Base Technology Projects

The "Base Technology Development" cluster consists of five applications-neutral research projects. The planned technologies form the basis for secure and legally compliant cloud computing solutions operations in Germany.

The technologies enable a confidential, secure and reliable development of cloud-based communications and transaction processes. These new technological developments serve as the base innovations developed and tested within the framework of the Trusted Cloud program. These should serve as the future tested, recognized and standardized base technologies for cloud computing.

- MIA - Cloud-based Information and Analyses Marketplace
- MimoSecco - Cloud Middleware for Mobile and Secure Cloud Computing
- Sealed Cloud - Secure Cloud Computing for Business-Critical Applications
- SkIDentity - Trustworthy Identities for the Cloud
- Value4Cloud

MIA - Cloud-based Information and Analyses Marketplace

The German-speaking web's six billion-plus websites provide extraordinary potential for applications ("apps") in all number of areas including, for example, market and trend research, sale of news information, speech processing and the general area of "business intelligence" (e.g. corporate management).

As part of the "MIA - Marketplace for Information and Analyses" project, a consortium made up of industry and research partners led by the Database Systems and Information Management (DIMA) research group of the Technical University Berlin is developing a prototype information marketplace for Germany.

The goal of the project is to market, sell and refine data and value-added services through the creation of a marketplace infrastructure. Cloud computing results and fundamental research obtained and carried out within the framework of the THESEUS project (e.g. ALEXANDRIA) and the German Research Foundation (DFG) "Stratosphere - Information Management in the Cloud" research group are transferred and adapted to realize MIA objectives.

MimoSecco - Cloud Middleware for Mobile and Secure Cloud Computing

The blurring of the boundaries between different communications networks (.e.g. mobile phone, internet etc.) and the increased networking inside and between companies make information and service mobility imperative. However, access and integration of data must be both reliable and secure.

Companies who outsource their data to software-as-a-service (SaaS) providers, for example, must be sure that the cloud-stored data is not misused. This creates new security requirements which can only be safeguarded through new concepts. On first sight, the protection from use of data on mobile devices and the integration of services in cloud computing are very separate issues. However, closer inspection shows that the concepts for solving both problems are very similar if not identical.

The MimoSecco project is concerned with the conception and development of a complete technical architecture which increases the security of mobile data processing in the cloud. Central to this is the development of a flexible “middleware” solution which guarantees the data management security through different SaaS providers and implements a

reliable rights management system. The MimoSecco solution will be conceived in such a way that it is not only optimal for use in SME environments but also strengthens business confidence in using cloud-based services.

Insider attacks represent a significant threat to cloud providers in particular. This problem is further complicated by the fact that a number of new services are the result of bundled multiple third party provider services. MimoSecco will ensure security by providing, for example, remote encrypted connection between a mobile device and an enterprise server (or the communication connection of a service with another within a physical execution environment).

So-called "hardware tokens" available on certified security hardware are used as a "trust anchor." These are special smart cards protected against physical attacks which are available in a number of forms according to end-device usage (e.g. SD cards, USB sticks and PCI cards). They form the basis for role-dependent models for data access control according to a need-to-know principle as well as encrypted rights management.

Inexpensive security solutions for mobile business applications can thus be made available, with remote accessing of data in the company or the cloud from mobile devices and services becoming possible. Project results will be demonstrated according to two applications scenarios ("Consulting" and "Sophisticated Technical Customer Services").

Sealed Cloud - Secure Cloud Computing for Business-Critical Applications

Cloud solutions to date have required the presence of a trusted cloud provider. Concerns regarding the security of business-critical data represent the decisive inhibition threshold for the deployment of cloud computing in the business and public sectors. This negatively impacts on the acceptance of software as a service (SaaS) for business-critical applications.

Sealed Cloud creates a "sealed" infrastructure for cloud computing which eliminates the risk of intentional or unintentional misuse of data. It uses a system of technical security precautions which act in combination across the complete processing chain to create a new “operator safe” security level.

The Sealed Cloud benefits will be established in two commercially relevant SaaS solutions:

- deleGate: Simplifies company control of web-based services accounts
- ID|GARD solves the problem of protection of the private sphere online

Sealed Cloud will - through a combination of open source, open concept and focus on market standards - reach a high level of transparency and general applicability.

Sealed Cloud is an ideal solution for all sensitive data applications. Large companies often build their own private clouds exactly for this purpose - a luxury that many small and medium-sized businesses simply cannot afford. Sealed Cloud allows these companies to make use of the advantages of the "public cloud" in an efficient and confident manner.

Sealed Cloud and the applications used there will be tested and verified by a broad group of end-users at their own cost.

SkIDentity - Trustworthy Identities for the Cloud

The aim of the SkIDentity project is to build a sustainable bridge between secure electronic identity cards (e-ID) and existing and developing cloud infrastructures. This will allow trusted identities to be made available for the cloud and complete process and value chains to be securely created.

Existing components, services and trust infrastructures will be integrated into the cloud and evaluated in pilot projects as part of a comprehensive, legally compliant, economically viable and secure identity infrastructure.

Particular focus will be placed on the needs and requirements of small and medium-sized businesses and public service authorities. The SkIDentity infrastructure contains, for example, an e-ID Broker which bundles all of the necessary e-ID services on the e-ID card in a form best suited to smaller businesses and local authorities.

Value4Cloud

Market-supporting value added services promoting legal conformity, quality and use of cloud services among the "Mittelstand"

The objective of Value4Cloud is the research and development of market-supporting value-added services for the promotion of trust, legal compliance, quality, and use of cloud services.

The integration of value-added services in existing marketplaces and information portals addresses users and service providers from the German “Mittelstand” and makes tools to reduce technical, organizational and legal barriers available.

Academic partners and companies in economic and law and business informatics are developing following market-supporting value-added services:

- Structured information
  Standardized service description, categorization of cloud services and case studies.
- Quality evaluation
  Quality evaluation of cloud services by users and third parties.
- Benchmarking
  Comparative overview of cloud services (scope of services, legal compliance and service quality.
- Trust support
  Supporting reputation and transparent-based services.

Value4Cloud services with provider focus:

- Legal compatibility
  Design proposal for developing compatible cloud services (specifically data protection and liability law).
- Open service innovation
  Clients, external partners and suppliers are integrated into the supplier innovation process.

The transfer concept is also an important component of Value4Cloud in order to disseminate previously generated results. As well as the implementation and piloting of the value-added services developed, business, service and operator models for market-supporting value-added services will also be developed. The results are also fed back into partner information portals, certification products and SME-based cloud services

Contact Us

Oliver Wilken

+49 30 200 099 306

Submit your question

Promoted by Federal Ministry for Economic Affairs and Energy in accordance with a German Parliament resolution.