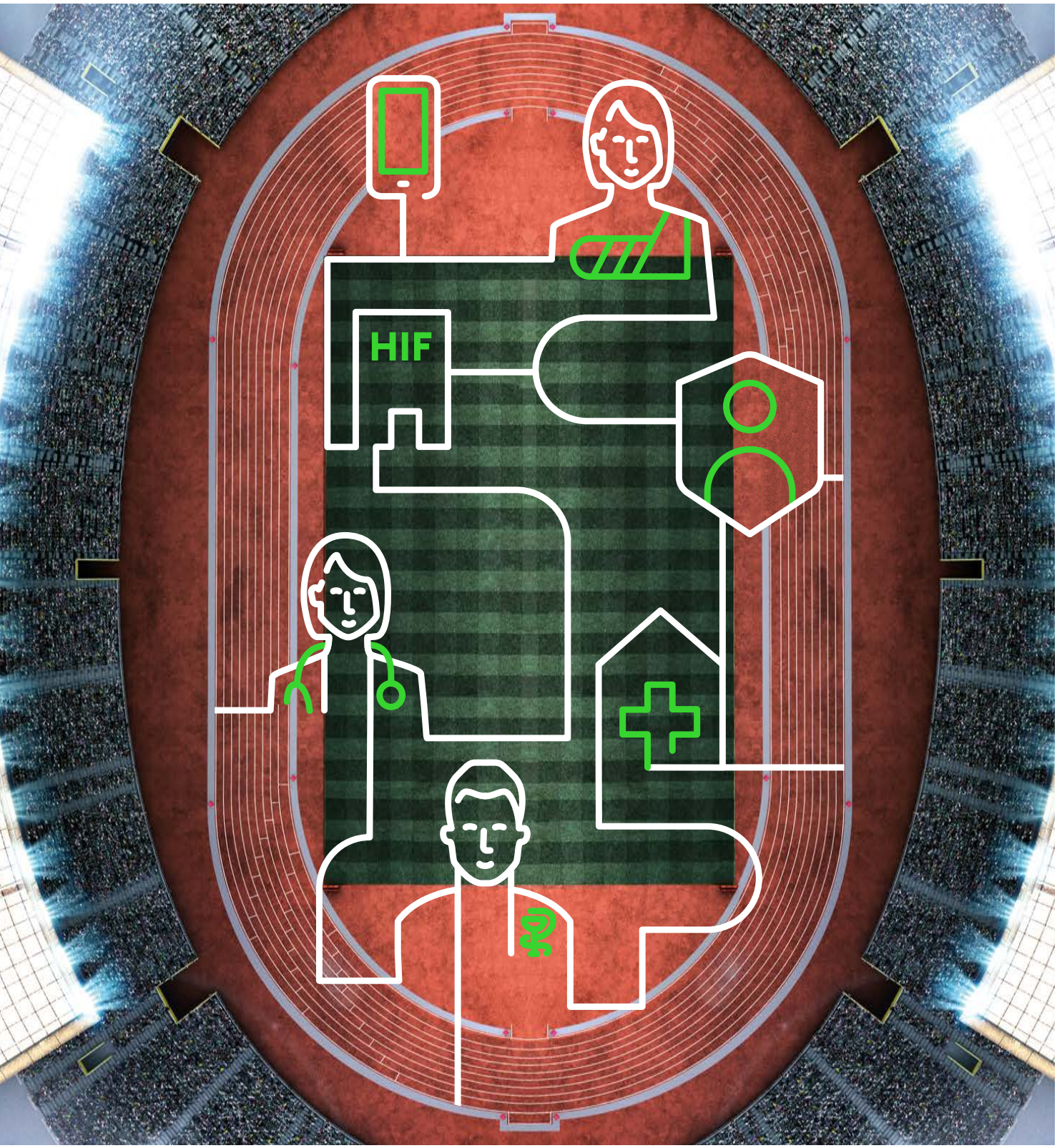
gematik



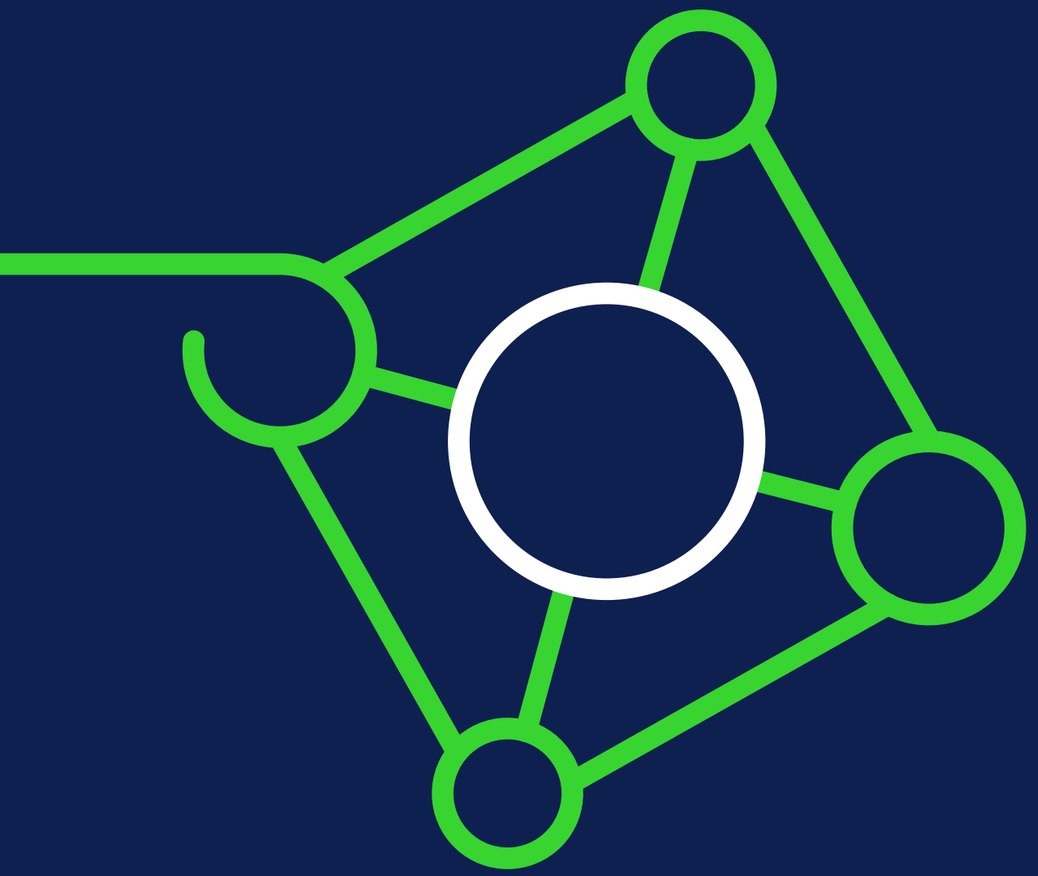
An arena for digital health

Telematics Infrastructure 2.0 white paper
for a federally networked healthcare system

A note on gender:
To enhance readability, masculine pronouns are generally used in this publication. Please do not regard this as an indication of gender-specific value judgments.

Table of contents

1 Introduction



1.1 What does this white paper aim to achieve?

After a long period of dormancy in Germany, the digital spring has arrived for many stakeholders in the country's healthcare system. Inspired by dynamic international developments and opportunities, there is now a noticeable zest for action in Germany.

This white paper aims to generate target-oriented and stimulating momentum for the shared process of shaping digital health in the German healthcare system and to promote a common approach for all the protagonists in digital health.

In pursuit of this goal, providers are invited to a constructive innovation dialogue, and TI users are invited to a focused value-added dialogue, with gematik.

The desired outcome is the concrete and iterative implementation of a stable and future-oriented **arena for digital health,** which should be jointly pursued and effectively supported and implemented by means of user-oriented partnerships.

