Access to the cloud

Identity and Access Management for cloud computing

Edwin Sturrus, Jules Steevens and Willem Guensberg

E. Sturrus
works as a consultant at
KPMG IT Advisory.
sturrus.edwin@kpmg.nl

J. J. C. Steevens
works as a consultant at
KPMG IT Advisory.
steevens.jules@kpmg.nl

W.A. Guensberg
is a partner at Label A.
willem@labela.nl

Cloud computing is maturing past the ‘hype’ stage and is considered by many organizations to be the successor to much of the traditional on-premise IT infrastructure. However, recent research among numerous organizations indicates that the security of cloud computing and the lack of trust therein, are the biggest obstacles to adoption. Managing access rights to applications and data is increasingly important, especially as the number and complexity of laws and regulations grow. Control of access rights plays a unique role in cloud computing, because the data is no longer stored on devices managed by the organizations owning the data. This article investigates and outlines the challenges and opportunities arising from Identity and Access Management (IAM) in a cloud computing environment.

Introduction

In recent years, cloud computing has evolved from relatively simple web applications, like Hotmail and Gmail, into commercial propositions such as SalesForce.com and Microsoft Office 365. Research shows that most organizations currently see cloud computing as the IT model of the future. The security of cloud computing and the lack of trust in existing cloud security levels, appear to be the greatest obstacles to adoption ([Chun10]). The growing amount of data, users and roles within modern organizations, and the stricter rules and legislation in recent years concerning data storage for organizations, have made the management of access rights to applications and data increasingly important and difficult. The control of access rights plays a unique role in cloud computing, because data stored in the cloud demands new, often different security measures from the organizations owning the data. Organizations must change how identities and access rights are managed with cloud computing. For example, many organizations have limited experience with the management and storage of identity data outside the organization. Robust Identity & Access Management (IAM) is required to minimize the security risks of cloud computing ([Gopa09]). This article describes the challenges and opportunities arising from Identity & Access Management in cloud computing environments.

What is cloud computing?

Although much has been published on the topic of cloud computing, it remains difficult to form a precise definition for this term.

One of the commonly used definitions is the following ([NIST11]): *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

KPMG has taken this definition as a starting point and has narrowed it somewhat to the perspective of a recipient of cloud services ([Herm10]):

> "Cloud computing, from the perspective of the user, is the usage of centralized computing resources on the Internet. Cloud computing differs from traditional IT via the following characteristics:
>
> - *Multi-tenancy*. Unlike traditional IT, the IT resources in the cloud are shared across multiple users.
> - *Paid services*. The user only pays for the use of cloud services and does not invest in additional hardware and software.
> - *Elasticity*. The capacity can either increase or decrease at all times.
> - *Internet dependent*. The primary network for cloud services is the Internet.
> - *On-demand services*. Unlike the greater part of traditional IT, cloud services can be utilized practically immediately."

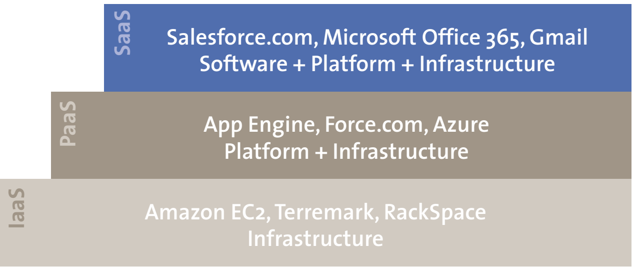
SaaS
Salesforce.com, Microsoft Office 365, Gmail
Software + Platform + Infrastructure
PaaS
App Engine, Force.com, Azure
Platform + Infrastructure
IaaS
Amazon EC2, Terremark, RackSpace
Infrastructure

Figure 1. **Forms of cloud computing.**

Different types of cloud services are available. First and foremost is Software-as-a-Service (SaaS) where software is provided as a cloud service. There is also Platform-as-a-Service (PaaS) where a platform (operating system, application framework, etc.) is offered as a cloud service. Finally, there is Infrastructure-as-a-Service (IaaS) where an IT infrastructure or part thereof (storage, memory, processing power, network capacity, etc.) is offered as a cloud service.

