Toward Digital Transformation of Processes in Legal Metrology for Weighing Instruments

Alexander Oppermann, Samuel Eickelberg, John Exner
Physikalisch-Technische Bundesanstalt (PTB)
Abbestr. 2-12
10587 Berlin, Germany
Email: {alexander.oppermann, samuel.eickelberg, john.exner}@ptb.de

Abstract—The digital transformation of sovereign processes is a driving force to streamline and innovate processes for measuring instruments under legal control. Providing trust is the essential purpose of Legal Metrology and still a challenging task in the digital domain. Taking the strict legal framework into account, a distributed software architecture is presented that offers privacy, security and resilience. At the same time, the platform approach seamlessly integrates existing public and private infrastructures. Furthermore, a service hub is created with interdependent services that support the digital transformation of paper-based processes, such as verification and software update. Exemplary, these two central use cases are introduced, and its requirements and implementation approach are described. The main goal is to provide the same level of trust and security, by developing new digital concepts, infrastructure and remote processes for a unified digital single market.

I. Introduction

THIS paper focuses on the progress of innovating sovereign tasks within Legal Metrology by the digital transformation of paper-based procedures. The field of Legal Metrology comprises around 160 million measuring instruments in Germany, which contribute about 157 billion Euros to the national GDP [1]. The main purpose of Legal Metrology is to establish and provide trust among all stakeholders such as customers, manufacturers, and users of measuring instruments. By law a Notified Body, e.g. the PTB in Germany, is obligated to carry out a conformity assessment of measuring instruments. The essential requirements of the Measuring Instrument Directive (MID) [2], such as reproducibility, repeatability, durability and protection against corruption of measuring instruments and measurements, have to be fulfilled before entering the market.

AnGeWaNt[1] is a joint research project to address the automation of measuring instruments and their challenges for society. The six associates are ranging from different areas like commercial partners in the weighing and construction industry to Notified Body in Germany, such as the Physikalisch-Technische Bundesanstalt (PTB), a local innovation hub (Zenit

[1]https://www.angewant.de/

GmbH) [3] and the Institute for applied labor science (Ifaa) responsible for aspects within social-economic and human factors [4].

In this paper, the digital transformation of two main procedures, such as verification application as well as the software update, are described and their progress in the digital transformation are outlined. Section II puts the related work into perspective with the AnGeWaNt project. In Section III, an overview of the requirements and the novel approach of the use cases is given. Section IV presents the approach to map the processes, their requirements, design decisions and shared infrastructures.

II. Related Work

A. European Metrology Cloud

The AnGeWaNt project can be considered as a national spinoff of the *European Metrology Cloud Project* (EMC) focusing only on weighing instruments.

The EMC project circumcises 16 different measuring instrument classes in a supranational setting within a European legislation context. One of the major goals is to support the unified digital single market that the European Commission has issued. While the EMC project aims to distribute hardware nodes [5] that will provide essential parts of the envisioned infrastructure, the AnGeWaNt project can be hosted, split up and distributed on any Platform as a Service provider (PaaS). The European Metrology Cloud concept is also in line with the General Data Protection Regulation (GDPR) [6].

B. GAIA-X

The GAIA-X project started as a joint initiative of Germany and France in 2019 with the goal to build a sovereign digital European Cloud-Ecosystem that is efficient, secure and highly distributed. Major key features are data sovereignty, privacy by complying with the GDPR, transparency and openness by supporting open-source principles and being flexible by building a modular and highly inter-operable platform for a broad spectrum of industry partners. These include Small and Medium Enterprises (SME) as well as government bodies [7].

III. Requirements and Use Cases

Due to the harmonization efforts in the EU, the respective national regulations in Europe are derived from the MID. It

defines regulations until the measuring instrument is placed on the market. Regulations for processes after the measuring instrument has been placed on the market, such as re-verification, are not regulated by the MID. In Germany, the Measurement and Verification Act (MessEG) [8] and the Measurement and Verification Ordinance (MessEV) [9] are applied.