1.2 Why do we need an arena for digital health?

One of the central challenges facing the German healthcare system is the cooperation across the borders of the individual service areas. Digitalization makes it possible to connect islands of medical care with the participating professions, provided that all the partners work together to define care processes and communication.

In 2005, gematik began to create the telematics infrastructure (TI) for this purpose. The image of the TI as a "highway for the healthcare system", which was commonly used in the following years, expresses the intended acceleration of the relevant processes, but also reveals a problem. A highway does not encourage interaction. On the contrary, direct interaction – the collision of two users, i.e. cars – is the worst case scenario.

From gematik's perspective, the chief goal is to serve the healthcare of the future and shape it by means of digital services. That requires participation in digital health to be as uncomplicated and flexible as possible. In order to enable cross-sector interaction and cooperation, this participation needs a protected framework and optimal conditions for fair and high-quality competition. From gematik's perspective, this is symbolized by an arena in which the providers and the users of digital health come together.

Future viability and long-term economic efficiency now require a technological leap

The development of the telematics infrastructure has been ongoing since 2005. A series of fundamental design decisions regarding the structure of the TI were made at a time when many of the technical requirements that are a matter of course today, such as smartphones and cloud data services, did not exist. Consequently, a technological leap is needed in order to ensure future viability. In addition, this leap offers the opportunity to achieve economic effects that are sustainable over the long term.

Necessity and motivation: Shaping the digital transformation together

Since the initial concept of the TI was formed, there have been fundamental changes in the cultural environment, the technical possibilities, the market and the political conditions.

Along with broad-based digitalization, a transformation has taken place in the healthcare system. The underlying digital connectivity, which has been the focus of the TI until now, is today regarded as a matter of course. As a result, needs have shifted toward higher-value opportunities for integration.

That's why useful applications that improve care processes and provide optimal integration opportunities should be offered. This will also provide opportunities to replace structures, components and procedures that have turned out in the past to be difficult to operate, minimally cost-efficient or functionally restrictive. And that opens up the perspective of significantly reducing the costs of the TI.

The conversion to the TI 2.0 should be accomplished by the year 2025 and should proceed step by step.

The key challenges to be solved through the iterative further development of the TI are:

1. Flexibility and user-friendliness in identity management
2. Universal accessibility of the TI services
3. Operational stability and adaptive modern security concepts
4. Intersectoral and international interoperability
5. Data sovereignty of the distributed services
6. Integration of data across services and applications

Challenges 1) through 3) can be met faster, and the technical solutions generate a direct value added. Challenges 4) through 6) are more multilayered and complex, and they require preceding iterations.

If all six challenges are mastered by means of targeted measures, there is tremendous potential for improving healthcare provision, healthcare research and economic efficiency in the healthcare system.

The **arena for digital health** is similar to a modern Olympic stadium in which many accredited top athletes and teams compete in their various disciplines and participate in the games according to transparent rules. The arena combines the democratic, fair, competition-oriented and formative guiding principles with the service and user-centred approach of a modern digital platform.

1.3 How does this fit in with the basic principles of the digital transformation?

Convergence and interaction are essential principles of the digital transformation, as well as the two central themes of the **arena for digital health**.

The harmonization of framework conditions and the standardization of information technology create the basis of a digital healthcare platform that not only makes network effects possible but also purposely stimulates them. That is because an increase in the number of players, offers and playing fields creates value added for the insured parties as well as their family members, the doctor, the hospital and the care facility.

1.4 What fundamental role is gematik playing in this transformation?

As a national centre of expertise for digital health, gematik supports the efforts of providers and users to make positive network effects possible. gematik's core area of expertise is relevant in five areas of action:

1) A platform for a national telematics infrastructure: gematik establishes the basic functionalities and security measures for a common nationally usable platform so that it can be shared by as many participants as possible.

4) A forum for future concepts of digital health: gematik has a wide network of contractual partners and supporters, including the central organizations of the healthcare system as shareholders. To promote the mutual dialogue about the future, gematik will develop the forum for sharing ideas and presenting innovative solutions.

2) A centre of expertise and a coordination centre for standardization: gematik coordinates the close communication with the community of standardization experts, the medical profession and industry. It hosts the round table for targeted and internationally implementable standardization on the basis of internationally recognized standards.

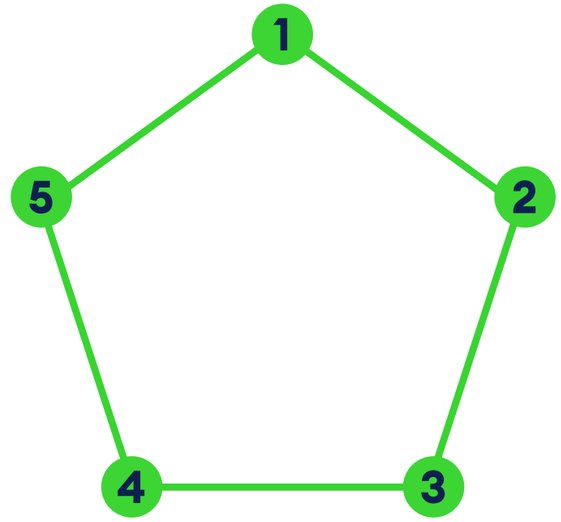
5) A European partner and moderator for national cooperation: In European projects, gematik specifically supports the promotion of uniform data formats for the cross-border sharing of patient data in the EU. It also closely cooperates with other national centres of expertise for digital healthcare and with European authorities.

3) A partner for providers and users: gematik advocates user-focused dialogue and provides advice regarding specific technical matters. It focuses on partnerships and these partnerships' support for solutions. Only in exceptional cases does gematik develop applications of its own.

For the arena for digital health, this means that:

Participation is reserved for qualified providers that are officially authorized.
gematik is the gatekeeper for participation. It safeguards the consistent quality of service and applies its house rules, so to speak, in order to ensure the quality of service if the necessary qualification is not available.

Essential basic services are provided so that value-added offers can be created on this foundation.
In order to create a wide variety of offers, gematik will provide generic services as open-source solutions in selected cases. All the participants have the opportunity to create their own value-added offers on the basis of these solutions.



The various disciplines will find their own user-friendly and ready-to-use playing fields in the arena.
gematik will ensure that all of the players who participate in healthcare can find the appropriate playing field for the respective application.

The competition will be based on internationally recognized and well-established uniform standards and regulations.
gematik sets transparent standards so that there will not be a confusion of languages or distorted competition. The rules and requirements will be transparent. Integration will prevent isolated stand-alone solutions.

The individual playing fields will be monitored in order to ensure compliance with the respective rules of play.
gematik will act as a referee to punish every foul. It will use technologies in order to enable the games to proceed as smoothly as possible and to facilitate an undistorted result.

2 Executive Summary

Against the background of major changes that have already taken place and in view of today's technical possibilities and the economic and political conditions prevalent in the market and in the cultural environment, a new conception of the TI is urgently required. This new conception is to prepare the TI for a future in which the German healthcare system is completely digitally connected, healthcare scenarios go beyond the care-provider environment, and many new players are connected, from the care sector to the providers of digital healthcare applications.

In the summer of 2020, structured, guideline-based interviews on the basis of an analysis by gematik took place with all of gematik's shareholders in order to identify the requirements for a further development of the TI. The results of these interviews were consolidated and presented and discussed in the context of the shareholders' strategy workshop. As a result of this shareholders' strategy workshop gematik created a suggested solution detailing how the requirements and conditions could be fulfilled by means of a further-developed TI – a TI 2.0. gematik sees the following five premises and requirements for the further development of the TI:

2.1 Acceptance can only be successfully promoted by a systematic focus on the user

Value-added applications for patients, doctors and nursing and care staff need secure basic facilities and usable healthcare data. The basis for this is provided by a network of partners and services.

It must be possible to make available application-independent basic services for value-added applications provided by third parties so as to provide the basis for an ecosystem to develop alongside the demands of the various user and application groups. From the point of view of gematik, this should ease the administrative burden on the medical professions and contribute to turning healthcare management into a team effort. The first example applications are communication in the medical sector (KIM) and the electronic certificate of incapacity for work (eAU).