What is Identity & Access Management?

Broadly speaking, IAM is the consolidated management of users and corresponding authorizations via a centralized identity register. IAM allows an organization to control who gets access to what and by what means. KPMG uses the following definition of IAM ([Herm05]): *"The policies, processes and support systems to manage which users have access to information, IT applications and physical resources and what each user is authorized to do with it."*

IAM is categorized as follows ([KPMG09]):

- *User management:* The activities related to managing end-users within the user administration.
- *Authentication management:* The activities related to the management of data and the allocation (and de-allocation) of resources needed to validate the identity of a person.

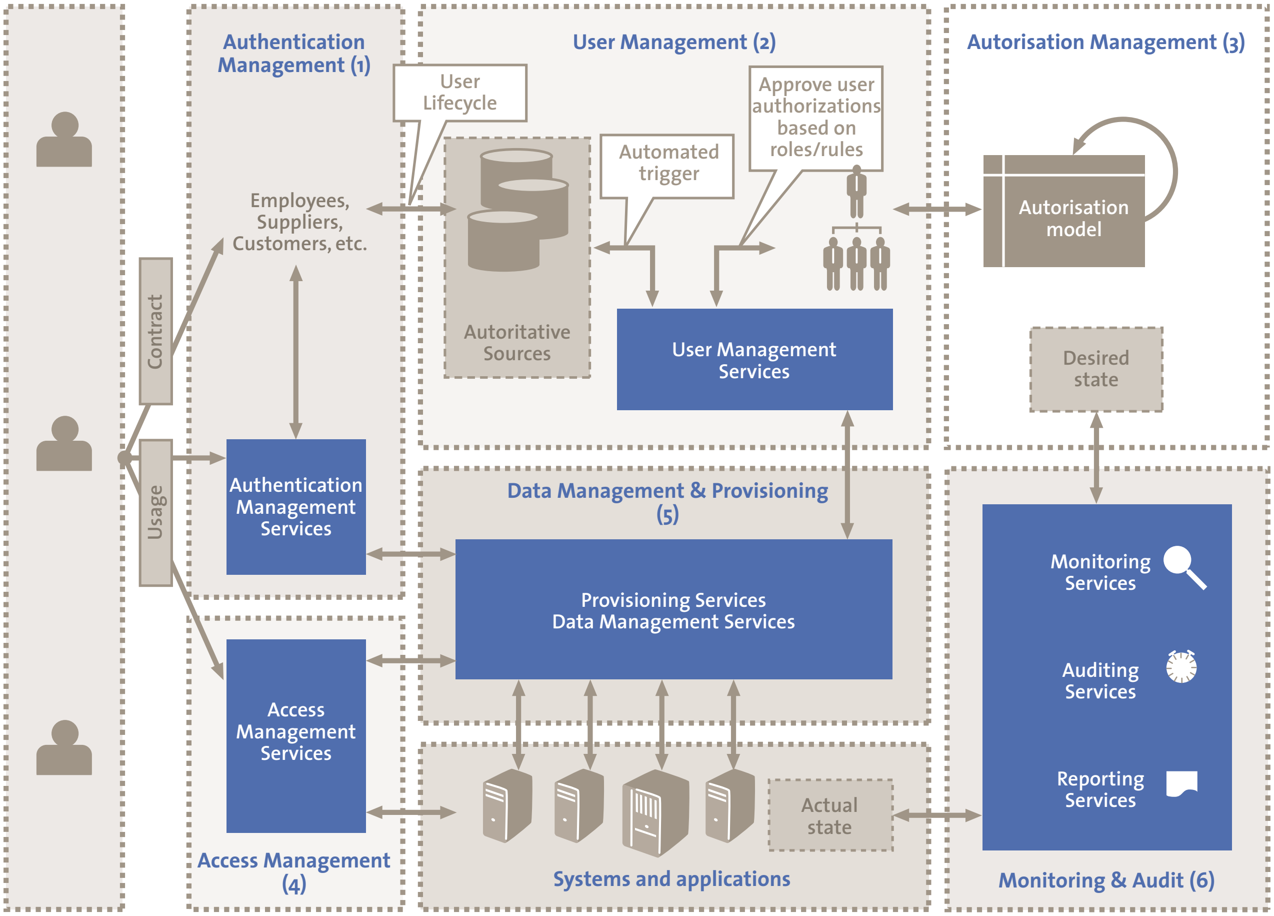

Figure 2. **IAM reference architecture.**

- *Authorization management:* The activities related to defining and managing the access rights that can be assigned to users.
- *Access management:* The actual identification, authentication and authorization of end users for utilizing the target system.
- *Provisioning:* The propagation of identities and authorization properties to IT systems.
- *Monitoring and auditing:* The activities required to achieve monitoring, auditing and reporting goals.
- *Federation:* The system of protocols, standards and technologies that make it possible for identities to be transferable and interchangeable between different autonomous domains.

IAM plays a major role in securing IT resources. IAM faces many challenges when cloud computing is used. IAM processes, such as adding a user, are managed by the cloud provider instead of the organization owning the data. It is difficult for the organization using the cloud service to verify whether a modification has been completed successfully within the administration of the cloud provider. Furthermore, it is harder to check whether the data stored by the cloud provider is only accessible to authorized users.

The next section elaborates on the various challenges related to the components of the IAM architecture in a cloud computing environment.

IAM challenges in a cloud computing environment

The existing challenges in managing users and access to information are complemented with new challenges brought along with cloud computing. Originally, the organization itself was responsible for all aspects of IAM. This ranged from maintenance of user administration to the propagation of user rights in the target systems and checking usage based on logging and monitoring.

The introduction of cloud computing has made these activities more complex. The boundaries are blurring between what user and IT resources belong to the “customer” and what belongs to the “cloud provider”. Who owns what resource and carries the accountability that goes with it? What is the difference between accountability and liability? This section summarizes some of the challenges of IAM.

User management

User management deals with the policies and activities within the scope of administering the entire lifecycle of users in the appropriate registers (initial registration, modification and deletion). For example, this could be the HR system for the employees of an organization. The HR system records the recruitment, promotions and dismissal of employees. In addition, user management controls the policies and activities related to granting authorizations to the users registered in the HR database.