The following recommendations are taken into account: the International Organization of Legal Metrology (*OIML*) [10], the *MID*, software recommendations of European Cooperation in Legal Metrology (*WELMEC Guide 7.2*) [11], recommendations of *WELMEC Guide 7.3* Reference Architectures [12], and technical guidelines of the Federal Office for Information Security (*BSI TR 03109*) [13].

Additional requirements are sufficient flexibility, the protection of personal data, planning of verification appointment, and transparency of the processes (status information for processing). Furthermore, there should be standalone services for user management, a revision-safe archive store, verification application submission, scheduling of verification appointments, and a revision-safe logbook.

A. Digital Administration Shell

Cornerstone of the digital transformation will be the *Digital Administration Shell*. This concept will be developed gradually. It evolves from a *device pass*, that stockpiles instrument specific data and thus creates a unique mapping to a measuring instrument. Based on this, the *digital type plate* will be created, that holds verification-specific information, e.g. the number of the EC type-examination certificate and the accuracy class of a scale. It will result in a general *document store* that hosts all documents related to a specific measuring instrument. A unique filter mechanism will be implemented to present information depending on the specific perspective of users, roles and access rights. For the first time, this administration shell will gather all relevant data over the life span of a measuring instrument and in addition to it fulfill the legal archiving obligations.

B. Digital Verification Application

After the verification period has expired, measuring instruments under legal control must be re-verified. Without valid verification, measuring instruments may no longer be used. This helps to maintain trust in officially verified measuring instruments. The flow-chart of the German verification process is made available [14].

A key requirement is the digital transformation of the paper-based verification application process. The prototype platform aims to provide a convenient, web-based user interface. Furthermore, it facilitates and streamlines the entire process across all 16 German federal states. The target platform DEMOL requires the verification applications in a specified XML-based data structure. AnGeWaNt collects the application data and checks for plausibility before submission.

C. Software Update Application

Measuring instruments under legal control consist of legally relevant and non-relevant software. The legally relevant part comprises the metrological characteristics of the measuring instruments [9]. Only updates of the legally relevant software part are regulated. According to §37 MessEG, a software update requires the approval of the responsible verification authority.

The verification authority must be informed about which devices should be updated. Instead of applying for a software update for each device individually, a bulk application is feasible. The flow-charts of the complex process are made available for the standard appeal [15] and for the emergency appeal [16].

D. Remote Authenticity

In the field, user and market surveillance verifies measuring instruments. With increasing usage of software in measuring instruments, a further decoupling of hardware and software is inevitable. As a result only small parts of the measuring instrument, such as the sensor and a communication unit, will remain in the field. Software will be outsourced into data centers (see [17]). Thus, it is in the utmost interest of the authorities to verify legal relevant software parts remotely. Despite its location and physical access. Oppermann et al. [18] already addressed this problem and created a virtual verification monitor that fulfills the need of user and market surveillance. The authorities must have the possibility to remotely verify the authenticity of used meter, processing unit, and associated logbook. The legal relevant software has to provide a form of identification. An acceptable solution according to the WELMEC Guide [11] would be: a *software name* consisting of a string of numbers, letters, or other characters; a string added by a *version number*; and a *checksum* over the code base.
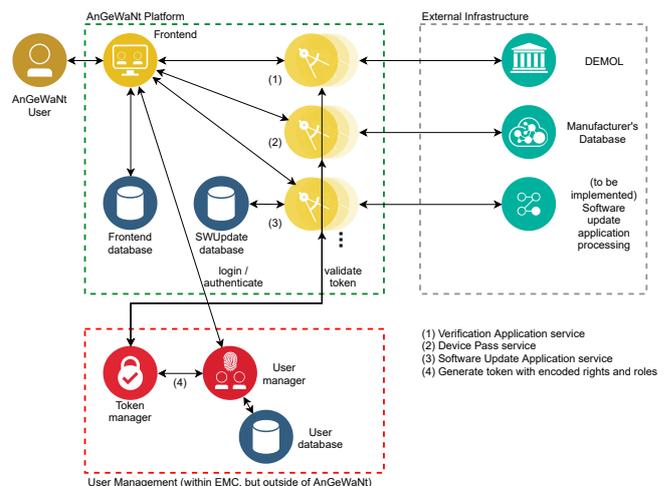