This will result in more efficient and effective healthcare management in the future.

2.2 Future viability and long-term economic efficiency now require a technological leap

The TI must develop further because it is based on considerations, design decisions and premises from the first decade of the 21st century. In the meantime, essential parameters have changed:

Since then, medicine has become based on data to a greater extent and dependent on available structured data that can be used on a secure platform. User-friendly mobile applications have become standard for users in many areas of social and economic life. IT security requires a holistic and adaptive concept that must be continually scrutinized anew.

New disciplines need new playing fields and a robust architecture. The objective is a well-equipped arena, in order to enable the best medical care.

In the future, digital health applications (DiGA) will provide a new, third pillar of patient care, alongside the institutions providing primary care and those providing inpatient care. Germany is taking on a pioneering role in the integration of medical apps in healthcare with the "DiGa-Fast Track". The electronic health record (EHR) will be introduced step by step from 1 January 2021. The interaction of these various players should be more strongly supported as a result. The fundamental architecture of the TI must become more independent of specific technologies so that data silos can be dissolved and mobile patient care made possible.

2.3 Reliability, availability and credibility are the result of a new operating and security model

More players and more levels require flexible trust relationships and clear rules of play. The TI arena provides the entrance control and the referees for the games.

gematik views the TI as the arena for all professional groups providing patient care in the future. The utility increases with growing numbers of user groups and applications. At present, not all of those involved in the provision of patient care are connected with the TI. The objective is to achieve a good balance between low barriers to entry, in order to develop a substantial force towards integration, and secure and stable operation of the TI. gematik intends to make possible flexible trust relationships that enable the various contexts, players, providers or services to interact and communicate securely. Specific rules of play collected in a policy and enforced by referees will apply to the different "playing fields".

2.4 Cross-border medical care and location-independent security for patients require interoperability

Diseases recognize no borders. Competitiveness and international connectivity require a compass for standards and jetties for cross-border applications.

According to the international Digital Health Index of the Bertelsmann-Stiftung, Germany was still in the relegation zone in 2018. Since then, the common incentive has been the jump into the international premier league. The specification of technical standards for a digital healthcare system on the national level is not adequate to achieve this. The perspective required is that of international connectivity. For this reason, the internationally recognized and used standards, such as FHIR with the introduction of the E-prescription, will also become widely accepted standards in Germany in 2021.

The political guidelines call for gematik to connect the TI to Europe and so enable concrete value added for patients. The international sharing of patient data creates safety for patients. Achieving this requires interoperable systems and formats. The associated vision is of a secure national arena with a wide jetty for Europe. In the future, patients should be able to use digital services such as the short form of the electronic health record and the electronic prescription everywhere in the EU, regardless of whether they are at home or travelling abroad. To this end, the telematics infrastructure will be further developed so that in the future it will be the secure international harbour for digital patient services

2.5 Continue speeding toward digital health in the fast lane with a holistic approach and a superordinate target

At present, the German healthcare system is experiencing its digital spring.

The race to catch up in digitalization is not only with respect to the level of our European neighbours and the possibility of international connectivity. It is also much more a matter of keeping pace with the level of technology that is already successfully and usefully integrated in many other areas of everyday life and economic activity. The aspiration that serves as the guiding principle of this white paper is to participate in shaping the new digital era and to better improve and protect health by means of a digital healthcare system.

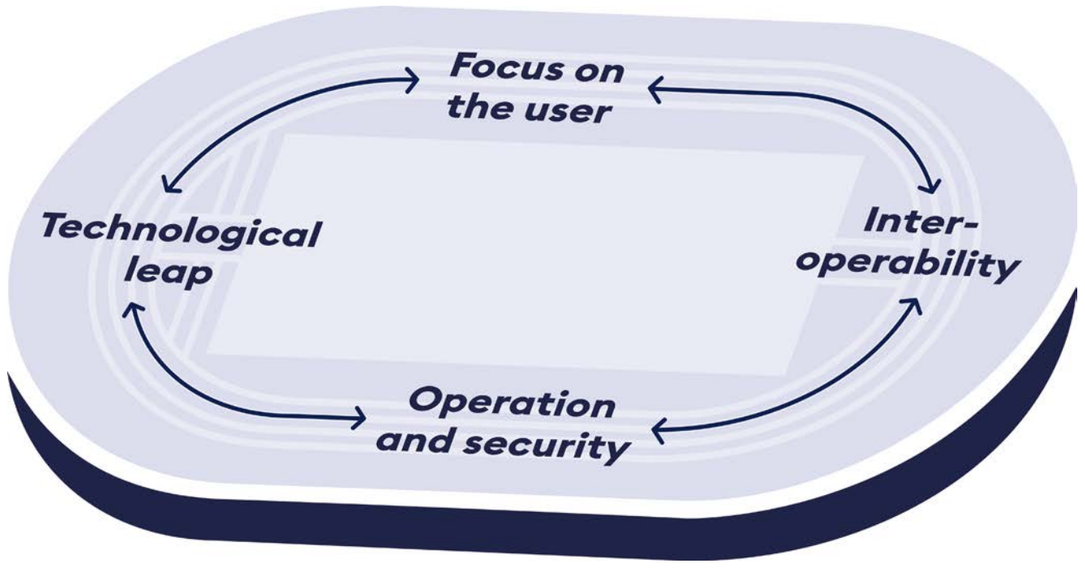


Figure 1 – The foundation of the **arena for digital health**

From the challenges of the TI to the new pillars of the **arena for digital health**

The overall architecture of the TI 2.0 is based on six supporting pillars:

1

a **federated identity management**, because this "bridge" enables greater flexibility and increased user-friendliness for the user groups' own digital products thanks to the simple use of the TI's identity confirmations.

2

the **universal accessibility of the services**, because the elimination of proprietary IT solutions (e.g. connectors) lowers costs and stabilizes operation.

3

a **modern security architecture**, because this will enable the independent provision of services by various providers and is both more secure and more efficient.

4

distributed services, because the linkage of data from various sources is necessary from the point of view of optimized healthcare processes.

5

interoperability and structured data, because research into and the provision of healthcare on the basis of use cases requires an improvement in the quality of data. Standards-based structured data and interfaces increase the availability of products and services.

6

an **automated processable policy** of the TI, because an automated review of the security, the data protection, the interoperability and the availability strengthens trust in the TI.

In the future, these architectural principles will more strongly support and promote the different healthcare scenarios from the respective user perspective. The TI serves to electronically share the healthcare data of all medically insured individuals in Germany securely in a manner that guarantees the insured individuals' right of self-determination. This requires comprehensive security measures, both in the technology and in the authorization structures.

The TI 2.0 offers simplified user integration and new user groups and of their systems. It focuses on recognized IT standards in order to strengthen the intersectoral and international interoperability.

Only then will artificial intelligence (AI)-supported interactions between the applications and the future application scenarios, e.g. in digitally supported medical care or medical research, be possible.

The restructuring of the TI reduces the complexity in regular operation and improves operational control by gematik. This promotes the stable and secure operation of the TI. These architectural principles and the effects they achieve in practical use offer the prospect of substantially improving the economic efficiency of the TI.

3 Why does the TI need to develop further?

3.1 What has changed?

The TI must develop further because it is based on considerations and premises from the first decade of the 21st century.

The technological basis of the TI was laid down more than ten years ago. There has been enormous technological development since then. The possibilities of Internet-based services have permanently changed technological standards and user behaviours. The new technological standards enable a much more economically efficient and qualitatively higher-value implementation of digitalization than would have been imaginable ten years ago. In addition, the new requirements and demands of residents and insured individuals, medical expert groups and healthcare companies can only be met by a modernization of the TI. Rapid technological progress and the resulting possible applications require a flexible and open application and data ecosystem.

