Digital Laboratory Notifications First Rollout Results for Sars-CoV-2 and the Extension towards Generic Pathogen Reporting

Andreea Ancuta Corici, Olaf Rode, René Wiegmann Rollet and Max Bureck
Institute of Fraunhofer FOKUS, Berlin, Germany

Keywords: eHealth, SARS-CoV-2, FHIR, Authentication, LDTv2, OAuth2.0, Mutual TLS.

Abstract: In each country, there is a set of pathogens that require the laboratories to announce the results to local authorities. The current systems based on Fax technologies are overwhelmed with the numerous results that laboratories have to communicate for SARS-CoV-2. For enabling the upgrade of the infrastructure in terms of communication technology employing security, data protection and routing of notifications towards the list of corresponding entities, a digital communication system was developed during the DEMIS SARS-CoV-2 project. In this paper, we present the design and implementation, the testbed used for development and the performance test results, as well as rollout status and the lessons learned.

1 INTRODUCTION

As the number of infections with SARS-CoV-2 are in the attention of the public health authorities, it is most valuable to convey the needed information about the undergone tests and their results to the institutions in charge of counselling the patients and taking decisions. It is clear that the initial system based on Fax communication, although widespread and well known, tend to a low quality of acquired data due to sending per hand information from one system to another remote system.

At the same time, using Fax technology when handling the tremendous number of positive results while the teams handling the reports also go through a rapid increase in work force and extra work hours, can lead to a poor accounting of the positive cases. Loosing track of an infected person due to human error can lead to serious negative impacts on that person health and their contacts.

Taking into account these aspects, a digital system for allowing accounting and efficient communication of the reported cases between entitled parties was initiated together with multiple stakeholders including the **Robert Koch-Institute (RKI)** during the **DEMIS SARS-CoV-2** project (see Figure 1 and Homepage of DEMIS project). The project started in Spring 2020, as a follow-up of a research project initially carried out for enabling doctors to report the pathogens that are compulsory to notify to the local health authorities. During the currently running project, the nation-wide network of laboratories are being digitally upgraded in order to accurately send the legally required information about the positive cases of SARS-CoV-2. The next phase of the project rollout, that will start in Spring of 2021, will cover also other pathogen notification, starting with influenza.

In this paper, we present the state of the art and background technology in section 2, an overview of the requirements in section 3 and the description of the derived system implementation in section 4. Section 5 presents the performance tests for the component handling the dispatching logic and the first phase rollout insights in section 6. Section 7 closes the article with the conclusion and future work.

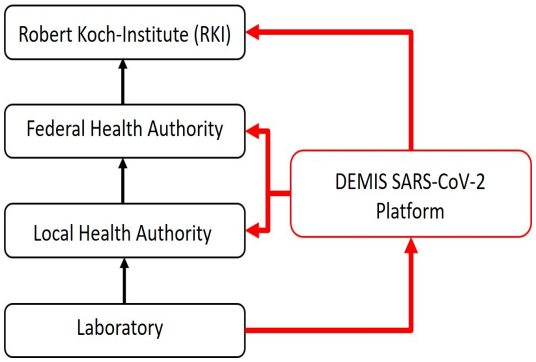

Figure 1: DEMIS SARS-CoV-2 approach compared to the old three steps procedure for centralizing the results.

Corici, A., Rode, O., Rollet, R. and Bureck, M.
Digital Laboratory Notifications First Rollout Results for Sars-CoV-2 and the Extension towards Generic Pathogen Reporting.
DOI: 10.5220/0010433800170025
In *Proceedings of the 7th International Conference on Information and Communication Technologies for Ageing Well and e-Health (ICT4AWE 2021)*, pages 17-25
ISBN: 978-989-758-506-7

2 BACKGROUND

2.1 Fast Healthcare Interoperability Resources (FHIR)

FHIR (see HL7, FHIR standard) is a standard defined by HL7 for electronic health records exchange defining data objects and the operations that can be performed upon them. Stored data objects (e.g. Observations, DiagnosticReports, Patients, Organizations) can reference each other, creating complex resource trees. The standard uses a RESTful approach for creating, updating, deleting and retrieving data objects. What is notable is the retrieval of big amounts of data, where the mechanism of Paging is recommended, in order to split the results into chunks. Another important aspect is the standardized search function, in which resource field values can be used to filter the results. The JSON, XML and RDF encoded payloads is transported using HTTP or HTTPS.