An organization that utilizes cloud services may be faced with challenges in user management that are new compared to the traditional on-premise situation. Managing the user life cycle in the traditional IT environment is a challenge, it is even more so in a cloud environment. The organization cannot always maintain control over user administration via their own HR system (or other centralized resource). The cloud provider usually also maintains a user administration system. What happens when users update their information via the cloud provider? How are the managers of the cloud services and their attributes kept up to date? Which laws and regulations (possibly outside own jurisdiction) apply to the storing of personal information? All these issues have to be dealt with again in a cloud computing environment. The allocation of authorizations is also a part of user management. The customer and cloud provider must agree on who is responsible for granting and revoking user rights.

Authentication management

Authentication management includes the processes and procedures for administering the authentication of users. If particular data is very sensitive, stringent authentication may be required to access this data (for example, by using a smart card). Defining and recording these requirements within objects in the form of policies and guidelines is part of authentication management. Authentication management also deals with the issuing and revocation of authentication means (for example, username and password and smart cards).

The following challenges in authentication management are new compared to the traditional on-premise situation: the authentication means for different cloud providers may vary. Sometimes, the cloud provider itself may only use mechanisms that do not match the (security) technical requirements of the customer. It can also be complicated to implement the level of authentication in a uniform way. In addition, synchronization of passwords can be a challenge, especially in environments where the user administration changes quickly or where users must change their own passwords. Finally, it requires that a working Single Sign-On (SSO) environment is maintained for technical integration with the cloud provider. SSO is a collection of technologies that allow the user to authenticate for different services once as a particular user, which allows access to the other services.

Authorization management

Authorization management deals with the policies and activities in relation to defining and administering authorizations. This allows authorizations to be grouped into a single role (based on so-called authorization groups). After granting this role to a user, that user can carry out a particular task or sub-task on certain objects. When a manager welcomes a new team member, he has to grant the appropriate role to the new user. Once the association is made, the authorizations that belong to this role are now available to the new user. As previously described, the granting of these predefined roles to users is carried out via user management.

