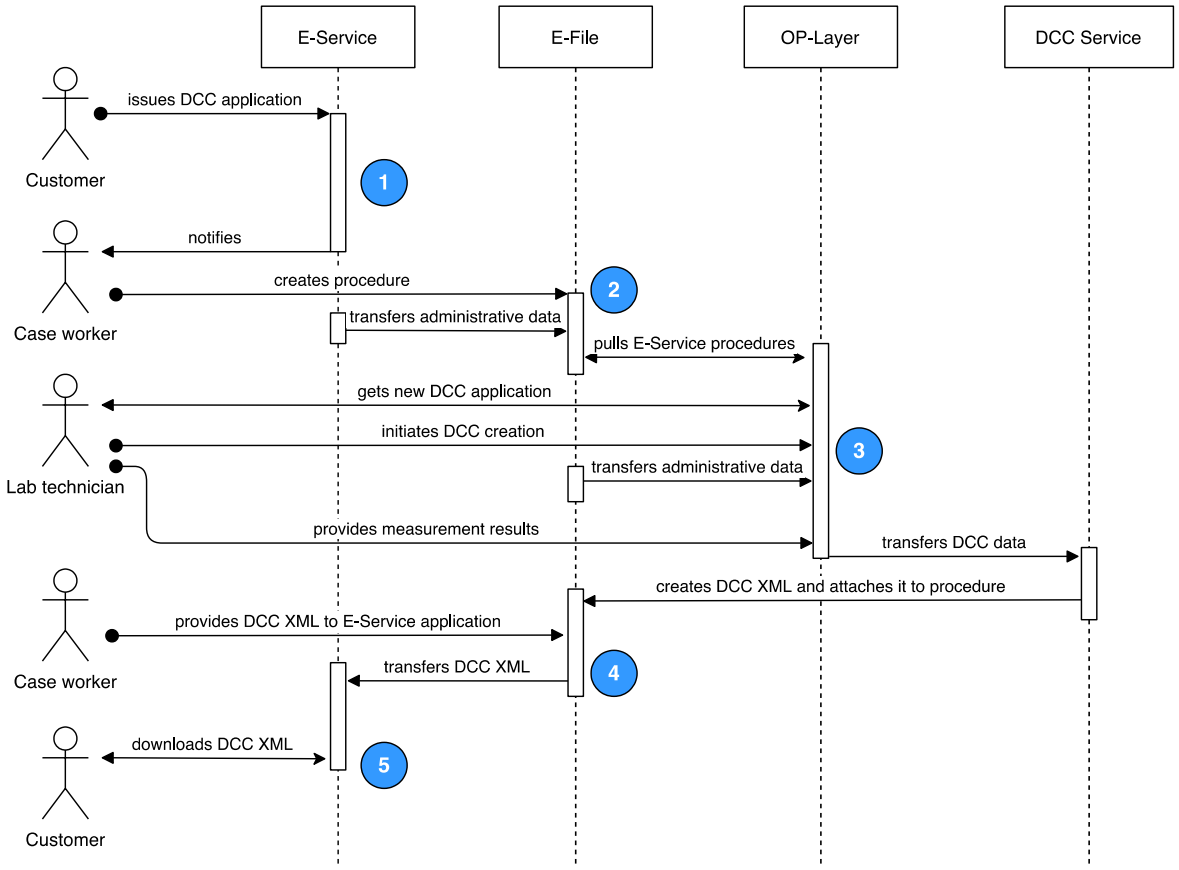

Figure 3. Sequence diagram of the digital calibration certificate process. The numbers resemble the necessary steps until the customer receives the DCC.

