ICEMAN: An Architecture for Secure Federated Inter-Cloud Identity Management

Gabi Dreo*, Mario Golling*, Wolfgang Hommel† and Frank Tietze*
*Universität der Bundeswehr München,
Munich Network Management Team, 85577 Neubiberg, Germany
Email: {gabi.dreo, mario.golling, frank.tietze}@unibw.de
† Leibniz Supercomputing Centre,
Munich Network Management Team, 85748 Garching, Germany
Email: wolfgang.hommel@lrz.de

***Abstract*—Similar as the Internet is the network of networks, the evolution from Clouds towards the Inter-Cloud, a global cloud of clouds, represents a huge developmental leap for cloud computing, enabling the development of new innovative value-added services. One of the challenges in the field of Inter-Cloud is Identity Management. Up to now, no concepts have been developed that consider the characteristics of Inter-Clouds as well as the needs and rights of the users. Therefore, ICEMAN (Inter-Cloud Identity Management) aims to develop technical and organizational solutions for secure Federated Inter-Cloud Identity Management.**

This paper shows the work in progress on this specific aspect introducing a realistic scenario (Inter-Cloud Services used in a disastrous event), giving an overview on the subject, identifying key issues of Federated Identity Management and presenting an outlook on further research.

***Index Terms*—identity management, access management, IT security architecture, trusted federated information sharing**

I. Introduction

New opportunities in cloud computing go hand in hand with new challenges [1]. For about ten years, the term *Federated Identity Management (FIM)* is referred as methods and protocols designed to replace user and authorization information across organizational boundaries. All these approaches, however, are based on the assumption of a data exchange between exactly two organizations one Identity Provider (IP) and one Service Provider (SP) ($1:1$ *relationship*).

Particularly in the area of Inter-Community Clouds, this type of relationship is not given. Here, according to the NIST definition [2], the infrastructure will be provided by one or more companies for a common purpose and may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them [2] (thus, usually $m:n$ *relationship*).

So far, no concepts for Inter-Cloud-wide Identity Management have been developed which are able to cope with both (i) the characteristics of Inter-Clouds (internal composition of several organizations that can act as IP as well as SP) and (ii) the needs and rights of users (eg user-friendly single sign-on, trust management and privacy).

Therefore, *ICEMAN* (Inter Cloud Identity Management) will develop technical and organizational solutions for secure federated Inter-Cloud Identity Management. *ICEMAN* not only considers technical aspects such as the need for an integration into existing IT infrastructures, data conversion between clouds and cloud-wide Key Management, which can be adapted to the security requirements of specific Clouds and Services, but in particular also organizational processes. Among other things, this includes the design of an Inter-Cloud Identity lifecycle, which spans from the automated on-demand creation of accounts to the corresponding deprovisioning. Furthermore, the integration of multi-tenancy as well as delegation concepts and the link to IT service management processes such as access management, incident management and security reporting is considered.

The paper is structured as follows: Section II provides a complex scenario of Inter-Cloud Services used in a disastrous event as a basis for the corresponding requirements presented in Section III. Section IV provides information on state of the art architectures for Identity Management whereas Section V introduces the authors approach to a Secure Federated Inter-Cloud Identity Management. The paper ends with an conclusion to the intended approach and an outlook on coming research in Section VI.

II. Scenario

Accessing all kinds of data anytime and anywhere in a secure way becomes more and more important these days. Nevertheless most enterprises hesitate to store and provide relevant data beyond their own infrastructure (including private clouds) due to the risk of unauthorized access and manipulation. This way new outstanding Inter-Cloud Services aggregating data from different enterprises / providers for the benefit of many won't be possible unless major aspects of security get addressed satisfactorily. The need to securely access different kinds of data from different organizations and thereby the need for a Federated Identity and Key Management is to be shown at the example of a disastrous event like an massive explosion, a conflagration or a traffic pileup. As Federated Identity and Key Management is used by other Inter-Cloud Services, it is provided as a service with the use of an Inter-Cloud Middleware (Identity Management as a Service - IdM as a Service).

