IT-Planungsrat

Germany’s government cloud strategy
The federal approach

- Version 1.4.1 of 17th November 2020 -

11/2020

Publication data

Published by

FITKO (Federal IT Cooperation)
Zum Gottschalkhof 3
60594 Frankfurt am Main
Email: poststelle@fitko.de
Institution under public law | Dr Annette Schmidt, president

Contact

Division DG II 2 - Digital Sovereignty for Public Administration IT
Federal Ministry of the Interior, Building and Community
Postal address: Alt-Moabit 140, 10557 Berlin, Germany
Street address: Salzufer 1 (enter from Englische Straße), 10587 Berlin, Germany
Email: DGII2@bmi.bund.de
www.cio.bund.de

Version of

November 2020

Table of contents

1 Introduction

1.1 Background

The federal, state and local governments have set themselves the goal of jointly strengthening the digital sovereignty of Germany's public administration. The blueprint for this effort is a policy paper that was drafted and adopted by the IT Planning Council.[1] Based on that blueprint, the present paper, "Germany's government cloud strategy – The federal approach", was developed as one measure to strengthen the digital sovereignty of the public administration.

In the policy paper, digital sovereignty is defined as the capabilities and possibilities of individuals and institutions to perform their roles in the digital world autonomously, confidently and safely.[2] Due to the growing use of digital administrative processes, digital sovereignty is crucial for public administration at federal, state and local level. Standard information and communications technology (ICT) products, often supplied by private and commercial vendors, are widely used in public administration to perform sovereign tasks.

A strategic market analysis[3] was conducted for the Federal Government Commissioner for Information Technology (BfIT) to find out how dependent the federal administration is on software vendors. The study found concrete indications that the use of software from individual private technology vendors limit digital sovereignty.

The study identified the following problem areas: limited information security, legal uncertainty, uncontrollable costs, limited flexibility, and innovation that was beyond the federal administration's control.[4] Following this study, the federal, state and local governments drew up a policy paper defining the goal of strengthening digital sovereignty and identifying five areas of action for achieving this goal (see Figure 1).

[1] "Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung; Eckpunkte – Ziel und Handlungsfelder (Strengthening the digital sovereignty of public administration – objectives and areas of action) (Resolution of the 31st meeting of the IT Planning Council, Resolution 2020/07 and Resolution no. 2020/01 of the CIO Council).

[2] As defined in the study "Digitale Souveränität" (Digital sovereignty) conducted by the Competence Centre for Public IT (ÖFIT).

[3] Strategic market analysis to reduce dependence on individual software vendors; study commissioned by the Federal Ministry of the Interior, Building and Community, August 2019.

[4] For details of these problem areas, see the strategic market analysis to reduce dependence on individual software vendors; study commissioned by the Federal Ministry of the Interior, Building and Community, August 2019.

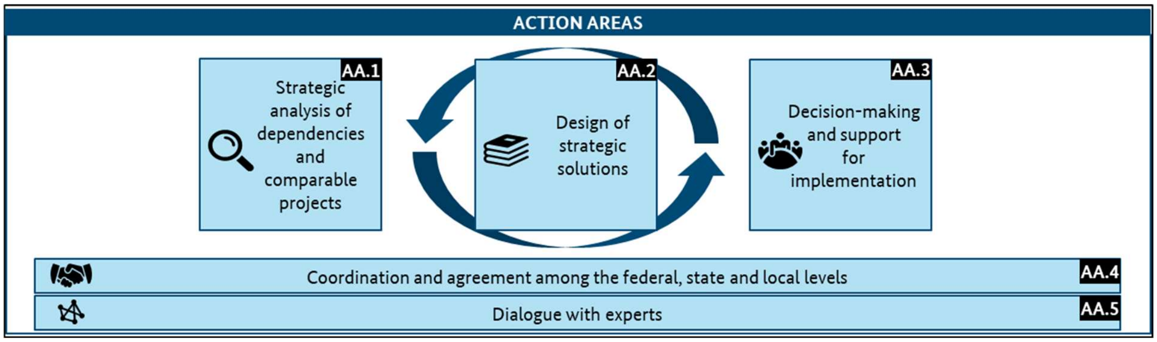

ACTION AREAS
AA.1
Strategic analysis of dependencies and comparable projects
AA.2
Design of strategic solutions
AA.3
Decision-making and support for implementation
Coordination and agreement among the federal, state and local levels
AA.4
Dialogue with experts
AA.5

Figure 1: The five areas of action identified in the policy paper

Action area 2 deals with the strategy for reducing critical problem areas and increasing independence from particular vendors. This action area covers among other things the need to standardise existing federal cloud solutions of the public administration.