In the meantime, essential parameters have changed:

- **In medicine:** Data-based diagnosis and medicine are the foundation for most current medical progress and are also becoming standard in healthcare. The COVID-19 pandemic has made it clear that health data and disease registries are only useful when they are networked and capable of analysis over the widest possible area. Rapid and comprehensive access provides value added for medicine.

- **User behaviour is more demanding nowadays:** Mobile devices and mobile use have long become standard, even in sensitive areas such as financial services and banking. The decisive criterion here is the user-friendliness provided by mobile access, which IT in the healthcare system still has to catch up with.

- **Technological:** Today IT security is planned and implemented differently than it was in the preceding decade. To this end, gematik broadens the previous area of consideration, continuously adapts new requirements and promotes open discussion with its partners. The fundamental architecture must become more independent of specific technologies so that data silos can be dissolved and mobile patient care made possible. The trend is clearly in the direction of the cloud, with unlimited resources and economies of scale. The spread of the open source culture in society and industry has increased strongly.

- **In the healthcare system:** In the future, digital health applications (DiGA) will provide a new, third pillar of patient care, alongside the institutions providing primary care and hospital care. Germany is taking on a pioneering role in the integration of medical apps in healthcare with the "DiGa-Fast Track". The electronic health record (EHR) is being introduced step by step from 1 January 2021. The interaction of these various players should be more strongly supported as a result. The standardization of the content of corresponding medical information objects (MIOs) is increasing. The sovereign patient demands the option of playing an active role in the treatment process.

gematik has been presented with new requirements and demands by the respective user groups.

An integrative platform is required, because otherwise the gathering momentum will increase the risk of further isolated solutions for functions. As a result, this platform is to integrate services from various care providers. These services will then be offered to all users of the TI (e.g. health insurance services).

The services providing connection and linkage to the TI that are offered should be as frictionless as possible in order that parties such as doctors can concentrate on the provision of medical care.

At the EU level, improvements in the provision of cross-border healthcare and more intensive cooperation in research are required and supported, in particular in the light of experience with COVID-19. Both require a secure platform and a uniform communication format for the useful exchange of health data.

The definition of appropriate structures for the health data and the established use of international standards are one current challenge. The next such challenge will be to master the establishment of processes and security mechanisms for the provision, utilization and secondary use of health data in the national and subsequently the EU-wide healthcare data space.

More players and more levels require flexible trust relationships and clear rules of play. The TI arena provides the entrance control and the referees for the games. The **arena for digital health** creates...

- an adaptive modern security concept and monitoring of the operations
- increased technological independence
- the restructuring of the closed user group into a controlled integrative ecosystem
- identities linked to sectors
- transparency between partners and with respect to the public sphere
- simplification of the process of expanding user groups

3.2 What are the key lessons learned from the TI's operation?

Since the launch of on-line productive operation of the TI on 1 July 2017 there have been various operating problems which gematik has taken as grounds to increase the stability of the system over the long term.

In line with its statutory task, gematik has to monitor the operation of the TI. This must be ensured by an appropriate governance structure covering the suppliers and service providers responsible for the operation of the individual services. gematik itself is not an authorized participant in this.

The purpose of gematik's monitoring is to continually improve key components of the TI and to minimize possible defined points of failure.

The following points are the primary focus of the further development of the TI's operation:

1. System stability

The failed change of the DNSSec trust anchor on 27 May 2020 demonstrated just how important it is to use various technical options to stabilize such a large and complex IT operation as the telematics infrastructure.

The change led to an interruption, the cause of which lay in the central part of the telematics infrastructure and was able to be rapidly (approx. 26 hours) resolved. Extensive manual measures (installation of a connector update) were, however, necessary in the decentralized zone. These measures gave rise to significant effort, and in consequence costs, over a longer period (52 calendar days) at the TI access services in particular.

Fundamentally, the incident once again demonstrates the importance of a functioning TI. Even though up to this point in time "only" the insured individuals' master data management application had been affected, it was already clear that the TI is increasingly becoming part of day-to-day business in the care-provider environments. With this realization the expectation is arising that the TI will always be available.

Nonetheless, major disruptions in the IT environment can never be ruled out, which means that gematik bears the responsibility for further increasing the resilience of the TI.

Connector failure 2020

- **Problem**: approx. 80,000 connectors lost the connection to the central TI
- **Focus**: all affected connectors (approx. 2/3 of the total) required the application of a manual update
- **Effect**: 52 days of fault rectification for a fault duration of 26 hours with ten days of uncertainty concerning the effects of the interruption on the care provider
- **gematik's response to the crisis**: coordination of 20 service providers affected and the stakeholders affected

2. gematik must be a participant in the telematics infrastructure

A complete monitoring of all of the services with the highest-security authorization structure requires that gematik possess all of the necessary rights (including identities) that would allow it to monitor individual services and the chains resulting from them. This would enable gematik to recognize complex fault scenarios at an early stage and to estimate their effects on the participants – insured individuals and care providers.

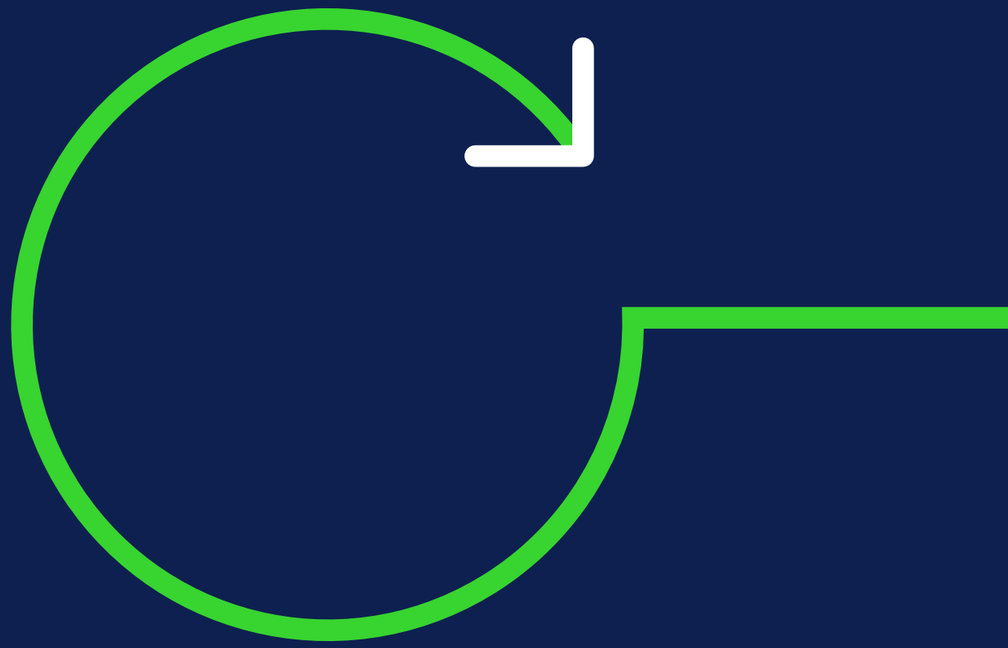
The essential challenges and areas of action of the further development of the TI may be summarized as follows:

- Enabling connector-independent access to TI services in order to make applications faster, more economically efficient and usable on the basis of the latest technological developments.
- Increased concentration of responsibility for the security and the protection of personal data at the professional computing centres of the TI in order to reduce the loads on the individual doctors, hospitals and pharmacies in the decentralized zone of the TI.
- Transferring the card-based applications to services of the TI in order to break up data silos and to enable fully fledged mobile patient care.
- Organizational and legal separation of the platform and the applications in order to make applications useful more rapidly and more economically and to be able to flexibly extend and migrate them.
- Expansion of a human-readable and machine-processable policy framework with properties to be attested. This will make possible reliable trust relationships between providers and with the users, enable acceptable use policies to be enforced technically, and enable users to select applications and services and link them with one another according to the users' own criteria.
- Creating the preconditions for a uniform eID for all applications of the German healthcare system in order to enable application-independent healthcare processes by means of single sign-on.
- Creation of a federated identity management according to uniform standards, in order to minimize administrative costs and the misuse of identities, also confirm identities for sector or statutory health insurance fund-specific applications outside the context of the TI, and to create an overall level of security.
- Support of uniform standards for improving interoperability between institutions, organizations and sectors of the German healthcare system (architecture of standards).
- Strengthening the sovereignty of the patient with respect to the conceptual administration of access rights in a federated healthcare system with distributed services.