Likewise for authorization management, there are new challenges when the organization utilizes cloud services. The cloud provider and the customer must agree upon where the authorizations and/or roles are managed. The IAM system must be capable of exchanging (automated) messages with the means of authentication that the cloud provider uses. In many cases, the cloud provider and customer use conflicting role models and the maturity of the role models differ. For example, the cloud provider may have switched over to centrally organized Role-Based Access Control (RBAC), while the customer still uses direct end-user authorizations that is administered in a decentralized manner. In accordance with user management principles, it is necessary to maintain a trusted-relationship on authorization management that is supported by contractual agreements.

Access management

Access management deals with the (operational) processes that ensure that access to IT resources is only granted in conformance with the requirements of the information security policies and based on the access rights associated with the users.

The domain of access management has the following new challenges compared to the traditional on-premise situation: access management requires agreements to be made between the cloud provider, third parties and the customer, on how to appropriately organize access to the target systems. For example, the exchange of authorization data (user names, passwords, rights, and roles) must be fast enough to grant or deny access instantly. The customer and the cloud provider can decide to establish a trusted-relationship supported by certificates and/or a Public Key Infrastructure (PKI).

The utilization of cloud services creates new challenges for authorization management

Provisioning

IAM must ensure that after a role is granted to a user, the user is created in the relevant objects, and that this user is then granted the appropriate authorizations for corresponding objects. Within IAM, this process is called provisioning. Provisioning deals with the manual and/or automatic propagation of user and authorization data to objects. In other words, provisioning consists of creating a user and assigning authorizations to the user objects. Manual provisioning means that a system manager creates a user with authorizations on request. Automatic provisioning means that the system automatically processes these requests without any intervention by a system manager. When a role is revoked from a user then deprovisioning has to take place, which means that the authorizations are revoked from the user.

Provisioning in a cloud environment has the following challenges: the propagation of accounts within the organization and also within the cloud provider is challenging, since technologies and standards are often different for each cloud provider. As more cloud providers deliver services to an organization, it becomes exponentially more complex for the customer to implement provisioning. The creation and modification of accounts and rights on target systems is generally driven by business need. However, it is often the case that less attention is given to deletion because it serves limited business need and it is believed that the security risk does not outweigh the additional effort required to follow through this deprovisioning process effectively. With respect to the contract with the cloud provider, customers often forget to give sufficient attention to the ending of the relationship. It is then unclear what happens to the data and user rights when the cloud provider no longer provides paid services to the customer.

Monitoring and auditing

The final piece in the IAM architecture is the monitoring and auditing process. This process focuses on checking compliance with policies utilized within IAM. This consists of continuously monitoring and auditing the systems and processes.

In the area of monitoring and auditing, the following are new issues compared to the traditional situation: it is a challenge for many customers to set up monitoring and auditing compliance with the requirements of the applicable information security policies. One reason for this is that the customer often does not have insight in what resources the cloud provider utilizes to manage and monitor the IT resources. A consequence of this lack of transparency is that it may be difficult for a customer to achieve full compliance. In particular, the use of accounts with high-level privileges is difficult to monitor.

Options for IAM in a cloud environment

Several options are available for managing identity and access to cloud services ([Blak09], [Cser10]). The ownership of the various IAM processes and attendant monitoring is different for each model. This has a significant impact on the relevant risks and challenges. The option preferred thus depends on the requirements of the organization and the level of cloud service adoption in the organization.

Traditional model

If an organization utilizes part of its IT needs as a cloud service, the components of the IAM framework must work together with the cloud provider. This may be achieved by linking the existing IAM with the cloud provider (see Figure 3). In this case, the organization manages identities and access rights locally and then propagates these to the various cloud providers. For each cloud provider, the authorized users must be added to the directory of the cloud provider. There are several packages on the market that automate the processes of creation, modification and deletion by synchronizing the local directory with the cloud. However, the "connector" that enables the synchronization to occur must be separately developed and maintained for each cloud provider. A drawback is the added complexity in management when there are multiple cloud providers.