2.2 Authentication Mechanisms

A best practice for securing the traffic between the system components, such as those between the backend services and the end users (laboratories and public health institutions) of the DEMIS SARS-CoV-2 project, is to employ strong authentication mechanisms like those from the OAuth2.0 framework (see D. Hardt, 2020), JSON Web Tokens (JWT) (see M. Jones et al., 2015) and mutual TLS for generating the tokens using the certificates of the end users. The OAuth2.0 was defined in order to enable delegated access to protected resources by introducing a token access retrieval from an authorization server before requesting the access to the protected resource.

Mutual TLS was recently finalized in the IETF RFC 8705 (see B. Campbell at al., 2020) in order to define a mechanism in which both client and server hosting the protected resource can authenticate to each other, having a result a much stronger data security than authenticating only the server via TLS.

2.3 Laboratory Data Transfer (LDT)

In Germany, the standard LDT (Laboratory Data Transfer) (see QMS und KBV) was employed as early as the 1990s for encoding and sending the laboratory results. The encoding is using labels for the type of grouped elements of the notification, with each element being Tag-Length-Value encoded. The file structure consists of a header, a set of records and a closing label. The microbiology and laboratory reports are those used primarily to communicate pathogen test results. Each record can hold one or more pathogen tests. Using Jokerfields one can extend the semantics of the LDT and introduce new fields that are needed but not yet standardized.

2.4 Deployment Tools

Running an application inside a container translates into executing the application in an instance of the hosting operating system, in comparison to mechanism of running the application in a virtual machine, executing on its own operating system.

OpenShift (see Openshift platform) is a PaaS (platform as a service) for the development and deployment of applications within containers. The software is based on the container virtualization tool Docker (see Docker tool) and the orchestration tool Kubernetes (see Kubernetes tool). Some of the functionalities of Kubernetes are container grouping, auto-scaling, load-balancing or self-healing. As a result, the features of OpenShift are that of a full-fledged development platform, like automated installation and updates, a webinterface, command line tools, support of continuous integration and deployment, logging- and monitoring support.

3 SYSTEM REQUIREMENTS

The DEMIS SARS-CoV-2 system has to respond to a wide range of functional as well as non-functional requirements. These are:

- **Notification Validation:** All notification about positive SARS-CoV-2 test results that are send by laboratories must conform to the HL7 FHIR based information model defined by RKI. The system must reject non-conformant notifications.
- **Notification Enrichment:** The system must add contextual information to inbound notifications. This includes, e.g. a timestamp, the verifiable identifier of the sender as well as information regarding the receiver of the notification.
- **Automatic Receiver Calculation:** The receiver of the notification (a specific public health office) must be computed by the system using information that is included in the notification. Relevant information include, e.g. the address of the infected person as well as the address of the sender of the specimen.

- **Generation of Notification Receipts:** For every notification that is send by a laboratory a receipt must be generated that includes information regarding the content of the notification itself as well as information on the calculated receiving public health office (e.g. contact information). The receipt should be encoded in the portable document format (PDF). In addition selected information should be returned in a machine processable format as well.
- **Support for the Detection of Duplicate Notifications:** The system must support the detection of notifications that where accidentally sent by a laboratory multiple times or notifications that are send by different laboratories but that refer to the same case (person and pathogen). As it is forbidden to store unencrypted personal data within the system the functionality must be implemented using pseudonymized notification data.
- **Receiver Oriented Encryption of Personal Data in Notifications:** Personal data of patients will not be stored unencrypted. Therefore the system must encrypt notifications as soon as the pre-processing has been finished. The implemented encryption mechanism must guarantee that only the receiving public health office is able to decrypt the notification.
- **Derivation of Epidemiological Information from Notifications:** The system must extract information from the notifications for getting an overview about the current epidemiological situation for the whole country. Personal data must not be included or must be replaced by pseudonyms. This information should be accessible by the RKI.
- **Extensibility to Support Additional Pathogens in the Future:** The first version of DEMIS will only support SARS-CoV-2 notifications. Nevertheless, the system must be designed in a way that additional pathogens can be supported with ease.
- **Usage of Strong Authentication and Authorization Means:** The system must use an authentication mechanism based on X.509 certificates. After an initial authentication with the corresponding cryptographic keys, derived security tokens may be used to access the API for sending or receiving notifications. An access control framework must guarantee that the APIs of the business services are only accessible when all access requirements are met and therefore a positive access control decision will be rendered. Attributes for the rendering of the access control decision must be extractable from the used security tokens (e.g. role information) as well as from the request or response payload (e.g. the notification itself).
- **Adaption of a Widely Used Laboratory Data Transfer Protocol to Support a Fast Rollout:** Implementing the HL7 FHIR based data format natively within the laboratory information system or within the connected communication servers might lead to delay in the planned rollout, as laboratories do not employ currently such technology. Therefore an adapter must be provided during a period of transition that is able to map LDTv2 based laboratory reports (that are widely used withing Germany) to HL7 FHIR based SARS-CoV-2 notifications.