The uptake of cloud solutions is a growing market trend; at the same time, a large number of clouds are already in use in the public administration at federal, state and local level. Examples of existing cloud solutions include the Federal Government's *Bundescloud*; the *Lower Saxony education cloud*; the cloud of the Mecklenburg-Western Pomerania data processing centre, *DVZ:DIGITAL*; Thuringia's *data exchange platform*; and Saxony's *cloud for secure data exchange*.

However, because individual layers of cloud stacks are not standardised, the existing clouds at the various levels of public administration are interoperable with each other only to a limited degree if at all, which makes it difficult to reuse the same applications in the different clouds (see Figure 2).

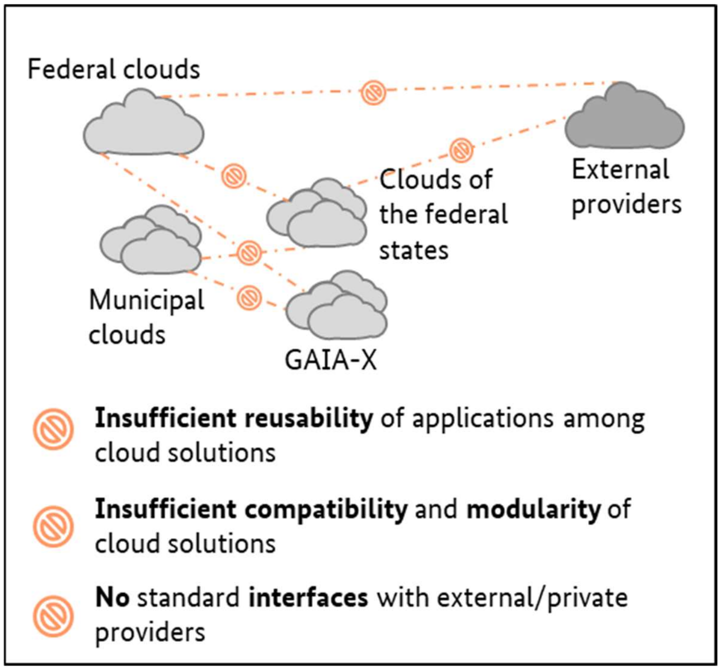

Federal clouds
External providers
Clouds of the federal states
Municipal clouds
GAIA-X
Insufficient reusability of applications among cloud solutions
Insufficient compatibility and modularity of cloud solutions
No standard interfaces with external/private providers

Figure 2: The current cloud landscape (illustrative)

It is therefore necessary to define common standards for existing and future cloud solutions at federal, state and local level. To do so, the necessary layers of cloud stacks which can be considered for standardisation must first be identified.

After the first presentation of the strategy for standardising clouds at all levels of public administration, the IT Planning Council, in its Decision 2020/08 of 25 March 2020, called on the working group on cloud computing and digital sovereignty to flesh out this strategy further and define the necessary standards. The present paper addresses the IT Planning Council's call and further develops the strategy.

At its meeting this summer, in addition to expanding the existing working group on cloud computing and digital sovereignty, which operates at ministerial level, the IT Planning Council also decided to create three subgroups focused on the following subjects: procurement; communication; and technology and operations.

After the present paper was adopted by the IT Planning Council, the subgroup on technology and operations began developing Germany's government cloud strategy further, drafting recommendations based on this paper for specifying the requirements for all areas of standardisation in the form of a target architecture. The recommendations are being drafted in consultation with the subgroups on procurement and communication.

1.2 Motivation

While private cloud infrastructures continue to be set up within the public administration at all levels, the use of these technologies requires both agreement on technical standards and changes to the processes of software development and provision. A common approach should therefore also jointly undertake the necessary changes to the process landscape, with attention to local conditions, and create compatibility among different cloud solutions. **In the following, the strategy for establishing and applying standards for existing cloud solutions at all levels of the public administration will be referred to as Germany's government cloud strategy.**

Common technical and strategic requirements can enable the technical reusability of applications, avoid dependence on individual cloud solutions (especially those from major hyperscalers), and increase the shared market power of public administration, thereby significantly helping to strengthen digital sovereignty.