Identification and authentication for cloud services occurs with the cloud provider. Handing these processes over to the provider requires strong confidence in the provider. There are tools on the market that make it possible to link with local SSO applications. With this method the user needs fewer identities to access services. Checking identification and authentication for cloud services is performed by the cloud provider. Strong confidence in the cloud providers and their policies is required.

This option is already actively used by a large Dutch retailer that has linked the local IAM infrastructure to their cloud provider of email and calendar services.

Trusted-relationship model

Another option to allow IAM to have the cloud provider support the IAM of the customer (see Figure 4). The customer manages the local identities and access rights. The users are stored locally in a directory and an access request for a cloud service is authenticated locally. The cloud provider checks the authorizations and validates these using the directory of the customer. The cloud provider thus trusts the IAM of the customer and it is on that basis that the users can utilize the services. Thus, in most cases, duplication of accounts is unnecessary (unless for auditing purposes).

If this option is used, the customer may continue to use the existing access methods to manage the user activities. A disadvantage for this option is that, when there are a large numbers of cloud providers, it is necessary to make agreements with each cloud provider about the confidentiality of the customer's local IAM. In addition, for many cloud providers, it is impossible to maintain trustworthy and appropriate monitoring of the IAM of all customers.

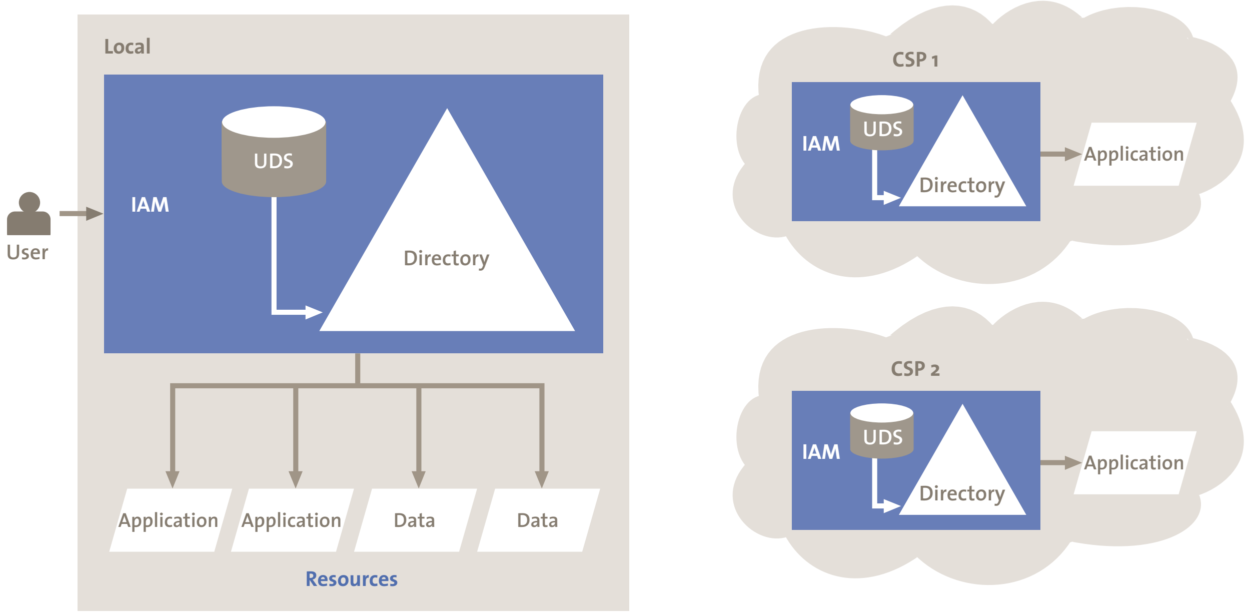

Figure 3. **Connecting with the cloud provider.**

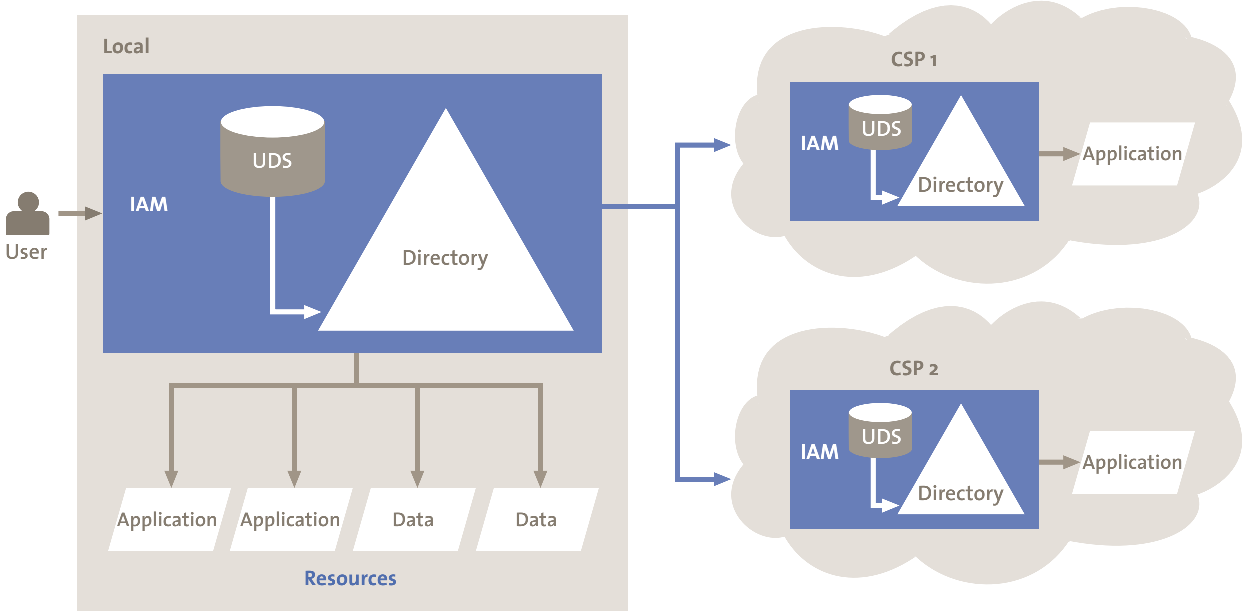

Figure 4. **Federated cooperation between customer and provider.**

The use of cloud services requires changes in the IAM domain