4 How should the TI 2.0 evolve?

A technological leap is intended to safeguard the future viability and improve the focus on the user so that the attractive and popular platform for digital applications and services in the healthcare system can continue to grow.

The further development of the TI should take place under the following premises:



4.1 Ten basic principles

1. Reliable infrastructure
2. Data sovereignty
3. Based on international standards
4. A federated, uniform eID system
5. Location-independent access and mobile usability
6. For its own applications and those of third parties
7. Focus on specific care scenarios
8. Modern delivery processes and cloud support
9. International connectivity thanks to initial EU-compatible applications
10. Step-by-step migration

Long-term aim: The arena for digital health.

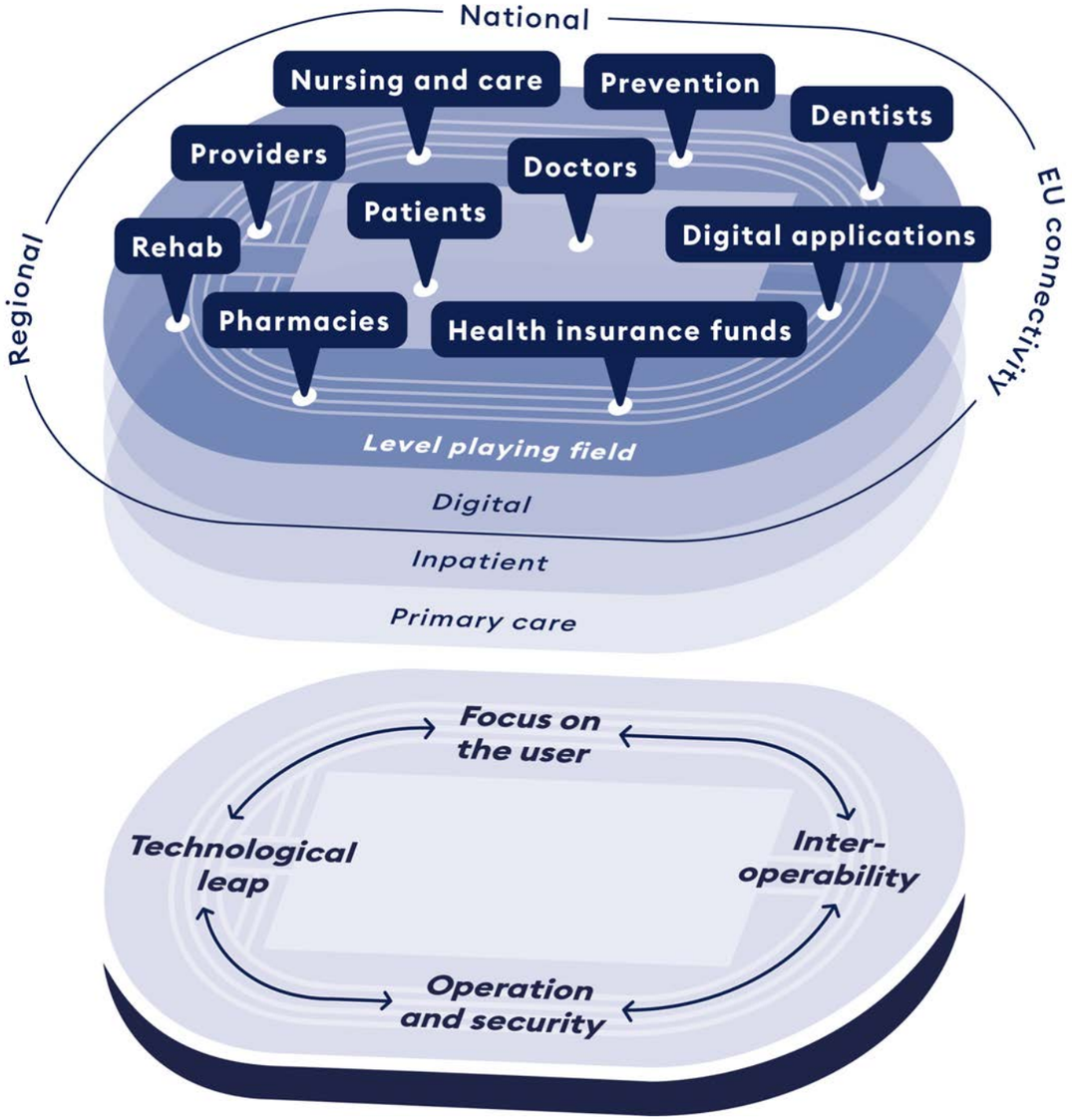


Figure 2

4.2 New disciplines need new playing fields and a robust architecture: The overall architecture of the TI 2.0

The transition to the TI 2.0 fundamentally changes the structure of the TI. **Four key changes** are essential during this process:

Universal accessibility of the applications thanks to interfaces on the Internet

The TI 2.0 will change the way that applications can be accessed. Specialized services will be made accessible via the Internet so that they can be used independently by insured users via apps on mobile devices and by care providers within and outside hospital environments. The TI's VPN will become obsolete as a result, because its access points are limited to inpatient care provider environments. Moreover, users will no longer need proprietary solutions – the connectors – to connect them to the TI. As a result, it will no longer be necessary to update the electronic health card (VSDM – insurance master data management) at doctors' practices, for example. Instead, the latest insured individuals' master data and insurance status will be provided to authorised users as a service on the Internet.

Guaranteeing security and data protection and the closed user group required by the regulatory regime will be accomplished by a contemporary security concept. Instead of access to a closed network, access to the individual services will be provided and restricted to the authorised users. The elimination of the VPN paves the way for the simplified integration of specialized services into the TI in the future and enables the intersectoral and cross-application integration of services. This also applies to services that are provided by players in the healthcare sector independently of the TI's specialized services as mandated by law. The elimination of proprietary networks greatly reduces complexity and thus enables new applications to be provided more quickly and improves operational stability.

A key consequence of this change is that users (especially care providers) have much easier and more cost efficient access to the TI applications. Moreover, new applications can be incorporated much more easily and cost efficiently than was previously the case.

Increased flexibility and user-friendliness as a result of eID and identity providers

Compared to the smartcards (eGK – electronic health card, HBC, SMC) used in the TI, which serve a dual function as identity carriers and a means of authentication, identity providers (e.g. health insurance funds, associations of medical doctors and pharmacists, associations of statutory health insurance physicians etc.) take over the task of user authentication in the TI 2.0. The specialist services implement access rights on the basis of electronic identities and other characteristics.

Thanks to this change, it is much easier to use the TI securely and the TI authentication mechanisms can also be used for the digital services of the shareholder organizations.

Reducing the operational complexity through standardization

The availability of all of the TI's specialist services via the Internet shifts almost all of the TI's operational performance to computer centres. This also applies to security services that are used in the care provider's environment. Examples include certain types of encryption as well as electronic signatures. These are being transferred to services, thus enabling users to dispense with proprietary TI-specific components as well as the connector and the eHealth card terminal.

The consolidation of previous services of the decentralized TI components in computer centres greatly reduces the amount of the TI-specific information technology that is required in medical practices and thus eliminates the need to implement various TI-specific security measures.

This change substantially improves the TI's operational stability, lowers dependence on individual specialized industrial providers and greatly reduces the costs of decentralized support.

Intersectoral and international connectivity through interoperability

One of gematik's central and most important tasks is to ensure interoperability with respect to the interfaces of the TI and its client systems, including the exchanged information objects.

Beyond the immediate borders of the TI, gematik has the task of promoting interoperability and thus helping to realize the vision of a pervasively networked healthcare system.

