Security and Privacy in the Digital World

Solutions from the Smart Security Industry

Digital Identity and Access Management as a Subset of Privacy and Security in Cloud-Based Services

Content

June 2012

1. Executive Summary

Until now, identity and access management – as part of Security and Privacy for Cloud-based Services with personal data – has not been comprehensively well defined by the European Commission. Actions and Pan-European regulations are still sorely missing. When it comes to gaining access to personal data, databank and data management systems, what is known as "two-factor" authentication is recommended by EUROSMART for all users, according to the proposed Regulation "on electronic identification and trusted services for electronic transactions in the internal market". Two-factor (e.g. "to have" and "to know") is strong authentication technology in the security domain. A European guideline on security and privacy for Cloud-based Services in the near future could foster the internal market in Europe and instil more trust among citizens, as well as for enterprises and the public sector with regard to data protection and privacy. We believe this could be an important element of the Digital agenda for Europe as well as the European Cloud Computing Strategy. This approach could avoid having to formulate national specific policies and guidelines in 27 Member States, which foster non-interoperability on security, privacy and data protection in Europe.

2. Introduction

Cloud computing is increasingly becoming a solution for small to medium sized businesses in Europe as they look for ways to increase efficiency and reduce costs. However, citizens in Europe have three valid questions regarding cloud computing:

(1) Where is my data stored?
(2) Is the data center really secure?
(3) Who has access to this data?

The objective of this White Paper is to describe existing international cloud security initiatives, what is required to achieve mutual recognition of electronic identification, authentication and signatures and to suggest a European definition of required identity and access management levels for different classes of cloud services.

Cloud computing, (definition by NIST[1]): *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

Cloud providers offer "as a service" either the Infrastructure (IaaS), that is to say a virtual configurable IT infrastructure, on demand, or a Platform (PaaS) upon which applications and services can be developed and hosted, or Software / Application (SaaS) implementations of specific business functions and business processes.

Security in cloud-based services can address various aspects on hardware and software components, devices and solutions. The focus of this position paper is the identity and access management for user, maintenance provider, service provider and other persons.

Digital Identity Management (IDM) is the capability to identify a user, and verify that he has the identity he claims, whilst protecting his personal data. Access Management (AM) is the capability of verifying that a user effectively has the rights to access to the resources / services, he is asking for.

[1] NIST is the National Institute of Standards and Technology, the US federal technology agency that works with industry to develop and apply technology, measurements, and standards.

The primary focus of this paper is on privacy and security in cloud services, meaning services with personal data. It has two pillars in the public domain:

- European Commission (EC) programmes and activities (e.g. public consultations, technical reports, speeches of EC member)
- EC funding projects (e.g. STREP, IP, CSA and CIP)

The secondary scope is an analysis of international cloud security initiatives from the ICT industry and their recommendations on identity and access management as a subset of privacy and security.

3. Problem Definition and Status in Europe

The European Commission wants to maximise the benefits from the cloud, while allowing organisations to respect their obligations under EU law. But potential users still hesitate. They worry about the service they will be receiving, about risks of lock-in and whether they can trust the provider with their data. The EC has decided to work on a European Cloud Strategy for mid-2012. The strategy will set out how different actions can serve this goal, how to make Europe not just Cloud-friendly – but Cloud-active. In this sense, it is evident that self-regulation among service providers, when it comes to security, can tend towards solutions that are "cheaper" due to the competitive nature of the market. This being the case, in order for European citizens and businesses to be protected from numerous and real threats, solid and well thought out regulatory guidelines must clearly outline the kinds of security measures that are suggested in this document.

3.1. European Cloud Strategy, focus on IDM (targets & timelines)

The need to develop an EU-wide strategy on Cloud Computing is highlighted in the Digital Agenda for Europe (DAE). Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, in her speech at Davos[2] in January 2012, outlined the European Cloud Computing Strategy. The three broad areas for the cloud strategy are:

1. The **legal framework**: this concerns data protection and privacy, including the international dimension;
2. The **technical and commercial fundamentals**: the aim is to extend the EU's research support and focus on critical issues such as security and availability of cloud services;
3. The **market**: pilot projects will be supported aiming at cloud deployment.

Work has already started in several of these areas, including a public consultation[3], which ended in August 2011. The outcome will be a document combining analysis and a plan of future actions, which will be presented in 2012.

[2] europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50
[3] ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf

Conclusion on security aspects in cloud-based services with focus on IDM/AM: in her speech in Davos, Vice-President of the European Commission Neelie Kroes pointed out **data protection and privacy concerns in cloud-based services, but Identity Management and Access Management were not explicitly addressed yet**.

3.1.1. Recommendations from the ENISA (17 January 2011)

After the European Network and Information Security Agency (ENISA) launched its "*Cloud Computing: benefits, risks and recommendations for information security*", 20th of January 2009, ENISA published a 2nd paper in this domain with "Recommendations to governments and public bodies" (2011).

