



Identities from the cloud

Security as a service

Cloud computing, cloud services and virtualization are no longer only buzzwords in academic discussions, but an ongoing practical trend. Many IT services are already available from 'the cloud' - consumed and used over the Internet.

CLOUD SERVICES ARE SCALABLE AND ELASTIC. They have a predictable pricing model and charges are based on actual usage. And, although cost efficiency is a major goal in optimizing IT operation, an organization should never neglect security concerns relating to the use of cloud services. The security of sensitive data and processes - often left unprotected within the boundaries of the corporate network - needs to be reconsidered.

The same economical and organizational arguments that apply for primary IT services hold true for security services and may justify outsourcing. Digital identities from the cloud add a new perspective to virtualization and cloud computing. This paper introduces identity cloud services that use Public Key Infrastructure (PKI) and related technologies for strong digital identities and validation. It further explains the important aspects to be considered when evaluating providers of security identity services.



Cloud services in general

There are numerous applications and services already available as cloud services. These can replace a company's existing IT architecture and processes while also providing interoperability through the universal use of commonly established Internet standard interfaces and protocols.

According to Gartner, the main cloud service characteristics are:

- ✓ use of Internet technologies
- ✓ a shared pool of resources
- ✓ service-based models, no purchase of licenses necessary
- ✓ scalability and elasticity: The service can be scaled up or down to suit specific needs, but the content of the service is usually fixed.
- ✓ it is metered by use. You pay for what you actually use.

A cloud service usually has narrow defined content and application. The idea is to provide typical, general purpose services in the form of complete solutions, which suit most customers' needs. With cloud services there should be no underutilization.

Cloud services offer various benefits with regard to availability, scalability and cost saving potential. But, security aspects top the charts of cloud services' challenges and issues.

Among the cloud computing applications that deliver software as a service you can find file storage solutions, project management software, and CRM tools. These services are usually accessible via web browsers without client installation or other special requirements.





Identity cloud services

Digital identity cloud services differ in some aspects from the aforementioned and more general cloud service models. Before we learn more about general benefits, constraints and differences, here is a brief introduction to cloud services for digital identities:

- **Identity Service**

The Identity Service will deliver ready-to-use and trustworthy electronic identities direct to end users. Identities are issued by a Certificate Authority dedicated to the client organization and hosted by the service provider. Software tokens, smart cards and smart USB tokens can all be supported. Services include replacement of lost tokens containing the original encryption keys.

- **Login Service**

The Login Service controls access to a service or application. It allows users to authenticate to the application using existing electronic identities. The identities are verified through a web service, which is easy to integrate into the application. Single Sign-On can be provided for convenience when accessing several applications. The Login Service can accept several different electronic IDs, such as the client organization's own identities or other organizations' federated identities, as well as national identities.

- **Signing Service**

With the Signing Service, digital signatures can be created and validated for a business or e-commerce process to express commitment and make agreements legally binding. The digital signatures are validated by an easy-to-use web service, which is also easy to integrate into the business application. Signatures can be used for financial transactions or contracts created on the web in XML or PDF format. The Signing Service can include archiving of the signatures and associated documents.



Identity service benefits

Compared to installing and maintaining an in-house system, there may be compelling benefits for digital identities from the cloud:

- ✓ The time to going productive is much shorter and cheaper.
- ✓ There is no need to pay for software licenses upfront.
- ✓ It is much easier to start small and then scale up.
- ✓ There is no need for different IT environments for testing and pre-production purposes.
- ✓ There is no need for knowledge of, expertise with, or control over the technology infrastructure that supports the outsourced service.

Considerations and constraints

Organizations considering outsourcing IT services must be aware of the loss of direct control and flexibility. A cloud service usually has a fixed framework that the customer must conform to and it might be difficult to add desired features within the framework of existing services. The reason is, of course, the economics of scale and volume.





WHITE PAPER

Heterogeneous IT environments can also cause problems. A cloud service does not automatically mean that all existing browsers and operating systems are supported. A certain level of reliability must be assured for the networks that are used to access cloud services.

Apart from the technical issues, social acceptance from end users can be a problem. Some end users are used to internal IT support services and may feel uncomfortable with more anonymous services.

Attention should also be paid to the loss of direct control and the implications this has for security. Responsibility for compliance will always remain with the company, even if control has been re-assigned. This should be taken into account when choosing a provider and defining appropriate security measures.