In order to largely prevent gematik from being tied to proprietary commitments, it uses the interoperability standard HL7-FHIR for the interoperable interfaces of the TI 2.0. This standard comes from the healthcare sector and is internationally recognized. Other standards, e.g. for interoperable messaging, are taken into account as well.

This change results in higher availability of and lower prices for the TI products and services. Moreover, the selection of the interoperability standard FHIR will provide momentum for a significant improvement in the data quality that is useful for healthcare.

The arena for digital health rests on six architectural pillars:

Federated identity management

The TI 2.0 is a federated system with a uniform level of confidence. In this system, the sectors serve as identity providers. The chip card is no longer the only means of authentication. On the contrary, the users can employ various means of authentication in order to obtain an electronic identity confirmation and use it for all services to access data. An identity-confirming service must be authorized before it can be included in the TI.

Universal accessibility

As users of the ePA (EHR — electronic health record) and the electronic prescription, insured persons are independent players within the TI. They can use their own devices and application front-ends to obtain direct access to the TI services via the Internet. Care providers can also gain such access in mobile scenarios if the services of the TI have also been made directly available for them via the Internet. This concept should also be transferred to existing applications (e.g. access to insured individuals' master data) and future ones.

State-of-the-art security architecture

In the future, the closed network for data exchange in the healthcare sector will no longer be defined by a hard physical network border. Only certified, authenticated user groups will be permitted to access the TI services. The communication relationships between users will be defined and controlled on the application level. This ensures that the closed user group of the TI is retained and access to and use of the TI will continue to be controlled. The security of digital interaction in the TI is generally achieved by means of secure, reciprocal authentication and further well established protective mechanisms of zero trust networking.

Structured data

The abstraction from the physical storage location makes it possible to create an interinstitutional structured data landscape in the healthcare sector. New processes can be implemented in this landscape without requiring separate means of access for each source of data. FHIR will be established as the overarching standard for the structuring of data in the TI. This enables the data in the TI to be addressed down to the field level. A flexible and use-case-related selection and restructuring is thus a precondition for multi-service and cross-application integration.

Distributed services

The zero trust network enables services to be supplied by various providers without requiring them to integrate themselves into proprietary networks. Access requires a reciprocally authenticated identity, the attestation of security properties and the access privileges for the requested data as stipulated by the owner and enforced by the service for this identity. Uniform interfaces enable the implementation of overarching, combined use cases from the healthcare processes.

The TI policy framework

In the federal system of the TI, uniform minimum standards are established by means of a policy. This policy framework is created in collaboration with the players responsible for the sector. Adherence to the defined legal, organizational and technical rules is enforced by gematik, which serves as a body with overarching responsibility. The policy framework encompasses the dimensions of security and data protection, interoperability, and availability. Moreover, it defines the measures that are taken to monitor the technical players and attest the participating services, clients and sites. The review of policy framework conformity is being automated.

4.3 Clear rules are needed for more players and more levels

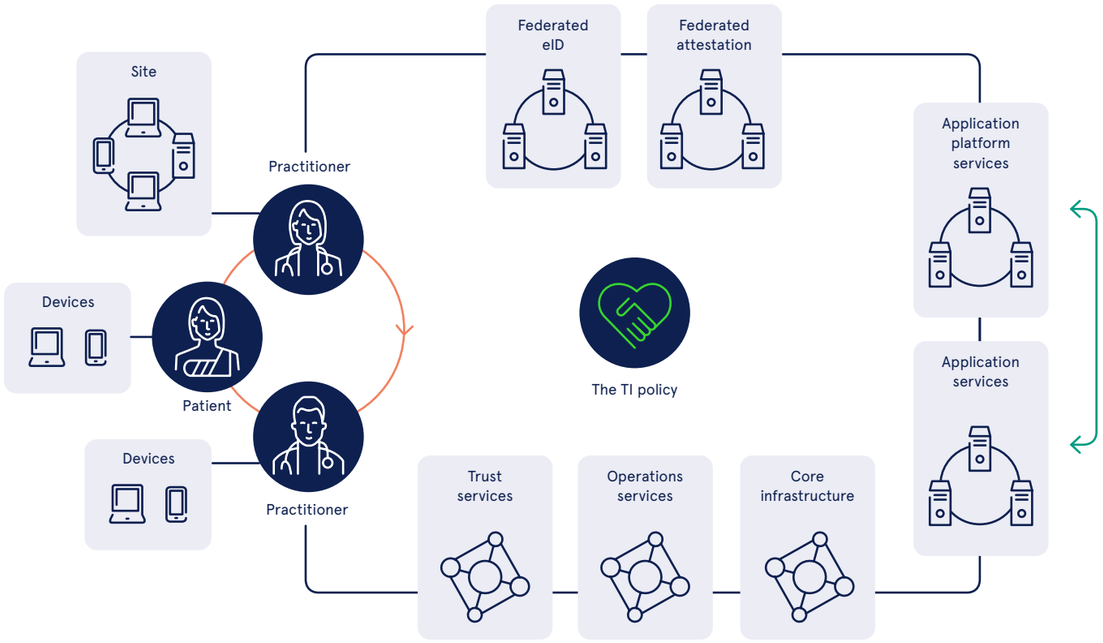
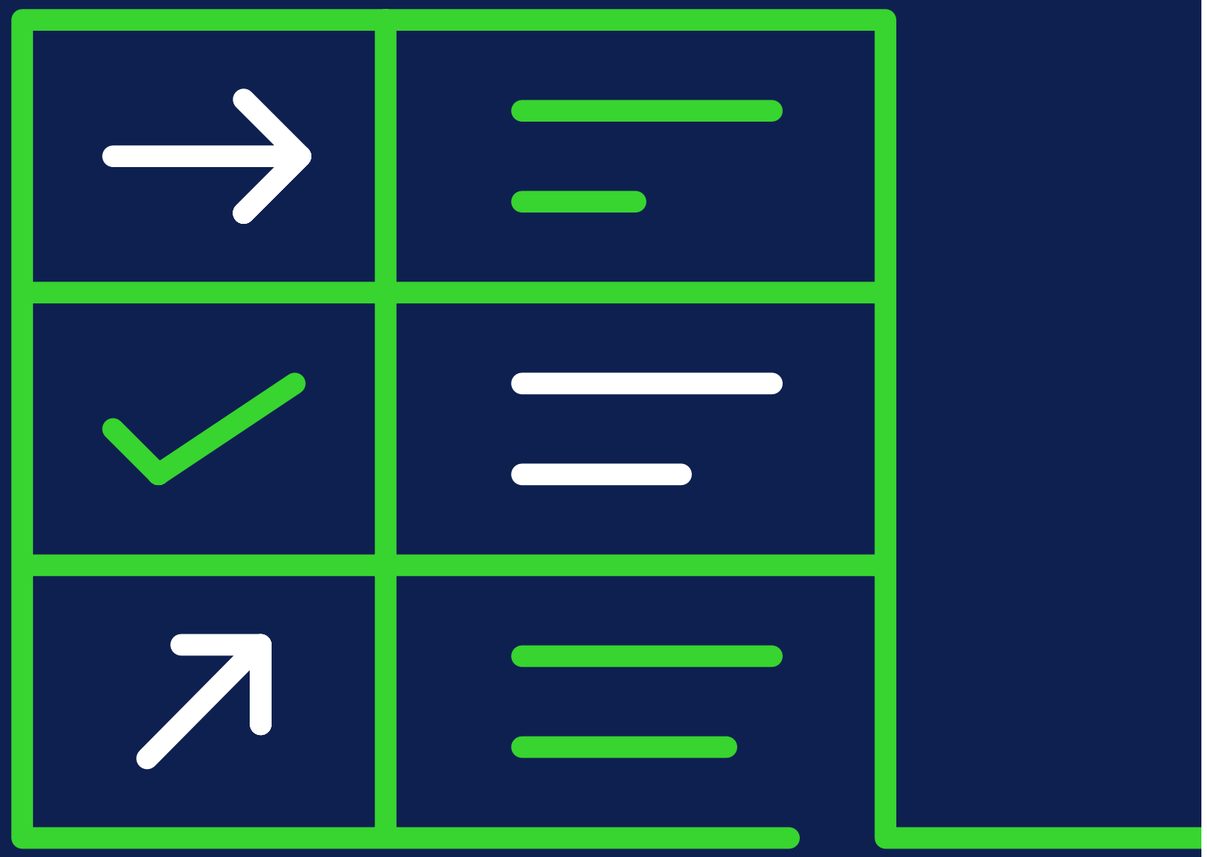