The present document describes the strategic objectives of Germany's government cloud strategy and the different levels of standardisation based on the layers of cloud stacks It also deals with the strategic requirements to be addressed in implementation.

1.3 Clarification

This document contains neither technical specifications nor standards for software systems (specialised IT applications or software as a service (SaaS)), nor does it address the use of public cloud services.

Fundamental requirements for internal and external service providers with regard to privacy, operational security, data storage, etc. will be specified in a separate document.

2 Strategic objectives and vision

2.1 Strategic objectives

To strengthen digital sovereignty, public administration at federal, state and local level is pursuing the following objectives, among others:[5]

1. **Reducing dependencies**
    a. Strong negotiating position thanks to critical market power
    b. Interoperability and interchangeability of public administration IT infrastructures
2. **Increasing efficiency and effectiveness in development, implementation and operation**
    a. IT infrastructures ready for the future
    b. Scalable IT infrastructures
    c. Developed solutions that are easy to reuse
    d. Standardised implementation and operation
    e. Existing services and applications of other operators that can be jointly used[6]
    f. High level of availability of IT infrastructures (including resilience)
3. **Ensuring and strengthening privacy and information security**
    Implementation of the relevant requirements and regulations, to be ensured in particular through privacy by design and security by design
4. **Optimising data exchange, shared storage and use by federal, state and local public administration**[7]

Germany's government cloud strategy addresses the objectives listed here by promoting possibilities to choose and switch vendors/providers, ensuring design capability and enabling influence on vendors. Common standards and interfaces also support compatibility between existing and future cloud infrastructures at all levels of public administration.

The federal, state and local levels must work together if these objectives are to be achieved.

[5] See "Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung; Eckpunkte – Ziel und Handlungsfelder (Strengthening the digital sovereignty of public administration – objectives and areas of action).

[6] Requires appropriate network gateways. However, these are not the subject of this paper.

[7] Legal framework and requirements (such as licensing conditions, privacy, IT baseline protection) must be taken into account. Germany's government cloud strategy only creates the technical prerequisites.

2.2 Vision and approaches to implementation

Germany's government cloud strategy calls for standardising cloud solutions at every level of public administration so that these solutions can be connected to each other. This standardisation is to cover key areas of the layers of cloud stacks, from development to implementation and the operation of applications. For this reason, five areas were defined:

1. **Development and development platform:** standardised platforms, processes and architecture requirements for developing applications

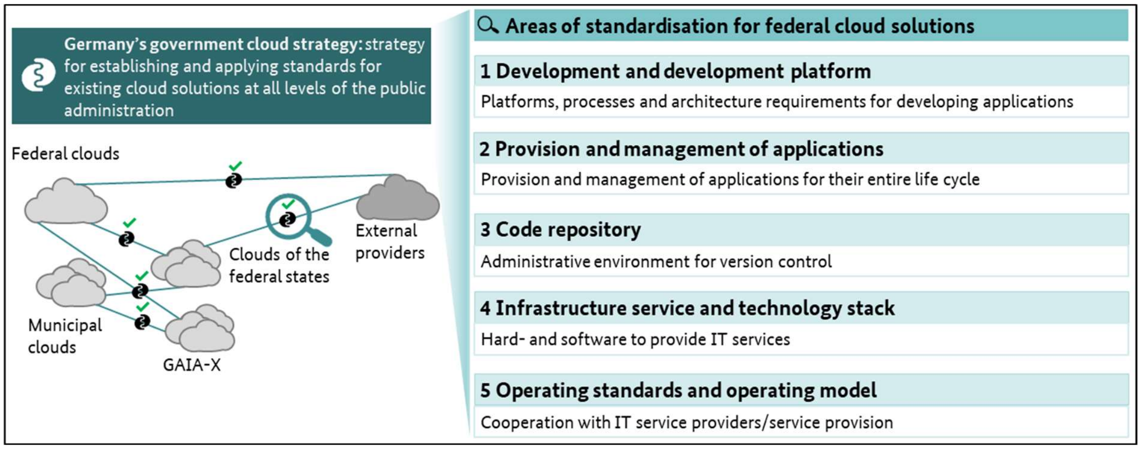
2. **Provision and management of applications:** standardised provision and management of applications for their entire life cycle

3. **Code repository:** standardised administrative environments for version control and central copies and/or storage of distributed source code and documentation

4. **Infrastructure service and technology stack:** definition of standards for the hard- and software components used to provide IT services

5. **Operating standards and operating model:** harmonised cooperation with IT service providers and service provision

Figure 3 illustrates this vision and shows the areas to be standardised.



