Karlsruher Institut für Technologie

Cloud Services – Trust, Operation, Usecase (Examples: Sync&Share, IaaS)

HIFIS – Conference 17./18.2019, Klaus Scheibenberger (KIT/SCC)

STEINBUCH CENTRE FOR COMPUTING – SCC

Terms: Cloud Services, Service Provider

- „Cloud service“ as it is used here, addresses actual more or less „federated services“.
  - (For an exemplary definition of cloud computing characteristics see NIST: NIST Computer Security Division (CSD): NIST SP 800-145, The NIST, Definition of Cloud Computing, S.6)
- „Service Provider“ one finds on different abstraction layers:
  - May mean a technical instance of a service (e.g. SP in SAML).
  - May also mean the organization which operates and provides a service.

- **Goal of this talk**: To point out relevant aspects to work on regarding future HIFIS Cloud Services, especially the „Survey of Cloud Services“, considering:
  - We (KIT/SCC) have gained experience with some questions regarding some (federated) services (bwSync&Share, bwCloud) over some years.
  - But of course (as anyone knows) therefrom no „golden solution“ for HFIS can be derived!

(Cloud/Fed.) Services: A lot about policies too

- For a (cloud) service all involved parties – provider (organizations) and users (user organizations) – they need reliable relationships.
- Therefore someone has to deal with (some examples):
  - Certificates for machines (IT security; „IT-infrastructure“).
  - Digital identities for humans and reliable user-related attributes for services (identification, authentication, authorization; „AAI“).
  - Agreements about processes (**may differ for each service**), all involved parties commit themselves to (reliability; „Trust“).
- And thus one talk actual also on the service level a lot about policies.

- Usage of Google, Facebook & Co. is also built upon policies:
  - Every single end-user agrees to / „signs“ (but seldom reads) the „user **contracts**“ with these companies - the policies (rights an duties) are defined in the „small print“.

Relation: Service – AAI
Example: bwSync&Share – bwIDM

- The service *bwSync&Share* (start 2014) for educational institutions (universities, colleges) within Baden-Württemberg (and the DFN-Cloud) **relies on** the bwIDM-federation (AAI, subset of the DFN-AAI):
  - In the bwIDM-background: Signed(!) agreements (2012) with many of such institutions about operating IdPs, delivering reliable attributes.
    - Organizations (their IdPs) are the structural elements in a federation
  - As we actually talk roughly about 50 organizations with overall about 40.000 accounts we regard the „federation of identities“ as one of bwIDM‘s central benefits.
  - This means: The responsibility for „correct“ digital identities (correct mapping to persons, handling of changes, …) as well the decision which persons within an institution are allowed to use the service (“entitlements”, access), **are delegated** to the institutions themselves.
- Such „bwIDM-institutions“ taking part in this federation may use *bwSync&Share* but under additional service policies, additional to the “bwIDM-related” policies.
  - The institution here as the user’s representative.

Relation: Service – Users
Additional policies (evolution)

- Aspects to be considered additional may be:
  - User categories, capacity, support, deprovisioning of accounts (e.g. access rights) and data, (contribution of) **costs,** reasons for dismissal, notice periods, data protection/privacy (DSGVO, AVV/ADV), et al.
- One aspect in particular (exemplary):
  - As long as the service was operated as a project sponsored by the MWK one could focus on technical issues on basis of a „contract light“, as especially the **financial** question – how to distribute costs (e.g. support costs for the software) – was masked by the sponsoring.
- As we want to continue this service after the end of the project (end of 2019) we had to find a financial model (policy):
  - Coarse grained: We decided on a flat rate model (easy to “implement” but of course needs coordination; “political”, not technical).
  - Thus we generated with the KIT‘s legal office a „**Contract** for usage and ADV for bwSync&Share“ to define aspects mentioned above (not only the financial) and thus getting signed(!) **agreements with institutions**
  - Signed from both partners: service provider and institution (user).

Use case: Sync&Share for HMC

- HMC will deliver a „Metadata Collaboration Platform“ for research data management all over the HGF (see https://www.helmholtz.de/forschung/information-data-science/helmholtz-metadata-collaboration-plattform-hmc/)
- Coarse grained: Communities will connect their domain specific portals to this platform to register their projects for to deliver project related research data (e.g. proposals) with its metadata to be published there.

- Idea: To enhance the acceptability of the platform‘s usage the data may be in the first instance held in a HGF-wide Sync&Share service.
  - Thus the projects can work on the material autonomously (in their „own structure“) and deliver only the final results into the HMC platform.

„Agreements (= policies) may differ for each service“

- This statement takes into account that already the **operation model** of services may be quite different, or the contribution of costs , or …

- Again two federated services as an example, both based on bwIDM:
  - *bwSync&Share* is operated concentrated only at the KIT but provided country-wide.
  - *bwCloud* (provides IaaS-functionality) is operated distributed on different infrastructures located at four universities (Freiburg, Karlsruhe, Mannheim, Ulm), but is also provided country-wide as one service (e.g. one registration process, one financial model).

Different Operation Models (examples)

- Concentrated Model:
  - Different Sync&Share software (e.g. Powerfolder, Nextcloud, …) running at the core of the service have „more or less“ a defined standard functionality.
  - More instances don‘t bring essential more functionality to the users.
  - Concentrating the service provisioning on one single provider may release others from this effort (not doing the same thing twice, tree times, …).
- Distributed Model:
  - Providing computing and storage Infrastructure resources from different IT-infrastructures and providers, but as an **integrated** service (e.g. one common registration procedure, common financial model).
  - This still permits variances to each provider: They can for example specialize „their part“ regarding their specific conditions (e.g. focussing more on IaaS, PaaS, SaaS), thus addressing different user communities for this service.
- Marketplace Model:
  - The IaaS example from above may also be operated as a „marketplace“ of different IaaS services (with different registration, financial, … models).
  - (Clear: May hold for the Sync&Share example as well).

IaaS (bwCloud): Resources for „different communities“

- Running a compute and storage infrastructure as IaaS means to abstract from hardware, systems and provide resources/resource pools to users.
- Dealing with different communities organized in different AAI-contexts (bwIDM „HGF-AAI“, …) using resources on the same infrastructure generate further questions.
  - Beneath (“simple”) resource management and scalability also questions about (again) different polcies, or as well data privacy and IT security.

To sum up – ToDos?

- The topic service access/usage policies shows up to be crucial/critical.
- Use cases as the HMC example generate interesting questions regarding e.g. user categories (projects) as well as connectivity between services, etc.
- Operation and financial models have to be regarded and may differ for each HIFIS cloud service.

- Idea for next step (ToDo): Regarding ONE service
  - Already existing providers for Sync&Share services (e.g. on Nextcloud) may **together** work on above issues to provide this service (first of all) on basis of a HGF-AAI (“low hanging fruit”)?

Karlsruher Institut für Technologie

Thank You For Your Attention!

STEINBUCH CENTRE FOR COMPUTING – SCC