Identity service provider model

A third option for cooperation between the local IAM of the customer and the cloud provider is using an Identity Service Provider (IdSP) (see Figure 5). The IdSP is a provider of identity services. As in previous models, the customer manages the local identities and access rights. The IdSP is responsible for validating the identity of the user. Both the cloud provider and the customer rely on this third party to validate the identity of users. DigiD and Facebook are examples of organizations that may act as an IdSP and be able to verify digital identities in the future. There are tools on the market that use a third party to manage and validate identities.

All-in-the-cloud model

The last option is to outsource the entire IAM and utilize it as a cloud service (see Figure 6). In this case, the organization delegates all IAM systems and processes to a third party operating in the cloud itself. The link with all cloud providers is managed and controlled by this third party. Access to local IT resources will also be conducted via the IAM Service. Effectively, all management and control of IAM are outsourced to the cloud.

High trust in the IAM service is required. It is difficult for the customer to monitor the status of the processes for either local or cloud services. Currently, there are no fully functioning IAM cloud services available, but it is possible that large IAM providers (for example, IBM, Microsoft and Oracle) will enter this market in the coming years.

Conclusion

By using (public) cloud services, the organization will need to revise its control measures to maintain the required level of security. Whilst security risks may well decrease by transferring selected services to the cloud, risks are likely to increase in certain areas such as IAM. To minimize the risk it is necessary to properly set up the IAM framework. The implementation of necessary changes to IAM in a cloud environment is critical in providing an adequate level of confidence and guarantee security.