Figure 3 – Overview of the architecture of the TI 2.0

- The image shows the users (**patient, practitioner**), who use their **devices** to interact within and outside the care-provider environment (site) within the treatment context.
- During the use of the TI, the focus is on the **application services**.
- In order to access application services, users authenticate themselves at the eID service for their respective sector. In addition, locations and devices are organizationally and technically attested (**federated eID and federated attestation**).
- **Application platform services** for supporting cross-application integration or as a platform for other services and applications.
- **Trust services**, e.g. a service catalogue, which depict the integration of the players in the TI federation at the technological level.
- **Operations services** such as service and security monitoring.
- **Core infrastructure** composed of reusable, cross-application services under the operational responsibility of gematik.

5 What strategic decisions does this necessitate?



Restructuring due to changed conditions

gematik should be able to implement the security and interoperability standards that are needed for achieving trust in the TI. These standards have to be formulated for the TI as a policy. This puts gematik into the role of an approval body.

For practical reasons, gematik has to use technical means to make every player's conformity with the trust policy of the TI transparent for all of the other players. As a result, gematik takes on the role of an attestation body. The performance of this role implies the following points:

- Formalization of the policy as a data structure for processing by machine
- Attestation of the TI participants (people, components, services) to third parties in accordance with the policy.

Depending on the use case, the attestation of participants by gematik can either be done by means of direct queries at gematik or indirectly if an attestation is provided by an independent provider whom gematik judges to operate in conformity with the policy.

The implementation of the policy implies that gematik has at least one way of carrying out organized tracing and escalation in cases of policy violations by TI participants. However, the policy should be technologically implemented whenever possible so that violations can be prevented in advance.

A new approach for the critical core area of the TI

gematik's restructuring requires the introduction of a series of new services in the core region of gematik's area of responsibility. The services' continuous availability is a precondition for the functionality of all of the services from other players in the healthcare system for which it forms the basis. At the same time, gematik remains responsible for a series of existing services. All of these services have to be continuously available because they provide critical infrastructure.

In the past, the provision of critical services could not be sufficiently ensured within the scope of the previously used deployment models. As a result, while contractual regulations with the providers did not give gematik any effective means of sanctioning mistakes, gematik was held politically responsible for breakdowns.
For this reason, the restructuring of the TI is associated with a new approach to providing critical TI services in gematik's direct area of responsibility.

It is intended to provide gematik with far more direct possibilities of action to ensure the availability of critical services for the processes that are needed for the TI.

New overall picture

The restructuring will create a TI that combines two complementary approaches:

On the one hand, the federation of services and responsibilities will create the required level of flexibility in order to ensure that the TI has substantial integrative power within the overall healthcare system.

On the other, it will centralize the structures that are needed for a continuously available TI core and embed them in processes focussed on direct possibilities for action and control.

In this way, the TI will be modelled on the operational examples of well-established and successful platform providers.

User-oriented migration path to the TI 2.0

The migration to TI 2.0 will be carried out in parallel with the regular operation of the TI. The location-independent access and the new security architecture enable new services and interfaces to be created without interfering with the ongoing operation of the TI. Moreover, the system does not have to be switched over for all users on a particular date.

The underlying migration approach is to switch one application after another to the new architecture in a step-by-step process and to stagger it according to user groups. Because the new architecture requires the user groups and corresponding sectors to actively participate more than ever before, gematik wants to engage in a dialogue with the shareholders and user groups to create a migration roadmap and coordinate the migration process.

Connectors

The first connectors that were introduced during the online rollout (Stage 1) will expire beginning in mid-2022. As a result, the functions of the connectors will have to be replaced by a provisional solution during the first stage of the migration to the TI 2.0.

The top priority for gematik is to ensure interruption-free operation, especially for early users of the TI. Corresponding concepts will be discussed and implemented in cooperation with shareholders and potential industrial partners beginning in early 2021.

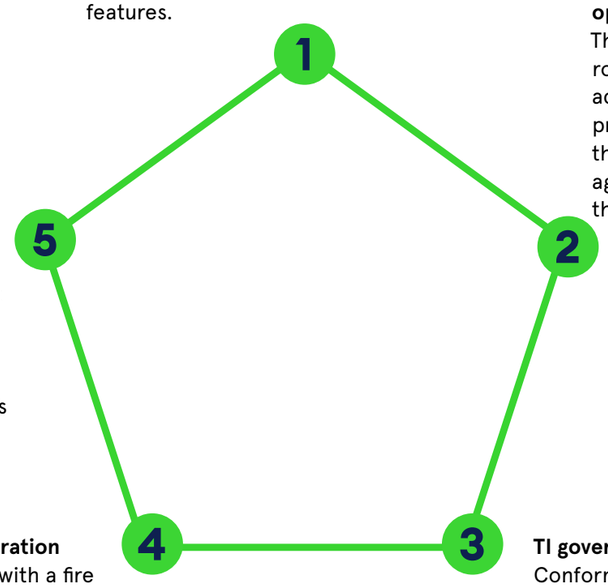
Federated components

The federated components of the TI 2.0 are being developed in close cooperation with the user groups and the sectors. In 2021 gematik will define the requirements for a federated system of electronic identities (eID system). The sectors' first eID systems are expected to go into operation in late 2021/ early 2022.

The organizational, technical and operational requirements for the attestation of the locations and devices will be specified by the end of 2021.

Five basic principles for the operation of the arena for digital health:

"Operation by design"
A product's operational aspects are taken into account during development and are put on the same level as new features.



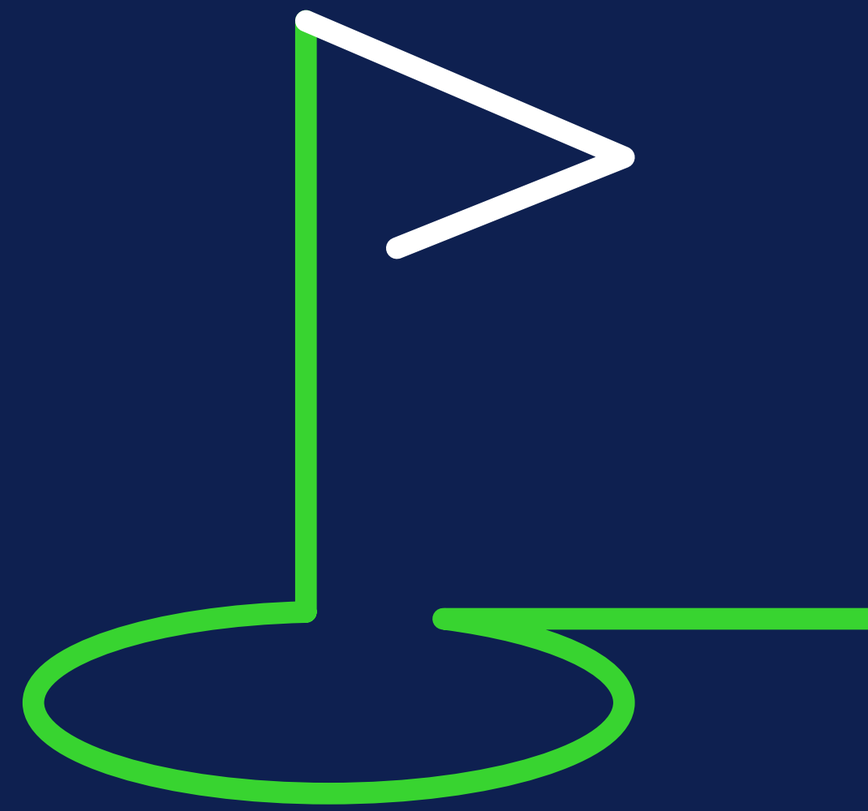
Monitoring of TI operations
The productive environment is monitored according to the logistics principle. It is not about the contents of a package, but its location and the process chain.