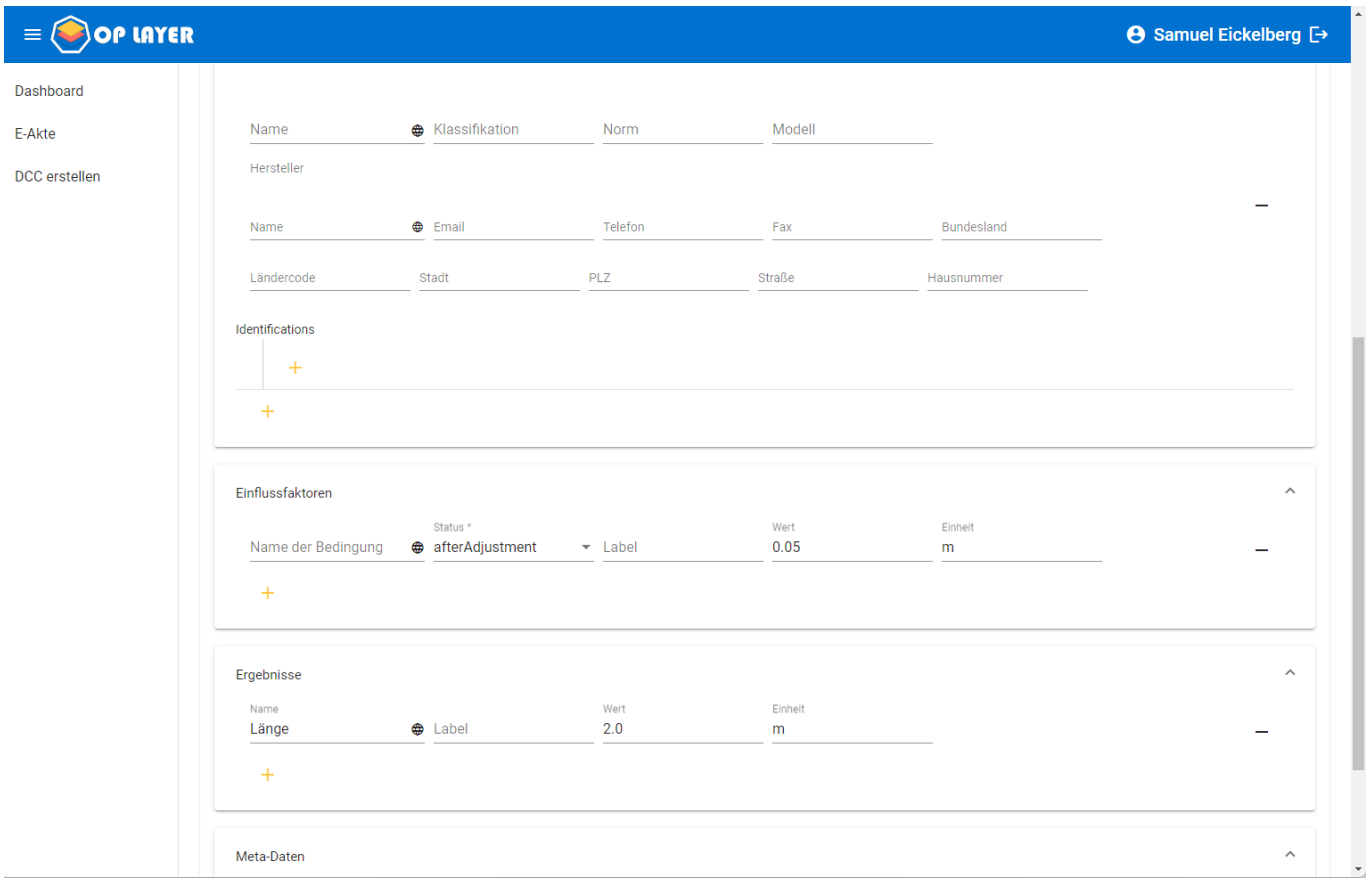

Figure 4. Screenshot of the DCC service form for manually entering measurement result.

frame and shaft of the document are the same, so that a parametrized service provides the requirements of each laboratory. This service harmonizes and unifies the DCC creation and simplifies the workflow for laboratories tremendously.

A first simplified use-case will consist of three steps. First selecting the object of calibration. Then importing the administrative data will take place. Depending on the selected object of calibration, the specific measurement and device management part will be imported from the laboratory workflow. Lastly, the creation of the digital calibration certificate will be executed, and an XML file will be made available for further processing.

Generated XML DCCs can then, depending on the requiring calibration laboratory, be automatically transferred into the given procedure within the E-File system via the E-File connector (see section 3.1). On the other hand, customer data from the E-Service request, which is managed by E-File, can be conveniently imported into a DCC structure, also via the E-File connector. This way, the need for providing data manually for a DCC is further reduced.

3.4. DoC Service

The digital declaration of conformity service (DoC Service) works similar to the DCC service. However, the resulting XML is not a calibration certificate but a declaration of conformity that consists of different norms and directives that the measurement instrument has to fulfil. The use-case consists of three steps, such as the selection if the measuring instrument, the import of administrative data for the declaration and the instrument specific norm and directive part that has to be included in the declaration document. Finally, the creation of the declaration of conformity takes place and the resulting XML file can be downloaded. The DoC service and the DCC service can be operated simultaneously, yet independently, as both accommodate similar, yet different use cases.

4. CONCLUSIONS

In this paper, the concept of the Operation Layer has been presented and demonstrated exemplary with the DCC workflow, which links already existing infrastructures at PTB via uniform interfaces to enable data transfers from previous isolated data silos. Through uniform interfaces (REST interface), the connected internal systems can maintain their previous workflow, while harmonizing data at the same time. The automatic data transfer drastically increases the productivity, integrity and availability of data and greatly reduces the susceptibility to errors. The OP-Layer makes an enormous contribution to the automation of workflows and can reduce the workload of employees. In times of decreasing numbers of skilled workers, an increasing automation can lead to more efficiency, more time for research, laboratory activities and related tasks.