978-3-901882-50-0 ©2013 IFIP

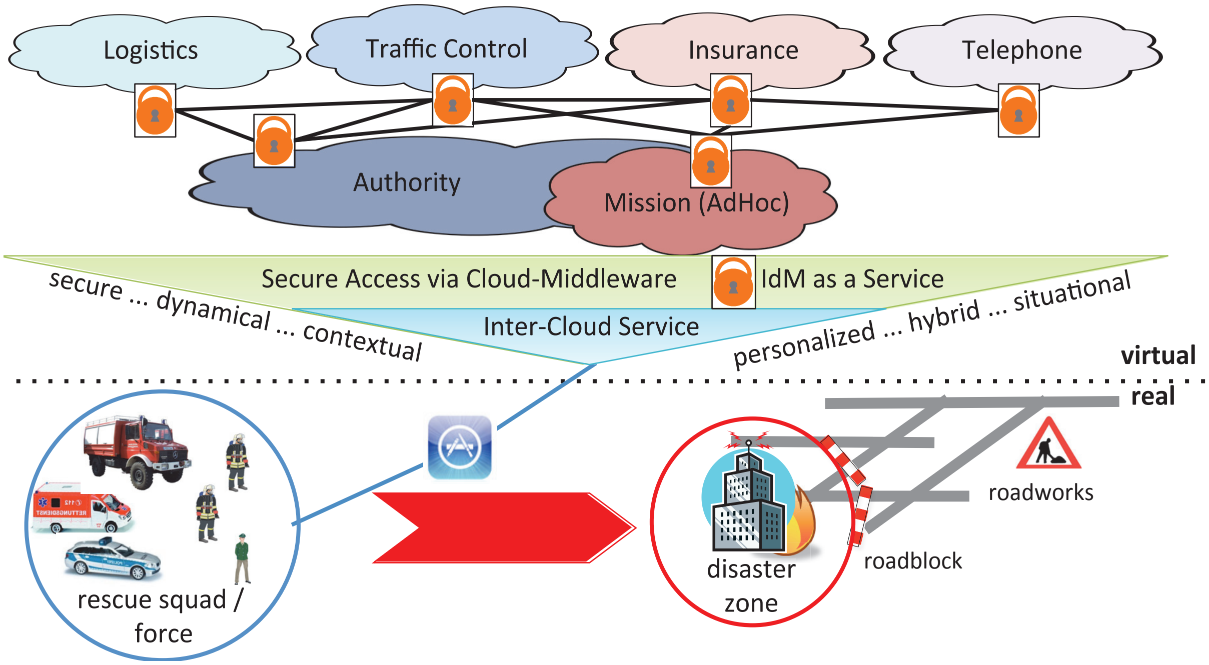

Fig. 1. Accessing data in different clouds via Inter-Cloud-Middleware

At a disastrous event the quick and reliable coordination of rescue and support forces as well as technical consultants and authorities representatives is essential. This can only be carried out satisfactorily by ensuring secure communication and providing secure access to data in a variety of Community Clouds e.g. Insurance Cloud, Authority Cloud, Logistics Cloud and others; each of which implementing their own Identity Provider, access management and role concepts. In case of a conflagration a firefighter, with his own identity and access authorization in the corresponding Mission Cloud, must be able to securely access data within the Authority Cloud to identify zoning maps, building layouts or to get information on disabled people living close to the event. Furthermore access to the Insurance Cloud for evaluation of dangerous goods within the building / block needs to be granted. Police officers as well as paramedics and doctors need secure access to the Traffic Control Cloud for getting data on traffic jams and rescue roads as well as a lot of other information. Furthermore access grants need to be context sensitive. In case of live and death a paramedic may be granted access to personal medical data of a victim but only for a short period of time or depending on the victims medical status. In this complex scenario, as shown in Figure 1, the flexible, fast, easy and secure granting and revoking of rights and permissions for a great number of participants is essential. The major challenges are verification of identities and corresponding people, evaluation of trust and trustworthy requests and prevention of data loss as well as unauthorized access.

III. Requirements

For the realization of Inter-Cloud-based services with a great number of data and computing providers, answers to many challenges and problems have to be found. In the area of Identity Management for Inter-Clouds, this particularly includes:

- **Exchange of identity information:** The used dichotomy (1 Identity Provider, 1 Service Provider) in Federated Identity Management (FIM) for identity provisioning and usage across enterprise boundaries, as depicted in Figure 1, may be of very limited value only, as in the case of Inter-Clouds - both - multiple Identity Provider, as well as a number of Service Providers, can be present.
  In this context, e.g. the following questions need to be addressed: What specific information about users, apps / devices, etc. need to be exchanged over the boundaries of a community cloud? What difficulties are there; for example different protocols, data formats, etc.? How do existing identities enter the Inter-Cloud? What does the provision of such technical and organizational inventory data imply (data protection, etc.)?
- **Managing permissions:** The exchange of identities is closely linked with managing permissions. Why do some identities have different permissions in different clouds? Is there a need for extending conventional authorization models, such as role-based access control, or a mapping of permissions between Clouds?
- **Dynamic extensibility:** Dynamic extensibility represents another challenge. It must be possible to perform adaptations to changing internal or external circumstances, and to add additional features as well. In this regard,

the following questions must be answered superficially (among other things): How can a dynamic extensibility with new Cloud services be ensured? How can a user determine whether such a new service is trustworthy? What are the guarantees that the user data is kept up to date and not simply provided on-demand and (when exactly, in which context?) can it be deleted? How can the compliance with these procedures be monitored by means of indicators / metrics and assessed?