4 SYSTEM DESCRIPTION

In this section we provide a system overview of both the backend services and the frontend components, followed by the description of the implementation during the first phase of the project in which only SARS-CoV-2 tests were handled and the currently under development extension for supporting multiple pathogens.

4.1 System Overview

4.1.1 Backend Services

On the server side of the system, the functional requirements were clustered around the entry point for the messages that are send by laboratories, the **DEMIS Notification API**. One of the main functionalities of this component is the validation of message (notifications) against a defined set of rules and as well as the routing to entitled parties (see Figure 2).

Further responsibilities of this component are:

- The enrichment of the message with additional attributes, such as the time of message receipt or the ID of the sending service provider
- the generation and persistence of pseudonyms using the **DEMIS Pseudonym Calculation**

Service and the **DEMIS Pseudonym Storage Service**,

- the generation of report receipts with the help of the **DEMIS PDF Generation Service**,
- the generation of non-named reports (information objects for better evaluation of the current epidemiological situation) for the RKI,
- encryption of the notification
- the transfer of the notifications and the generated information objects to the **DEMIS Notification Clearing API**

Furthermore, on the **DEMIS Notification Clearing API** both the encrypted notification and the information objects required for the evaluation of the current epidemiological situation are persisted in a database (**DEMIS Notification Clearing DB**) by the DEMIS Notification Clearing API and held for retrieval by the respective authorized agencies.

The service thus functions primarily as a retrieval point for the corresponding notifications and information objects and, in this context, implements the access rules defined indirectly via the health law.

Although for a detailed assessment of the epidemiological situation, it is helpful to identify all SARS-CoV-2-related reporting events for a person in the data set and to consider them accordingly. For good reason, the infection protection act allows only the respective competent health authorities to access personal information, such as the name of an affected person. A centralized search, for persons reported multiple times on a central database with personal information available in plain text, is thus explicitly not allowed. For this reason, the **DEMIS Pseudonym Calculation Service** creates special pseudonyms via selected personal characteristics (first name, last name, date of birth) in the course of pre-processing the reports. These pseudonyms later make it possible to recognize all SARS-CoV-2 related reporting processes for a person in a defined time interval without revealing the identity of the respective person concerned.