There are many recommendations related to all types of risks pertaining to cloud computing. Among them, one is relative to the need of managing identity, but without details:

"Take into account relevant national and international regulations applying to third parties (e.g., electronic digital signature directives, ISO third-party assurances) in order to ensure the trustworthiness of the communications between all the parties involved in the provision of the service (Public Authorities, citizens, services provider-business parties, as well as systems). The authenticity of the identities of the parties and their authorization to perform an action, the point in time (i.e. timestamp), and location should be assured."

It is worth noting that in its analysis of the Healthcare record use case, ENISA referred to the use of the Spanish system for identity management, stating *"that it appears to be of particular interest. The identity card (DNIe) incorporates a device for the creation and verification of an electronic signature. The verification is performed against two formal systems for the validation of certificates. The system works for citizens in the private and public sectors, and the technical specification have now been made public in order to allow distinct developments".*

In a presentation, Dr. Giles Hogben (ENISA) stated that the cloud could not work without federated identity providers. Poor identity verification makes cloud platforms vulnerable to attacks. Federated Identity Management is the only solution that scales to the cloud.

The proposal for a Regulation on «Trust and confidence in electronic transactions in the internal market»[4] aims at enabling secure and seamless electronic transactions between businesses, citizens and administrations. Thereby increasing the effectiveness of public and private electronic services, e-business and e-commerce is indicated. The target is **that electronic identification, authentication, signatures and related ancillary trust services (eIAS)** are mutually recognised and accepted throughout the EU. Available eIAS services could facilitate efficient and secure Digital Identity and Access Management for clouds.

Conclusion: **Identity and access management as a subset of privacy and security in cloud-based services are particularly addressed, e.g. in a health domain. Comprehensive approaches on technology and standards as well as recommendations in the cloud service domain are missing today.**

[4] COM(2012) 238/2

3.2. Results of Public Consultation

A public consultation on cloud computing in Europe was opened on 16 May and ran until 31 August 2011. The largest single group of respondents claimed to represent companies (230 from 538). The second largest group where individuals (182). The remainder were public administrations (33), academics (42) or others (51).

The main conclusions are that the EU legal framework creates uncertainty. Rights, responsibilities, data protection and liability, especially in cross-border situations must be defined. The public sector, as cloud computing adopters, could set the requirements for standards in security, interoperability and data portability. As cloud computing is not restricted to the EU, international agreements on certain principles such as certification, data protection and security are needed. Research and development should improve the model considerably.

Conclusion: **Some references in the public consultation address security and privacy in cloud computing in a broader view. Specific recommendations on identity and access management in cloud-based services are not on the scope of the consultation report.**

3.3. EC Funding Programmes on IDM/AM along a Cloud-Based Service

The European Commission has been directing a great deal of funding efforts in the field of Cloud Computing. The content of this chapter is a short analysis of current public funded research programmes, the IDM/AM split and the targets of funding programmes on IDM/AM.

Overall, **62** public funding projects co-financed from the EU Commission were identified by EUROSMART in December 2011. The total budget was defined at round **600 Million €**. There were 35 publically funding projects running under STREP, 20 publically funding projects under IP, 5 public funding projects were under the Cloud Security Alliance, and 2 public funding projects working along the Competitiveness and Innovation Programme.

3.3.1. General Targets of EC Funding Programmes Along Cloud Computing

Most of the public funding programmes address the following aspects of Cloud Computing:

- Technology targets, e.g. interoperability, semantic, middleware, data storage, transport protocol, mobile application, infrastructure, tools etc.;
- Open source, open architecture, open network;
- Application-related services, e.g. intelligent cargo, medicine information cross barrier or border, energy consumption control;
- Security, e.g. virtualisation;
- Controlling and analysing new threats and vulnerability.

Many programmes deal with cloud performance, e.g. speed, services and availability. Some programmes are related to specific frameworks, such as Smart Cities[5].

[5] www.smart-cities.eu/

3.3.2. Identity Management Targets in EC Funding Programmes Pertaining to Cloud Computing

Six publically funding projects out of the overall **62 projects** address and/or touch aspects of IDM/AM; these are mOSAIC[6], BIVEE[7], CLOUD4all[8], TCLOUDS[9], SECFUNET[10] and NOVI[11]. These 6 projects represent a total budget of about **40 Million Euros**, which is around 6% of the overall public funding budget in the current cloud computing domain. Particular aspects of these projects are:

- User-profiling in cloud application;
- Personalised accessibility in a cloud computing network;
- Privacy protection on cross border infrastructure;
- Secure identification and authentication.

There is one specific funding project on IDM/AM for cloud services which began in 2011 in Germany, sponsored by the Federal Ministry of Economy, called SkIDentity[12].

A mainstream or guideline approach on IDM/AM is not observable with the 6 identified funded projects. No public funding project addressing only IDM/AM has been identified. The topic of IDM/AM typically takes on a "side aspect" in the project.

More than 10 EC funding projects are running under the seventh Framework Programme for Research and Development (FP7) with the scope on electronic identity management. Some examples include ENDORSE, EuroPrise, FIDIS, GINI-SA, PRIVACYOS, PRIME, PrimeLife, TAS, ABC4Trust, EVITA, PICOS and TDL. These projects account for more than 50 Million Euros. An explicit scope on IDM/AM to capture privacy and security in cloud services has not been found.