IV. Overview of State of the Art Architectures

In this section we give a short overview of activities and results of standardization bodies, academic research, and projects that are relevant for ICEMAN. For a more comprehensive overview please also take a look at [1].

The ICEMAN approach attempts to leverage and integrate suitable existing Federated Identity and cloud Management standards in order to foster quick service adoption. Boards and bodies such as OASIS, the Kantara initiative, and the Cloud Security Alliance have elaborated on the necessity of Identity Management in and for cloud environments. The Trusted Cloud Initiative and the Open Identity Exchange Initiative also focus on Identity and Access Management in the context of cloud computing. However, they have not yet been adapted to Inter-Cloud scenarios.

While standardization bodies focus on the enterprise perspective, academic research vividly discusses privacy issues from the users' perspective. Bertino et al. [3] and Huang et al. [4] provide an insight into the requirements regarding privacy in clouds. Celesti et al. specify a reference architecture for Identity Management in Inter-Clouds [5]; the exchange of identity data is based on a new Security Assertion Markup Language (SAML) profile. While this research solves some of the most urgent problems in theory, it still lacks adoption and wide-spread use in practice.

Many research projects work on closing the gap between theory and practice w. r. t. cloud Identity Management. The SkIDentity project, which we use as representative due to space constraints, is a member of the Trusted Cloud Initiative and integrates electronic ID cards with the management of cloud user identities. Unlike the traditional Identity Provider/Service Provider paradigm, SkIDentity is based on the concept of trusted eID brokers that provide the digital access tokes necessary to access cloud services. While this simplifies several workflows, it requires the specific adaption of each cloud service to make use of these eID credentials.

V. Architecture for Secure Federated Inter-Cloud Identity Management

The primary distinguishing feature of ICEMAN is that it combines technical aspects of Inter-Cloud Identity Management, such as $n : m$-relationships regarding identity data exchange, with organizational measures, such as a fully specified identity life-cycle for Inter-Cloud services and metrics-based security reporting. ICEMAN's working areas are:

- **Base technologies**: ICEMAN makes use of existing cloud APIs and Federated Identity Management protocols, including the Cloud Security Alliance's guidance for Identity & Access Management, Identity Management as as Service (IdMaaS) and the Liberty Identity Federation Framework maintained by the Kantara Initiative.
  For the practical Inter-Cloud application, a global Inter-Cloud namespace based on XRI is proposed, and dedicated data models are created for various types of Inter-Cloud identities, including users, devices, apps, services, and clouds. For each type of identity, attributes are specified and authentication as well as authorization mechanisms are selected.
  Major challenges are a) the integration of new users of Inter-Cloud services, i. e., natural persons without previous contract with one of the Inter-Cloud Identity Providers, and b) the classification of data processed by Inter-Cloud services along with a mapping of traditional intra-organizational access management rules and workflows. ICEMAN therefore proposes a data classification and indexing mechanism, for which a federated key management protocol is devised that allows for the delegation of access permissions, clearing or re-classification of data, and allows to assign temporary permissions to cloud services and other users in order to support Inter-Cloud data processing workflows.
- **Identity data exchange and access control**: For Inter-Cloud use cases, ICEMAN needs to extend traditional Federated Identity Management protocols, especially SAML, to support $n : m$ instead of only $1 : 1$ relationships between Identity Providers and Service Providers. One important aspect is that Inter-Cloud workflows typically require bilateral identity data exchange, i. e., unlike previous Federated Identity Management protocols, the same service or organization will act in both roles, identity data sender and recipient. Therefore, communication can no longer be modelled as a bipartite graph; instead, arbitrary meshed communication networks must be supported, which ups the ante for data synchronization to avoid temporary identity data inconsistencies especially during the initial identity provisioning and the deprovisioning phases, i. e., the initial on-demand account creation before first service usage and the cleanup after service usage has finished; the latter is required by European data protection and privacy laws, i. e, organizations are not allowed to store personal data longer than required for service provisioning and related processes, such as billing.
  ICEMAN furthermore strives for leveraging existing identity information: Ideally, user databases that are already available in organizations and cloud service providers should be re-used, clearing the hurdle for users to manually sign up for additional Inter-Cloud services. However, in practice those identity repositories rarely follow best practice or even standardized data models, which means that identity data cannot immediately be