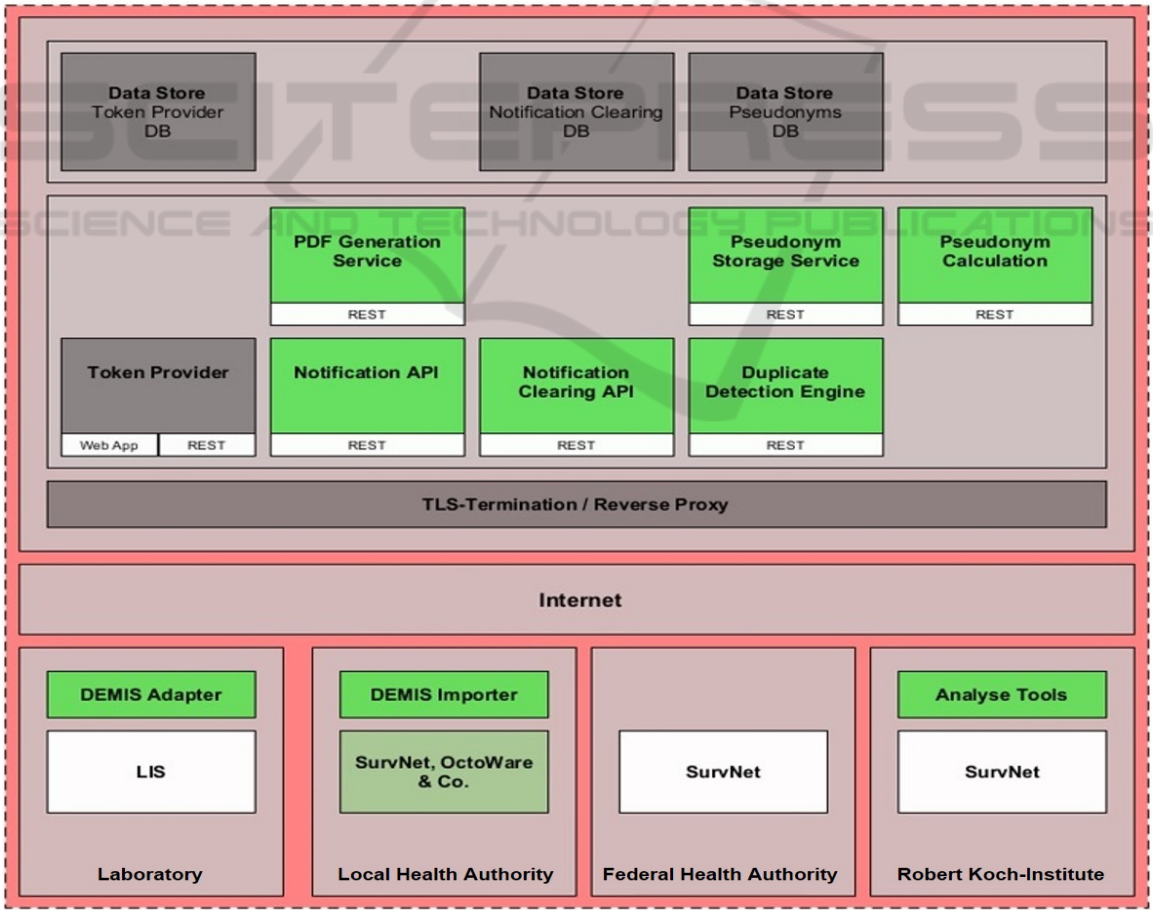

Figure 2: Demis SARS-CoV-2 system overview.

In order to be able to recognize all SARS-CoV-2-related reports or reporting processes for a person within a defined time interval, the **DEMIS Duplicate Detection Engine** was developed. The DEMIS analysis tools can pass a pseudonym to this service and have it check whether the pseudonym has more than one reporting procedure associated in the system. The implemented pseudonymization procedure also supports a fuzzy search, i.e. if desired, reporting procedures for persons in the database with a very similar name are also matching, for supporting the case of typing error).

All access to the central specialized services of the DEMIS infrastructure is protected by an access control system. In order to be able to call the operations required for the respective use case, the client must include a standardized security token in the header of the call. The **DEMIS Token Provider** issues these security tokens after successful authentication of the respective user. The authentication of the user is certificate-based. The **DEMIS Token Provider** also manages the user accounts. Corresponding information is persisted in a database (**DEMIS Token Provider DB**).

4.1.2 Frontend Components

For the first expansion stages of the DEMIS a highly specialized software component **(DEMIS Adapter)** is offered to the reporting laboratories. It fulfils the following tasks:

- Loading of LDT messages supplemented by Jokerfields from a data transfer directory
- Transforming LDT information into the data format defined by the RKI for the presentation of SARS-CoV-2 notifications (based on HL7 FHIR)
- Authenticating the laboratory against the DEMIS Token Provider
- Secure sending of notification message to the DEMIS Notification API
- Creation of audit logs for tracing the processing steps
- Saving the notification transaction receipt (PDF) returned by the DEMIS Notification API.