TI ownership
gematik is the owner as the organization that is responsible for the security services and the services that are essential to the system's operation.

Taskforce operation
As is the case with a fire brigade, drills have to be regularly conducted for the elimination of faults and risks have to be evaluated in advance.

TI governance
Conformity with regulations is checked according to auditing principles; operating regulations are created and checked on a regular basis.

6 Conclusion: How useful is this approach to a solution?



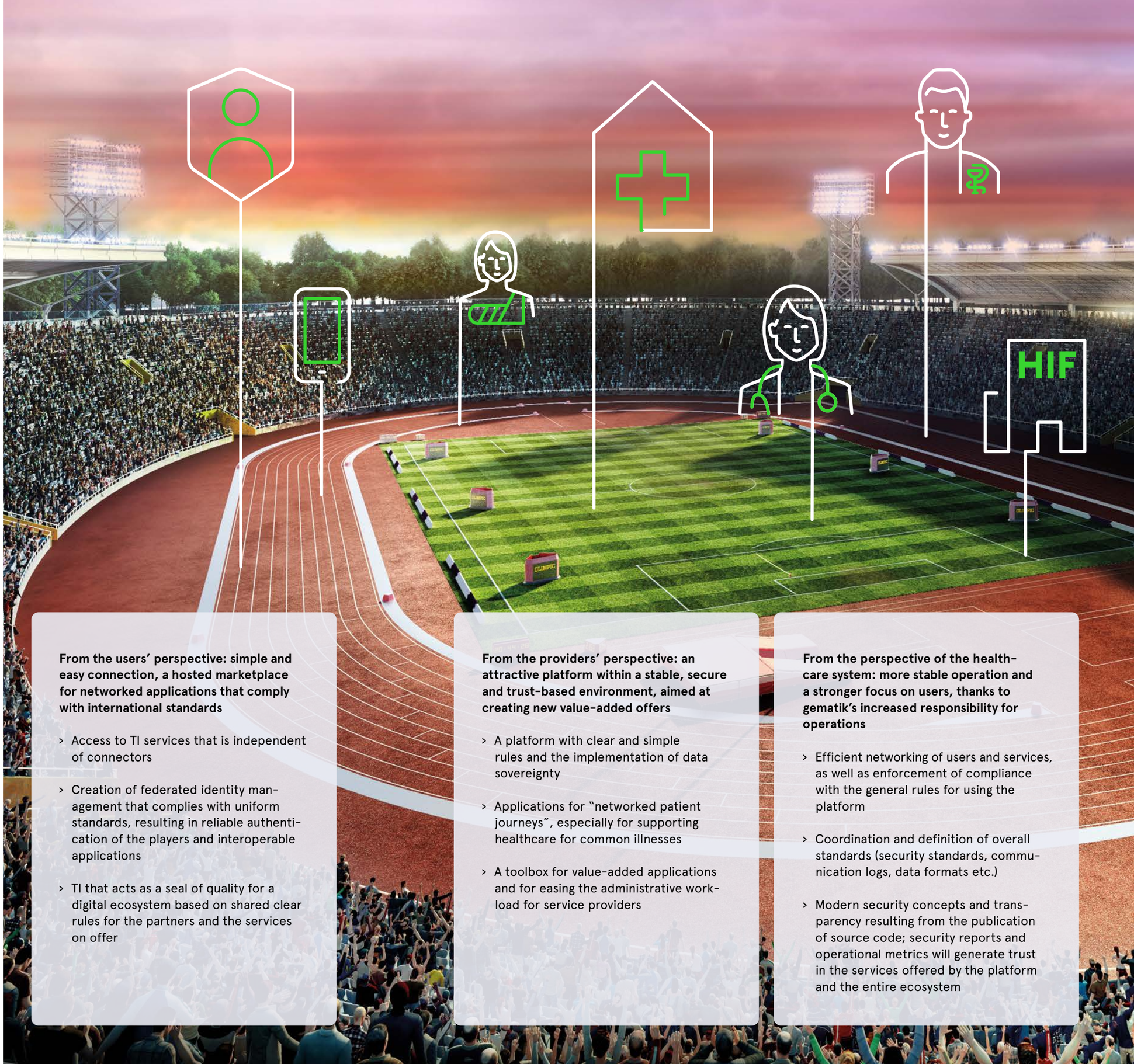
As an **arena for digital health**, the TI 2.0 will focus on user-friendliness and promote the safeguarding and improvement of health in Germany by means of a stable and secure operational process. Through its interoperable interfaces and standards, the TI 2.0 will be capable of international connection and thus well-prepared for the future. From a long-term perspective, this means it will provide sustainable and targeted support for the management of healthcare and health, as well as reducing complexity and costs.

As a platform, the TI 2.0 basically does not provide any applications. Instead, it makes possible the provision of services and enables unobstructed communication between these services and their users. The actual TI 2.0 consists of the platform itself and the services made available by third-party providers. This enables all providers to provide digital healthcare products with a proven high level of security and data protection. The users can rely on the TI 2.0 to maintain this high level. The TI 2.0 reinforces the patients' sovereignty by means of modern security concepts and access rights management.

The definition of overall standards enables unobstructed communication between the various users and services, as well as efficient cross-sector and cross-border cooperation in the area of medical care and research within the EU. On the basis of existing healthcare data, the TI 2.0 also ensures optimal patient care in other EU countries and avoids information deficits and media discontinuities. This improves the security of individual patient care.

As an **arena for digital health**, the TI 2.0 helps to improve the quality and efficiency of patient care. That's because stable, available and secure applications simplify the work processes of medical care providers and provide everyone involved in medical care with a quick and constantly accessible overview of the healthcare information they need.

Digital health will be invigorated on the basis of a platform that can grow as a digital ecosystem and generate new value added. The **arena for digital health** will lift the prediction, prevention, treatment and aftercare of illnesses, as well as the cooperation between medical healthcare practitioners and patients, to a new and better level.



From the users' perspective: simple and easy connection, a hosted marketplace for networked applications that comply with international standards

- Access to TI services that is independent of connectors
- Creation of federated identity management that complies with uniform standards, resulting in reliable authentication of the players and interoperable applications
- TI that acts as a seal of quality for a digital ecosystem based on shared clear rules for the partners and the services on offer

From the providers' perspective: an attractive platform within a stable, secure and trust-based environment, aimed at creating new value-added offers

- A platform with clear and simple rules and the implementation of data sovereignty
- Applications for "networked patient journeys", especially for supporting healthcare for common illnesses
- A toolbox for value-added applications and for easing the administrative workload for service providers

From the perspective of the healthcare system: more stable operation and a stronger focus on users, thanks to gematik's increased responsibility for operations

- Efficient networking of users and services, as well as enforcement of compliance with the general rules for using the platform
- Coordination and definition of overall standards (security standards, communication logs, data formats etc.)
- Modern security concepts and transparency resulting from the publication of source code; security reports and operational metrics will generate trust in the services offered by the platform and the entire ecosystem

Imprint

Publisher:
gematik GmbH
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 400 41-0
Fax: +49 30 400 41-111
info@gematik.de
www.gematik.de

Design:
Realgestalt, Berlin

Translation:
TransForm, Cologne

Printing:
Gallery Print, Berlin

Picture credits:
© Dmytro Aksonov via iStock, cover, page 35
© Hinterhaus Productions via Getty Images, page 5
© Geber86 via iStock, page 15
© Maskot via Getty Images, pages 22, 23
© mixetto via Getty Images, page 29

Status:
January 2021