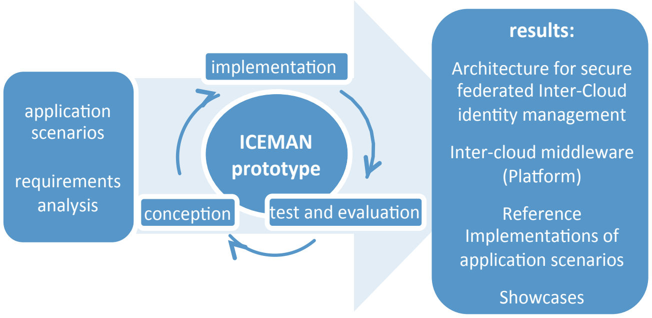
application scenarios
requirements analysis
implementation
ICEMAN prototype
conception
test and evaluation
results:
Architecture for secure federated Inter-Cloud identity management
Inter-cloud middleware (Platform)
Reference Implementations of application scenarios
Showcases

Fig. 2. Iterative approach within ICEMAN

applied to Inter-Cloud services due to syntactical and semantical discrepancies. ICEMAN proposes a dynamic data conversion component, which can be used by Identity Providers or Service Providers to convert identity information on-the-fly when sending or receiving it as part of an Inter-Cloud workflow. By making data conversion rules available in a distributed repository, the implementation cost for each in involved organization can be kept minimal.

- **Organization and management of Inter-Cloud Identity Management**: ICEMAN specifies the complete Inter-Cloud identity life-cycle for each of the identity types outlined above. It defines the workflows starting with the creation of identities, their on-demand provisioning to Inter-Cloud services, and their de-provisioning, i. e., removal, along with the roles and tasks of each involved organization. For each life-cycle phase, Identity Data Management processes are specified, such as inter-organizational consistency checks, and push-based notifications about changes to identity data, e. g., grant or removal of access permissions.

  As a distinctive feature, ICEMAN works on privileged account management for Inter-Cloud services, including cloud service administrators, auditors, and other roles with additional privileges. In order to avoid bottlenecks due to centralized administrative tasks, delegation and multi-client mechanisms need to be integrated without violating the strict separation of concerns.

  Inter-Cloud Identity Management has several interfaces with other service management processes. ICEMAN therefor defines the specific tasks regarding incident management, service billing, and several others. For example, from the user's perspective there needs to be a single point of contact regarding an Inter-Cloud service, as the user usually does not even know at which of the involved Inter-Cloud providers an incident, such as a service interruption, does occur. A Federated Fault Management process needs to locate the underlying error and trigger its removal by the responsible organization.

  ICEMAN also defines security metrics and a measurement process to acquire and refine security-related performance figures, such as the availability of services and the number of security incidents in Inter-Cloud workflows. Security reports are created for different target audiences, such as administrators and end users.
- **Practical application**: All developed technologies and the specified processes will be assembled to a demonstrator that reflects several of the identified use cases and shall ensure the use of the project results by fellow researchers and third parties. The Inter-Cloud Key Management and identity data exchange protocols will also be immediately be applied to on-going development projects of the project's industry partners; they will also bring selected results into the standardization bodies which they are members of.

VI. Conclusions and Outlook

The goal of the research project ICEMAN is to set new standards for the secure and trusted interoperability of community clouds by designing and implementing a Federated Identity and Key Management in an Inter-Community Cloud environment. The development of a Federated Identity Management approach, where (i) personal and property-related identification can be combined safely and (ii) a Federated Key Management for Inter-Cloud authorization is realized, are crucial for the further development of cloud computing, and thus of strategic importance.

The mixture of project partners in ICEMAN (covering the entire value chain: research, product development, service provider, end-users) also ensures that the project results are not only integrated in academic courses and the on-going development of concrete products, but that also service portfolios of, e. g., cloud strategy consultancies are updated accordingly.

Having defined the working areas of ICEMAN, the next step will comprise a first prototype (see Figure 2). ICEMAN uses an iterative approach to foster discussions with users as well as the industry and to begin with standardization efforts at an early stage.

Acknowledgment

This work was partly funded by Flamingo, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

References

[1] G. Dreo Rodosek, M. Golling, and W. Hommel, "MuSIC: An IT Security Architecture for Inter-Community Clouds," in *IFIP/IEEE International Symposium on Integrated Network Management*. Ghent, Belgium, 2013.

[2] P. Mell and T. Grance, "The nist definition of cloud computing (draft)," *NIST special publication*, vol. 800, p. 145, 2011.

[3] E. Bertino, F. Paci, R. Ferrini, and N. Shang, "Privacy preserving digital identity management for Cloud-Computing," *IEEE Data Eng. Bull.*, vol. 32(1), pp. 21–27, 2009.

[4] X. Huang, T. Zhang, and Y. Hou., "ID management among clouds," *First International Conference on Future Information Networks (ICFIN) 2009*, pp. 241–273, 2009.

[5] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Security and Cloud Computing: InterCloud Identity Management Infrastructure," in *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on*, june 2010, pp. 263 –265.