In coordination with the producers of software for public health office, the **DEMIS Importer** was developed for the first expansion stages of the system. It serves as a reference implementation for the adaptation of the various processes and will also be used in selected health offices for a transitional period. The DEMIS Importer fulfils the following tasks, among others:

- Authentication of the respective health office against the DEMIS Token Provider
- Retrieval of encrypted notification messages via the DEMIS Notification Clearing API
- Decryption and storage of the messages in the file system

The actual processing of notification content is implemented in the various software products (e.g. SurvNet@RKI) that is used by the different public health offices.

For future versions of the system it is envisioned that neither the DEMIS Adapter nor the DEMIS Importer will be used any longer. The corresponding functionality is planned to be implemented by the vendors of the respective sending and receiving information systems by then.

4.2 Implementation

To guarantee a good portability of the DEMIS services and components, only Java-based software published under an Open Source licence was selected or developed. In this context especially the extensive use of Hapi FHIR library (see UHN, Hapi FHIR library) should be mentioned.

The FHIR profiles are publicly available so that all involved participants can access them. Especially that some of the laboratories have decided to implement the last hop component in order to have a deep integration with the DEMIS platform and system. The profiles, code systems (for country code, material, method, postal codes) and value sets (test code values) have been published on the platform simplifier.net.

In the initial design, the DEMIS Adapter had also the role to verify the values received in the LDT file. The advantage of this solution was to have a fast feedback on possible errors due to the input values and not overload the system with error notifications. In the end it was decided to have the validation only at the Notification API, in order to have a uniform approach in technical support for laboratories that use the DEMIS Adapter or their own software.

The following sections will only focus on selected implementation aspects for the first and second development phase of the system.

4.2.1 First Phase: SARS-CoV-2 Only Tests

During the first phase of development the backend service had to go into maintenance mode quite often, e.g. to rollout new versions of the software. Therefore, special care was needed for detecting the maintenance and handling the error codes received by the frontend components from the DEMIS Token Provider (see Table 1) as well as the DEMIS Notification (Clearing) API (see Table 2).

Both the DEMIS Adapter and DEMIS Importer assume that there is an established internet connection when starting. This is why timeouts by connecting are considered as configuration failure, or in the case of DEMIS Adapter a misconfiguration of the proxy.

When designing the error handling in the case of the responses from the Notification API, it was also included the case that a component called by the Notification API, like the Notification Clearing API for example, would return error to the Notification API, thus a retransmission is necessary, similar to the maintenance state.

As the pandemic situation progressed, it was decided to include more information than the positive diagnostic and that encompasses information about the virus variant and the genomic information. Currently only the support for the case when the laboratory itself has the necessary analysis devices. The next step is to enable correlation between primary laboratories that receive the probes and the secondary laboratories that provide the genomic information or even invalidate the initial positive diagnostic.

4.2.2 Second Phase: Multi Pathogen Tests

During the development of the system it became clear that the DEMIS information model, especially certain ValueSets (e.g. test codes), had to be updated from time to time. Therefore, a functionality was developed that downloads the most recent versions from the FHIR data model server. Nevertheless, to implement the support for additional pathogens (e.g. influenza virus) this mechanism needs to be refined.

Both the DEMIS Adapter and the DEMIS Notification API have to be extended in order to be able to programmatically download, process and interpret not only updated ValueSets and CodeSystems but complete FHIR profiles (including StructureDefinition resources (see Figure 3).

While loading the profile into memory, the DEMIS Adapter implementation will be extended in order to build generic classes and factories that can model the notifications elements. A new input information element Pathogen Code will be added in order to retrieve the GenericPathogenFactory object from the internal mapping built during the loading of profiles. Using this GenericPathogenFactory, the input values that have an associated FHIR ValueSet are validated and the correct Profile URL is set in the notification elements that depend on the pathogen.

The DEMIS Notification API inherits the validation mechanism from the HAPI FHIR library validator that needs the profiles downloaded beforehand. Thus, downloading of the profiles is decoupled from the validation of notification so that the profiles download occurs during packaging and the validation during runtime. Although the FHIR Profile Loader has slightly different usage in the two components, the shared functionality of profiles download is quite important, especially that some special handling was needed because some aspects

Table 1: Token Provider response codes processing.