The fact that some of the IT resources are no longer contained in the organization itself raises several questions in the IAM domain. Even though liability remains with the organization utilizing services, keeping control of the IAM processes is more difficult because these are often part of the cloud provider's domain. For user management, it is important that organizations verify whether changes to user data are taken over by the cloud provider. Organizations must comply with company, national and international laws and regulations with regard to personal information. When considering authentication, it is important

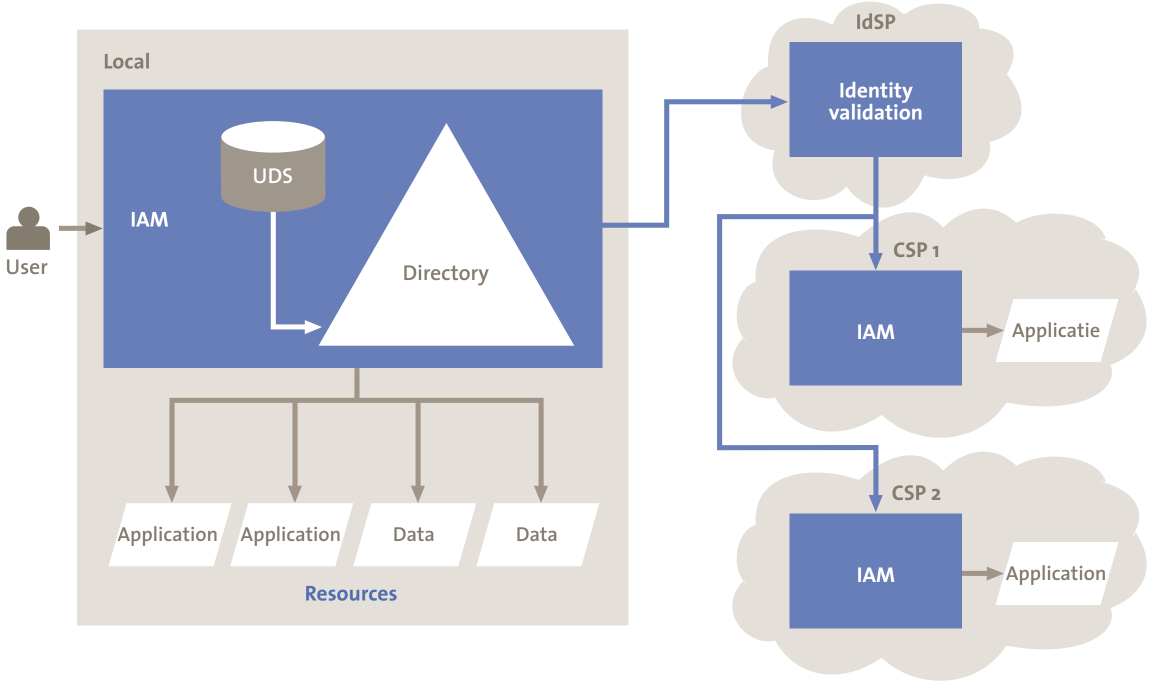

Figure 5. **Utilization of an identity service provider.**

that the authentication methods and requirements used match those of the cloud provider. Furthermore, the authorization models should align, so that the correct rights are granted to the authenticated users. The processing of both authorizations and authentications must be timely and accurate in order for the partnering organizations to have confidence in the actual use of cloud services. Finally, it is essential that the monitoring and auditing processes meet the requirements of the applicable security policies.

Several options are available for managing identity and access to cloud services. Firstly, the IAM framework can be connected with the cloud provider. The customer itself manages and propagates users and the rights to the cloud provider. It may be possible to automate this process. Identification and authentication occur in the cloud provider domain. A second option is to allow the cloud provider to support the customer's IAM framework. The use of this trusted-relationship makes it unnecessary to propagate user to all cloud providers. In addition, identification and authentication occurs locally. A third option is to use an IdSP. This is a third party which is trusted by both customers and cloud services providers and validates the identity of users. The last option is to outsource the entire IAM stack and consume IAM as a cloud service altogether.

Which option is the most suitable depends on IAM requirements of the organization and on the type and number of cloud services consumed. The IAM framework should be properly established before cloud services are utilized to minimize risk exposure. Furthermore, it is very important to align the IAM framework with the cloud landscape to allow effective cooperation with the cloud provider and adequate security safeguards.

References

[Blak09] B. Blakley, *The Business of Identity Services*, Midvale, Burton Group, 2009.