Fig. 1. Overview of the platform architecture concept

IV. ARCHITECTURE OF THE PLATFORM

The envisioned platform is a central hub, that will offer access to all connected infrastructures and their provided services. All stakeholders can take advantage of the offered services and data within the platform domain. Consequently, this service hub is a first step to a interdependent service ecosystem. It will provide opportunities to develop new data-driven business cases beyond the classical domain of manufacturers and increases the innovation for future success.

Furthermore, by its modular approach, the architecture allows new services to be added with minimal effort. To increase flexibility and ease later expandability, the project strives for standardized and harmonized REST interfaces across all services. The distributed architecture offers independent deployment as well as operation of services. However, a web-based user front-end must be able to find and communicate with all provided services within the platform ecosystem.

The setup of the platform (see Fig. 1) consists of three independent modules. The main module is the AnGeWaNt Platform (see upper-left dashed box). It offers a web-based user interface and services, such as verification application and software update. The user management module (lower-left dashed box) consists of the user and token manager services. That offers a secure, stateless and flexible authentification and authorization layer. The External infrastructure module (right dashed box) ties third-party systems to AnGeWaNt platform, such as DEMOL or manufacturers' systems, to provide verification applications or device passes.

A. Common Principal Data Service

All stakeholders, devices, and device types are using the same core data across different types of processes and documents. Thus, a service which handles all common principal data is implemented, and accessible through the front-end to fill in e.g. a software update application or a verification request.

From the data model perspective, essential requirements are the mapping of the processes between stakeholders, and a document-centered view of the processes in legal metrology. A step in a process often creates a document, such as a validation application, or a software update application. At the same time, these documents must be saved in an audit-proof manner. For this reason, documents and stakeholders are being loosely coupled in the current state of development. A lot of information can be held in an abstract class `Party` rather than to specific types, such as user or manufacturer.

B. Software Update Application Service

The implemented service has specified endpoints for submission of an application, updating status, receiving a hearing, as well as placing a response to a hearing. These are the only steps in the request processing that require interaction via the AnGeWaNt platform. The software update request is processed according to the following steps (see Fig. 2):

C. Role and User Management

The project aims to separate user credentials as well as rights and roles management from the AnGeWaNt platform. First, the User manager and Token manager services can be re-used in other projects and services across the EMC. Secondly, all user-related data is not coupled to a specific application, increasing the security of the platform. Another design paradigm is to avoid sessions, because they cannot be held in a highly distributed architecture across potentially different domains. Instead, tokens are being generated and assigned to either a user that logs in successfully, or a service to prove its authenticity.

1) The user manager: handles entities which contain the user name, the password as encrypted byte sequence, granted rights, assigned roles, as well as flags whether or not the user account is enabled, locked, or its credentials are disabled. All communication with the User manager takes place via REST. The user authentication process deals with *authenticity* and *authorization*. By communicating with stateless tokens, a session which contains currently logged-in user information is not required.

2) The token manager: provides JSON Web Tokens (JWT) containing the authorization, which in turn depends on rights and roles from user manager, for a user to access specific services. The service evaluates the request header of a token to determine a valid authorized request. Like the User manager, all communication with the Token manager takes place via REST. This service only provides authenticity.