Type of Response	**Action**	
Token Provider	**DEMIS Adapter**	**DEMIS Importer**
Could not connect	Signal misconfiguration and shutdown	
Unknown resource path		
Invalid credentials		
Maintenance	Retry after a specific interval	
All ok	Save token for sending the FHIR Request	

Table 2: Notification API and Notification Clearing API error response codes handling at the DEMIS Adapter and DEMIS Importer respectively.

Type of Response	**Action**	
DEMIS Notification API & Notification Clearing API	**DEMIS Adapter**	**DEMIS Importer**
Could not connect	Signal misconfiguration and shutdown	
Unknown resource path		
Input Data invalid	Move input file to error folder	Abort operation
Internal Error	Retry after a specific interval	
Maintenance		
All ok	Move input file to submitted folder and save the Report Receipt	Save data in the local database

related to snapshot download from the publicly available FHIR data model server of simplifier.net are not yet available.

5 PERFORMANCE TESTS

There were several tests carried out in a laboratory setup, from which here selected are those related to the performance tests of the Notification API, the system entry component.

In the setup, depicted in Figure 4, the VMware ESXi, 6.7.0 hypervisor was deployed on a PowerEdge MX740c hardware with an Intel(R) Xeon(R) Gold 6126 CPU @ 2.60GHz processor. The VMware configuration included twenty-four logical processors and three network cards.

The Token Provider keycloak and the Postgres database of the Notification Clearing API were dedicated each a virtual machine of 4 virtual CPUs and for the rest of the system components the number of CPUs was increased starting from scenario A with 4 CPUs and finishing with scenario C with 16 CPUs.

The simulator for generating the requests was developed based on the Scala based gatling test load generator (see Gatling Toolkit) and it was used to simulate 20, 40, 80 and 160 parallel laboratories.

In Figure 5 the measurement results regard the mean response time and the associated standard deviation on the enfolded scenarios.

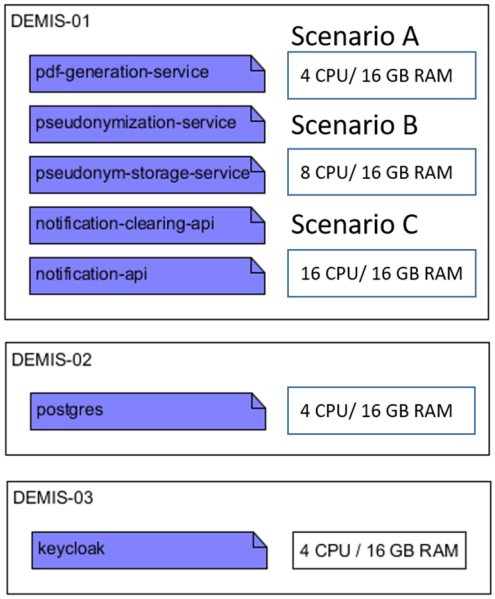

Figure 4: Test setup.

One can observe that the response time is decreasing when the number of allocated CPUs increase. At the same time, in scenario C,80 the highest mean speed is reached at about 49 000 requests per second and there are error response codes encountered. It was concluded that the Notification API is the bottleneck and an adjustment of the setup using load balancing between multiple instances of the Notification API has proven to extend the performance of the system as a whole.