[Chun10] M. Chung and J. Hermans, *From Hype to Future: KPMG's 2010 Cloud Computing Survey*, KPMG Advisory, Amstelveen, 2010.

[Cser10 A. Cser, S. Balaouras and N.M. Hayes, *Are You Ready For Cloud-Based IAM?*, Cambridge, Forrester Research, 2010.

[Gopa09] A. Gopalakrishnan, *Cloud Computing Identity Management*, SETLabs Briefings 7 (7), p. 45-54, 2009.

[Herm05] J. Hermans and J. ter Hart, *Identity & Access Management: operational excellence or 'in control'?*, Compact 2005/3, p. 47-53.

[Herm10] J. Hermans, M. Chung and W. Guensberg, *De overheid in de wolken?* (The government in the clouds), Compact 2010/4, p. 11-20.

[KPMG09] KPMG, *IAM Methodology*, KPMG International, 2009.

[NIST11] NIST, *The NIST Definition of Cloud Computing*, Information Technology Laboratory, Gaithersburg, National Institute of Standards and Technology, 2011.

About the authors

E. Sturrus works as a consultant at KPMG IT Advisory. He gives advice in the domain of Identity and Access Management and is involved in IT Audit assignments. He recently completed his research at Erasmus University Rotterdam about Identity and Access Management and cloud computing.

J. J. C. Steevens works as a consultant at KPMG IT Advisory. He specializes in advising on Identity & Access Management in which authentication and authorization management plays a major role. In addition to advising, he carries out IT audits on Public Key Infrastructures (PKI) and the like.

W.A. Guensberg is a partner at Label A. Label A develops practical and sexy apps and sites. Dummy-proof and high-tech, with a focus on mobile and cloud technologies. Willem was a consultant at KPMG IT Advisory from early 2007 to late 2011. He gave advice in the domain of Identity and Access Management (IAM) and cloud computing. He completed his IT audit course at Vrije Universiteit and received his CISA accreditation in 2009. In 2010, he worked for six months as a cloud computing consultant at KPMG in Boston (US).

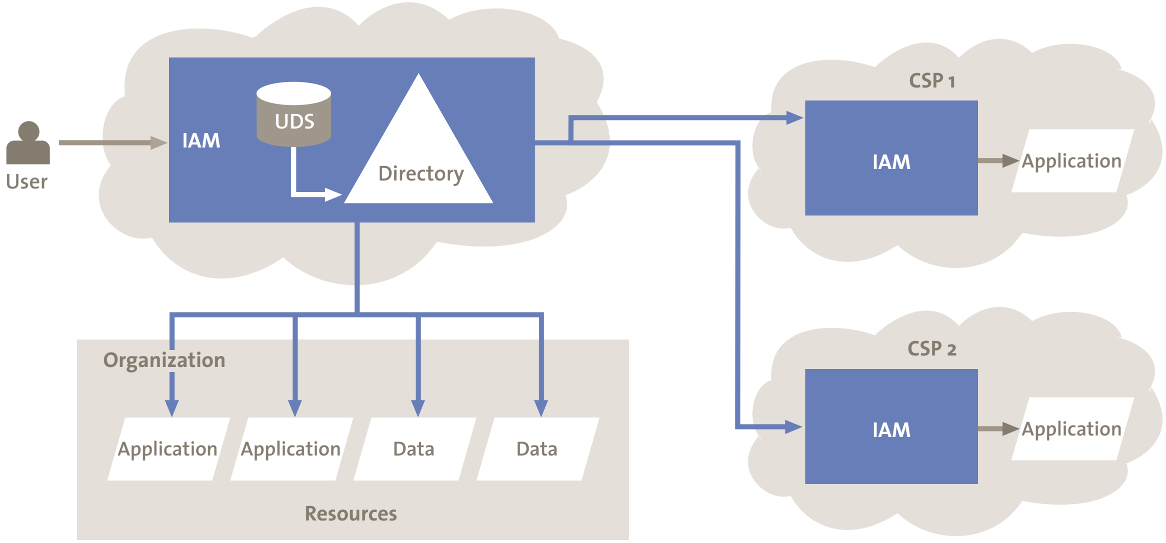

Figure 6. **IAM as a cloud service.**