Special aspects

Compared to the more common cloud services for managing file storage, word processing, customer contacts, etc., the service for digital identities has some special features:

- **Limited mobility**

A cloud service is usually independent from specific physical client computers. The user can use any workstation and access the service via a browser. But certain credentials, like software tokens, must be installed locally on a specific computer. To utilize the software token the very same computer must be used.

- **Dependency on internal identity management**

To produce identities in the form of certificates, personal information about the user must be transferred to or accessed by the service provider. Therefore, the cloud service inherently requires internal identity management.

- **Variety of applications**

The distributed identities can be used by end users in many different applications not controlled by the service provider.

- **Involvement of several parties**

Common cloud services are focused on end users. Identity cloud services involve other individuals, e.g. administrators of identities, application owners, human resources departments, security managers. When issuing digital identities, there must be a central control function for security and management. Administration costs can be reduced, but will not be eliminated.

Individual requirements

When it comes to making decisions about the use of cloud services for identities, knowledge of cloud services' benefits, constraints and differences is not enough. Individual requirements in terms of existing IT and organizational structures can be decisive, so these aspects have to be considered as well.

- **Organizational structures**

In very large international organizations, it can be difficult to create centralized management for all identities, a so-called trust centre. The reason is not so much technical, but rather political, organizational and administrative. In such an organization, it makes sense to have a central policy that sets requirements for the services used, but lets the units decide for themselves. From a PKI perspective, it is a question of having one central certificate authority (CA) or allowing the units to have their own CAs, externally hosted or not.

- **Making applications ready for security services**

The internal infrastructure must be made ready for the cloud service – it cannot be the other way around. It is recommended to choose cloud services that are based on common standards with standard-based interfaces. In the event of switching to another service provider or back to an in-house solution, the effort and costs will be much lower.

Before the end users are given digital identities, it must be clear which applications should be available to them. The services to be used with digital identities have to be identified, prepared and tested accordingly.





This can be costly, especially with proprietary legacy applications.

- **Clear picture of cost**

The total cost will consist of the fees for the identity service, as well as any internal investment to prepare the organization's IT environment. The pricing model should be transparent right from the start and not leave room for surprises.

The internal costs are hard to estimate. The best way is to test the service and see how much effort it requires. The identities – either hardware or software-based – can be a critical cost factor.

- **Management of identities**

Account provisioning and, more importantly, de-provisioning are crucial for all organizations. This is one area where digital identities using PKI excel: by revoking the identity, access to all applications using certificates for login is instantly terminated.

Using identities from the cloud does not mean that responsibility for identity management is transferred to the service provider. This responsibility will always remain with the organization. The trustworthiness of digital identities depends specifically on the quality of internal identity management. If the personal information about the subject of the identity is incorrect from the source, the issued digital identity will be unusable. Therefore proper quality assurance must be applied for the personal data that is transferred to the service provider.

National legislation

Depending on the applications used with the identities, national legislation can be an important aspect to consider when selecting the service provider. Providers follow the national laws and regulations of the country where the services are offered. This is especially important for PKI-related services, because they can be used for legal actions covered by legislation, e.g. financial transactions, taxation, invoicing, and signing of contracts.

It's a question of trust

Services for identities are security services and will be part of the overall security system of the organization. Any security system relies on a chain of trust. Each part must put trust in its interconnected parts. A chain is only as strong as its weakest link. The provider of the cloud services must not become the weakest link.

Cloud services from Nexus

For Nexus offering cloud services is a new way of utilizing mature Nexus software technologies. At Nexus, we want to make use of our long experience with PKI, smart cards, and secure and user-friendly lifecycle management processes while offering cloud services. With full service identities we would like to maximize usability, minimize the risks of human error, and enable access to a broad range of applications.

Conclusion

The management of identities and related security services for access control and digital signatures can be provided as a service, just like other IT services. Hosted security services may be the perfect answer to the challenge of more stringent security demands related to hosted business applications.

Apart from the generally applicable considerations for purchasing cloud services, some specific aspects need to be considered, such as the loss of direct control and flexibility, the need for standard compliant interfaces with the business applications to be protected, proper internal identity management processes, and proper mapping of policies to suit the needs of large, widespread organizations.

Still, if the reported general benefits of cloud services are convincing, outsourcing identity services is usually the right choice. The most benefit might be gained from sourcing all related security services – identities, login and signatures – from the cloud and from the same provider.

With this paper the reader should be in a good position to make the initial investigations and considerations required for an identity outsourcing project.