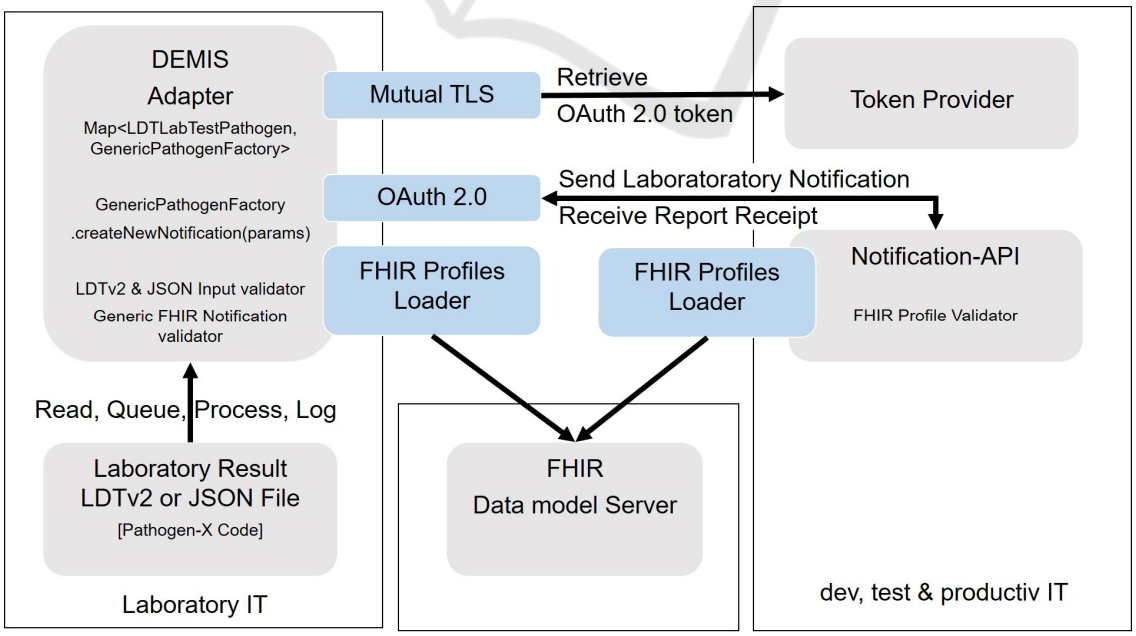

Figure 3: Support for multiple pathogens.

6 ROLLOUT

In order to prepare for the productive system, the development team deployed a replica of the DEMIS platform on an internal network Openshift testbed in order to have preliminary validation of the releases. Another replica was used for the most recent develop version as stub test system.

A replica of the productive system was deployed for testing purposes, so that both laboratories and local health authorities can test their settings and implementation.

The rollout of the system took place gradually, starting with the first validated release of the project and only a small number of laboratories and public health offices in July 2020. By now (January 2021) more than 250 laboratories and all public health offices (375) are using the system (see Figure 6).

During the rollout numerous workshops took place for familiarizing the laboratories and local health authorities' workers with the new platform. Their feedback was used to adapt the system and build the roadmap for future releases. For example, on the side of the laboratories, some of them decided to have a deep integration, with their primary information system, either implementing the interfaces towards the DEMIS Token Provider and DEMIS Notification API from scratch or using the code from DEMIS Adapter. Others, due to lack of IT resources, decided to continue the use of the DEMIS

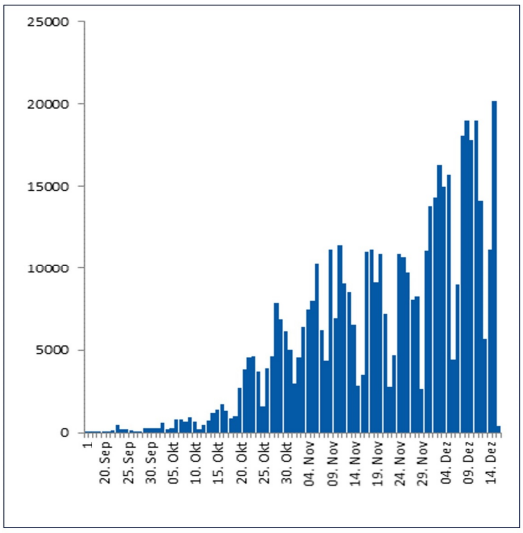

Figure 6: Number of laboratory notifications sent per day via the DEMIS SARS-CoV-2 platform.

Adapter and asked to include additional functionality, e.g. support for an alternative input format (proprietary JSON), a monitoring interface, multiple test results in a single notification as well as the support for multiple notifications within one LDT file.

An important feature request from RKI has been to support the transfer of information that is associated with a molecular surveillance system for SARS-CoV-2 and other pathogens. This functionality was already implemented and rolled out.