Special tailored application can be hosted via the OP-Layer internal service hub structure. Preferably, working groups design their application with a generic entitlement to serve a larger audience. The strict design framework reduces the administrative

overhead for the research staff to claim more time for original research. In addition, the strict framework increases security and quality for special tailored applications. The OP-Layer development is based on three main pillars:

1. **Container Environment:** A self-hosted sophisticated container environment with prepared CI/CD pipelines, secured networking and resource-management – Kubernetes is the current state-of-the-art solution.
2. **Identity and Access Management:** A central solution for handling authentication (with organization-wide PTB ID) and access control for services in the OP-Layer – the de-facto standard solution Keycloak[5] is employed.
3. **Service Guidelines:** Providing and enforcing principles of modern software design for distributed services. Furthermore, it is encouraged to publish the code as Open Source. A service should be as lightweight as possible, provide REST interfaces and come with basic documentation.

A huge potential for automation and optimization is shown by the initially built Digital Calibration Certificate Process. Especially for future use cases, similar efficiency gains and simplifications for digital transformed processes can be anticipated.

However, digitally transforming processes also pose challenges of harmonising work procedures and finding standards as well as minimal shared requirements within a federal organized body such as PTB.

On-boarding working groups to the OP-Layer service hub infrastructure will be the next phase. Provided these early adopters have sufficient IT skills to migrate their special tailored applications to the OP-Layer, the phase will be completed. This is a great opportunity to enhance the service guidelines and to connect PTB's development community. Contributing tremendously to IT security by harmonizing development and deployment procedures, will serve the whole organization.

REFERENCES

[1] F. Thiel, J. Nordholz, Quality Infrastructure 'Digital' (QI-Digital). Federal Ministry for Economic Affairs and Energy, 2020. Online [Accessed 28 March 2023] https://www.bmwk.de/Redaktion/EN/Artikel/Digital-World/GAIA-X-Use-Cases/quality-infrastructure-digital-qi-digital.html

[2] A. Oppermann, S. Eickelberg, J. Exner, Digital transformation in legal metrology: An approach to a distributed architecture for consolidating metrological services and data. In Information Technology for Management: Towards Business Excellence: 15th Conf. ISM 2020, and FedCSIS-IST 2020 Track, Held as Part of FedCSIS, Sofia, Bulgaria, 6–9 September 2020, Extended and Revised Selected Papers 15, Springer International Publishing, 2021, pages 146–164. DOI: 10.1007/978-3-030-71846-6_8

[3] A. Oppermann, S. Eickelberg, J. Exner, Toward digital transformation of processes in legal metrology for weighing instruments, Proc. of the 2020 Federated Conference on Computer Science and Information Systems, M. Ganzha, L. Maciaszek, M. Paprzycki (eds). ACSIS, Vol. 21, pp. 559–562. DOI: 10.15439/2020F77

[4] A. Oppermann, F. Grasso Toro, F. Thiel, J.-P. Seifert, Secure Cloud Computing: Reference Architecture for Measuring Instrument under Legal Control, Security and Privacy, 1(3), 2018: e18. DOI: 10.1002/spy2.18

[5] S. Eickelberg, Th. Bock, M. Bernien, A. Oppermann. Integrating a Calibration Laboratory Workflow into a Metrological Digital Ecosystem: A Case Study. Proc. of the IMEKO TC6 Int. Conf. on Metrology and Digital Transformation, Berlin, Germany, 19 - 21 September 2022, 4 pp. DOI: 10.21014/tc6-2022.016

[6] A. Keidel, S. Eichstädt, Interoperable processes and infrastructure for the digital transformation of the quality infrastructure, 2021 IEEE Int. Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0&IoT), Rome, Italy, 7 - 9 June 2021, pp. 347–351. DOI: 10.1109/MetroInd4.0IoT51437.2021.9488563

[7] S. Eichstädt, A. Keidel, J. Tesch. Metrology for the digital age. Measurement: Sensors, 18, 2021, 100232. DOI: 10.1016/j.measen.2021.100232

[8] A. Oppermann, S. Eickelberg, Digitale Transformation in der Metrologie: Harmonisierung digitaler Identitäten mittels OpenID. Werkwandel, Zeitschrift für angewandte Arbeitswissenschaft, Ausgabe #1, February 2022, pp. 26–30. Online [Accessed 28 March 2023] [In German] https://magazin.werkwandel.de/

[9] S. Hackel, F. Härtig, J. Hornig, Th. Wiedenhöfer, The Digital Calibration Certificate, PTB-Mitteilungen 127 (2017), No. 4, pp. 75-81. DOI: 10.7795/310.20170403

[5] https://www.keycloak.org