Germany's government cloud strategy: strategy for establishing and applying standards for existing cloud solutions at all levels of the public administration

Areas of standardisation for federal cloud solutions

1 Development and development platform
Platforms, processes and architecture requirements for developing applications

2 Provision and management of applications
Provision and management of applications for their entire life cycle

3 Code repository
Administrative environment for version control

4 Infrastructure service and technology stack
Hard- and software to provide IT services

5 Operating standards and operating model
Cooperation with IT service providers/service provision

Figure 3: Vision of interconnected existing cloud solutions

The focus is on standardising the five areas of cloud solutions, so that federal, state and local public administration, among other things

- can be sure, when using one or more clouds at different levels of public administration, that data processing is transparent (standards for infrastructure service and technology stack as well as operating standards and operating model) and complies with data protection law (including on the handling of personal data);
- can adopt, operate and reuse applications from other public administrations at federal, state or local level within their own clouds (technically) without licence restrictions (standards for development and development platform);
- can offer their own public administration and citizens applications from other federal, state or local clouds (standards for provision and management of applications).

3 General requirements

Germany's government cloud strategy identifies five areas to be standardised. The requirements described below influence the five areas of standardisation in general and should be taken into account during implementation:

1. The standards must be adopted by public administration at every level and must be consistently applied.
2. The standards must correspond to the IT baseline protection (*IT-Grundschutz*) of the Federal Office for Information Security (BSI)[8] in the protection categories "normal" and "high".
3. The software architecture of cloud infrastructure should ideally be based on open-source software which is not subject to technical or legal limits on use.
4. The creation and use of modular (cloud) architecture with open interfaces[9] which enable automation throughout the entire life cycle of the application are promoted.
5. The individual public administration clouds to be standardised are operated by the public IT service providers at federal, state and local level within their secure environments as in a private cloud.
6. The standards also take into account connections to public cloud solutions and edge computing.
7. Solutions that have been developed can be reused in different contexts and by different operators within the public administration without modifying code ("Build once, run anywhere").
8. Cloud architecture should pay attention to use within a modern, mobile environment.
9. Data processing is transparent and understandable for users. Data flows and transfers, in particular to external IT systems, are comprehensibly documented, easily monitored and able to be inspected as needed.
10. Service portfolios are made up of basic services and can be expanded to include additional services and possibly also billing procedures. At a later stage, it should be possible to select

[8] ISO Standard 27001 based on IT baseline protection.

[9] Examples of processes with interfaces include deployment, resource requirements, billing, monitoring and logging.

individual services from the portfolio, as in a shop, in order to create a custom context for a particular procedure.

Additional requirements in the five areas (development and development platform, provision and management of applications, code repository, infrastructure service and technology stack, operating standards and operating model) can be found in the accompanying document “Germany’s government cloud strategy: Annex 1”.

4 Annex

4.1 Glossary

For a detailed description of various technical terms, please see the BSI publication “Digitale Gesellschaft - Cloud Computing Grundlagen” (Digital society - Fundamentals of cloud computing; in German).[10]

- edge computing: distributed data processing at the margins of a network instead of a data centre.
- hybrid cloud: multiple autonomous cloud infrastructures used in common via standardised interfaces.
- private cloud: cloud infrastructure which serves only one institution. It may be organised and run by the institution itself or by a third party; it may be located in the institution’s own data centre or in that of a separate institution.
- public cloud: services are offered by a single provider and may be used by the general public or a large group, such as an entire industry.
- software as a service (SaaS): applications which meet the criteria for cloud computing, such as word processing, spreadsheets and collaborative applications.
- software development: design and standardised implementation of software projects and associated processes.

[10] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html (retrieved 26 September 2020)

4.2 List of abbreviations

Abbreviation	English equivalent
BfIT	Federal Government Commissioner for Information Technology
BSI	Federal Office for Information Security
ÖFIT	Competence Centre for Public IT
SaaS	software as a service