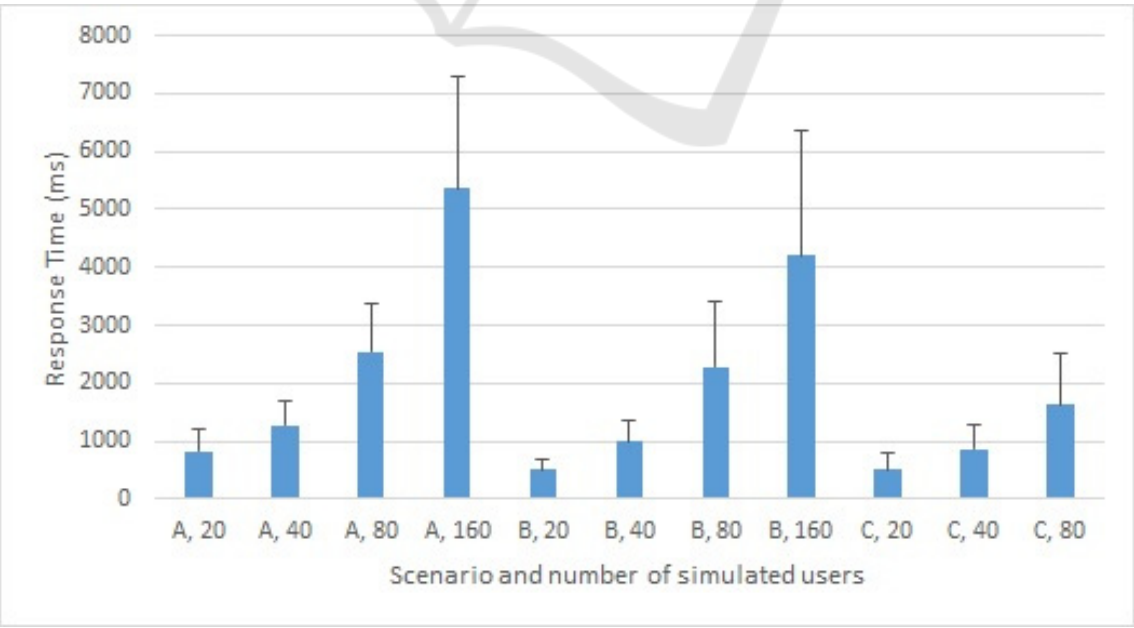

Figure 5: Test results.

7 CONCLUSION AND FUTURE WORK

The DEMIS SARS-CoV-2 project included a broad set of stakeholders in the domain of laboratory tests that ranged from hospitals to laboratories of all sizes, including mobile test sites and even veterinary laboratories that decided to help by performing SARS-CoV-2 tests. Their feedback and engagement have contributed tremendously to the success of the project and upgrade of the infrastructure in a matter of a few months.

The next milestone will be the support for the other more than 50 notifiable pathogens defined within the German Infection Protection Act. This major extension - as well as many other smaller improvements - will make the DEMIS platform even more powerful and ready to be adapted to other countries that need to improve their reporting systems.

ACKNOWLEDGEMENTS

DEMIS SARS-CoV-2 was financed by the German Ministry of Health (BMG). The functional requirements as well as the data model were defined by the Robert Koch-Institute (RKI), Fraunhofer FOKUS was responsible for the design and development of the system, gematik GmbH and RKI accompanied the design and development process and coordinated the test, operation and rollout.

REFERENCES

RKI, Homepage of DEMIS project, https://www.rki.de/DE/Content/Infekt/IfSG/DEMIS/DEMIS_node.html

HL7, FHIR standard, http://hl7.org/implement/standards/fhir/

D. Hardt, 2012, OAuth 2.0 authorization framework, RFC 6749, IETF

M. Jones, J. Bradley, N. Sakimura, 2015, Json Web Token (JWT), RFC 7519, IETF

B. Campbell, J. Bradley, N. Sakimura, T. Lodderstedt, 2020, OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens, RFC 8705, IETF

QMS and KBV, LDT Standard (Labordaten-Transfer), https://www.qms-standards.de/standards/ldt-schnittstelle

Openshift Platform, https://learn.openshift.com/

Docker tool, https://www.docker.com/

Kubernetes tool, https://kubernetes.io/

RKI, Homepage of SurvNet tool, https://www.rki.de/ DE/Content/Infekt/IfSG/Software/software_inhalt.html

University of Health Network (UHN), Hapi FHIR library, https://hapifhir.io/

Gatling Corp, Gatling Toolkit, https://gatling.io