D. Security Aspects

Risk assessment of distributed metrological software has already been addressed by Oppermann et al . [19] and Esche et al. [20]. As the prototype platform is concerned with legally relevant processes regarding measuring instruments, the following attack vectors (according to [11]) must be taken into account when choosing a publicly available, widespread application framework, such as Spring Boot: *A_WEB_XSS* (Cross-site scripting attack), *A_WEB_DOS* (Denial-of-Service attack), and *A_WEB_SOCKET* (introducing malicious code via web socket). Spring Boot addresses the aforementioned security
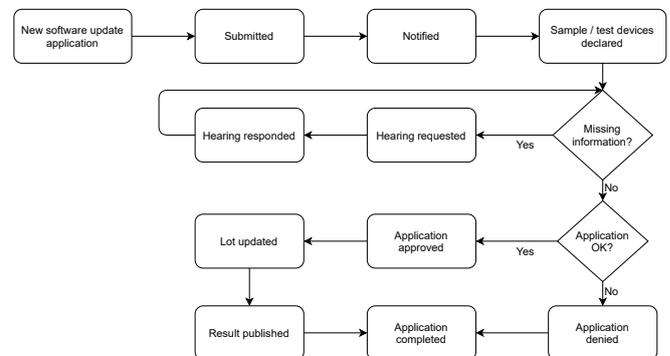

Fig. 2. Processing flowchart of the software update request process from the AnGeWaNt perspective

concerns, given that the appropriate implementations and application server configurations are being carried out.

V. Conclusion And Future Work

In this short paper the AnGeWaNt project introduced its approach to seamlessly integrate existing public and private infrastructure. The legal framework with its security requirements are briefly described and also its implication for the platform design. Legally regulated processes, such as verification application and software update, are central use cases. Their digital transformation is the driving force to innovate and streamline the underlying infrastructure.

By creating a central platform with a service hub, the digital transformation of paper-based procedures is supported. The platform is modular and built to integrate independent services. This provides new opportunities beyond the classical realm of all stakeholders and increases data-driven innovation for future success. Moreover, other research projects can easily profit from the implementation progress, e.g. the user management can be integrated into the EMC project. Furthermore, each service can be easily separated and integrated into another context. This will assure that a lot of progress made in this project can be reused and avoid time intensive and costly reimplementation. The highly modularized nature of this platform allows a greater flexibility, adaptability and eases the burden of distributing the services across different domains. This increases indirectly the resilience of the platform, because several instances of a service can be run at the same time in different domains. At last, this platform paves the way for a unified digital single market.

Furthermore, the AnGeWaNt platform is designed from the beginning with *Multi-tenancy* concept in mind. The need for different stakeholders, such as manufacturers, market and user surveillance authorities, and notified bodies to access only its own relevant data is crucial. This is guaranteed by the *User Manager*. With the introduction of *Token Manager*, a single sign on solution is created that can be used to verify a user and grant access for documents across infrastructures. This is especially helpful, e.g. to send verification applications to external systems like DEMOL or to import device passes from manufacturers.

In the next iteration, *Multi-factor Authentication* will be introduced, to increase security and enhance trust in the platform. The user manager will be extended to use a second factor for authentication. This can be a mobile device running an authenticator app, or a physical device, e.g. a fingerprint scanner attached to a client computer. Furthermore, the support and integration of OpenID connect frameworkis intended.

In the long run, the *Digital Administration Shell* will be extended to import an XML-based Certificate of Conformity (CoC) in the near future. This will offer new services, e.g. remote verification, issuing and revoking certificates. The PTB is working to establish the same level of trust for digital certificates as conventional paper-based certificates guarantee nowadays.

References

[1] N. Leffler and F. Thiel, "Im Geschäftsverkehr das richtige Maß - Das neue Mess und Eichgesetz, Schlaglichter der Wirtschaftspolitik," 2013.

[2] European Parliament and Council, "Directive 2014/32/EU of the European Parliament and of the Council," *Official Journal of the European Union*, 2014.

[3] M. Guth, H. Hoffzimmer, and N. Ottersböck, "Entwicklung hybrider Geschäftsmodelle vor dem Hintergrund der Digitalisierung," *Betriebspraxis & Arbeitsforschung*, 2020.

[4] N. Ottersböck, M. Frost, T. Jeske, and V. Hartmann, "Systematischer Kompetenzaufbau als Erfolgsfaktor zur Etablierung hybrider Geschäftsmodelle," *GfA (Hrsg) Digitale Arbeit, digitaler Wandel, digitaler Mensch? Bericht zum 66. Kongress der Gesellschaft für Arbeitswissenschaft vom 16. – 18. März 2020*, 2020.

[5] M. Dohlus, M. Nischwitz, A. Yurchenko, R. Meyer, J. Wetzlich, and F. Thiel, "Designing the European Metrology Cloud," *OIML Bulletin*, vol. 61, no. 1, pp. 08–17, 2020.

[6] F. Thiel and J. Wetzlich, "The European Metrology Cloud: Impact of European Regulations on Data Protection and the Free Flow of Non-Personal Data," in *International Congress of Metrology*, Array, Ed., 2019. doi: 10.1051/metrology/201901001 p. 01001.

[7] Federal Ministry for Economic Affairs and Energy (BMWi), "Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem - Executive Summary," *Official Journal of Federal Ministry for Economic Affairs and Energy*, Oct. 2019.

[8] "Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (Mess- und Eichgesetz - MessEG)," Nov. 2019. [Online]. Available: https://www.gesetze-im-internet.de/messeg/

[9] "Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung (Mess- und Eichverordnung - MessEV)," Apr. 2020. [Online]. Available: https://www.gesetze-im-internet.de/messev/

[10] O. de Métrologie Légale, "General requirements for software controlled measuring instruments," 2008.

[11] "WELMEC 7.2 Software Guide," *WELMEC European cooperation in legal metrology, Welmec Secretariat, Delft, Standard*, 2019.

[12] "WELMEC 7.3 Guide Reference Architectures - Based on WELMEC Guide 7.2," *WELMEC European cooperation in legal metrology, Welmec Secretariat, Delft, Standard*, 2019.

[13] BSI, "Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems," *Bundesamt für Sicherheit in der Informationstechnik, Bonn*, 2013.

[14] J. Exner and A. Oppermann, "German verification process," May 2019. [Online]. Available: https://www.angewant.de/wp-content/uploads/2020/06/Eichantrag.pdf

[15] ——, "German software update emergency appeal," May 2019. [Online]. Available: https://www.angewant.de/wp-content/uploads/2020/06/Standardverfahren_Softwareaktualisierung.pdf

[16] ——, "German software update process," May 2019. [Online]. Available: https://www.angewant.de/wp-content/uploads/2020/06/Eilverfahren_Softwareaktualisierung.pdf

[17] A. Oppermann, A. Yurchenko, M. Esche, and J.-P. Seifert, "Secure cloud computing: Multithreaded fully homomorphic encryption for legal metrology," in *International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*. Springer, 2017, pp. 35–54.

[18] A. Oppermann, F. G. Toro, F. Thiel, and J.-P. Seifert, "Secure Cloud Computing: Reference Architecture for Measuring Instrument under Legal Control," *Security and Privacy*, vol. 1, no. 3, p. e18, 2018. doi: 10.1002/spy2.18. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.18

[19] A. Oppermann, M. Esche, F. Thiel, and J.-P. Seifert, "Secure Cloud Computing: Risk Analysis for Secure Cloud Reference Architecture in Legal Metrology," *accepted in Federated Conference on Computer Science and Information Systems (FedCSIS), IEEE*, 2108.

[20] M. Esche and F. Thiel, "Software Risk Assessment for Measuring Instruments in Legal Metrology," *Proceedings of the Federated Conference on Computer Science and Information Systems*, pp. 1113–1123, 2015. doi: 10.15439/2015F127