Conclusion: **The analysing of public funding programmes in the cloud computing domain co-financed from the EC indicates that IDM/AM do not take an important place on the priority list of EU funding streams, such as FP7. This is surprising, because in the past many very efficient and successful "inner" attacks were made in cyberspace that may not have been possible if sufficient research funding had been made available.**

Inner attacks pertain to users, who are working in or with the ICT-Network. Many examples of successful attacks from inner attackers are well known - for example in critical infrastructures. In the cloud computing domain as the number of users in the ICT-Network increases so consequently does the probability of inner attacks. If cloud computer networks work with person-related information, new threats are predictable.

6 www.mosaic-project.eu
7 www.bivee.eu
8 www.cloud4all.info
9 www.tclouds-project.eu
10 www.secfunet.eu
11 www.fp7-novi.eu
12 www.skidentity.com

3.4. Statements/Recommendations of Industry Associations on IDM/AM along Cloud-based Services

3.4.1. Worldwide

Four main bodies are playing a significant role in identity & access management in the cloud environment, these are OASIS[13] , Kantara[14], OpenID[15] and oAuth[16]. These bodies have already defined largely used protocols around identity management, such as SAML & oAuth, to secure access management in the cloud environment.

- OpenID has played a role in the identity federation at early stage, but is now moving to some convergence with oAuth.
- The Kantara Initiative (ex Liberty Alliance) has issued numerous protocols and has innovated with the User Managed Access (UMA) approach, which breaks away from the major schemes used today in authorisation management.
- oAuth/IETF is becoming a major influential body in the credential flow around the cloud and in a multi-actor context.
- OASIS is a non profit Organisation that drives the development, convergence & adoption of open standards. A technical committee “OASIS Identity in the Cloud” works on standard evolutions for identity in/from the cloud.

All these entities recognise the need of trust frameworks that allow the trust to be established and controlled among multiple entities. Trust Frameworks cover both legal and technical aspects. Several trust frameworks are already enforced in the US, such as the Kantara Initiative, Open Identify Exchange (OIX)[17] or NSTIC. The US Government has launched its own Trust Framework programme for achieving identity recognition across all administrations, for example. **No equivalent framework exists today in Europe**, but this is needed, in order to establish architecture of increased international trust & confidence and to ease open trusted market exchanges.

These trust frameworks also implement multiple Levels of Assurance (LoA) that should be standardised to allow trusted identity exchange or recognition within the trust frameworks. The Level of Assurance is a unit of measure of the level of confidence given by an authentication mechanism that the subject is really the one it pretends it is. This approach would also improve the user experience while accessing services by reducing the number/variety of authentication methods, letting the user select his preferred choice.

The “claimed based authentication” is an important movement, taking place in several bodies as well. The principal idea is to avoid a wrong identity by checking attributes. An example is the authentication of somebody being “above 18 years” to access some restricted sites, without the need to provide the identity “name” attribute in aim to keep the privacy of the subject.

There is an important need for an identity “verifier” that could confirm that an identity is really the identity it claims to be. This role could be enforced by federal or state governments. But some private sector activities, such as Google Street Identity, now complement this verification of “claims” that are necessary to validate some attributes.

[13] www.oasis-open.org

[14] kantarainitiative.org

[15] openid.net

[16] http://oauth.net

[17] openidentityexchange.org

An important topic in identity management for the cloud is the enforcement of controls (Mandatory Access Controls) at the different layers of services, or when services are accessed through “web services” or an Application Programming Interface (API). Signature schemes would help in increasing integrity checking, as well as the non-repudiation, required in most business transactions. The Kantara initiative has initiated the User Management Access that intends to give the control back to the user and change the way authorisations are managed: from application centric to user centric. This concept would, for example, permit the user to have access to all authorisations he gave independently of the service provider, and have the ability to easily audit and remove his unnecessary grants.

Another organisation focuses more on the compliance aspect: the Cloud Security Alliance (CSA). It works in coordination with ENISA on Cloud Security Risk & Compliance topics. After issuing an industry recognised document on Cloud Security Compliance best practices, the CSA is extending its scope. The concept of “Security as a Service” is refined, and revisions of the IDM/AM are starting in 2012. Implementation recommendations will be issued in a later chapter.

3.4.2. Europe

In Europe, activity on Cloud identity began in a very fragmented manner, within diverse organisations, and country by country, such as in France with ANSSI, Germany with BSI, and so on. One focus is on privacy concerns and Personally Identifiable Information (PII) concepts. The main focus of the European Commission is to watch data use and protect citizens, and their privacy.

The focus on the protection of employees and enterprise is not perceived as strong enough from the security industry point of view, and relies mostly on international practices that do not always match EU needs or laws. A new work item in the ETSI TC cloud has just begun and is focussing on “private sector user requirements” that will be centred on enterprise users, more than on citizens.

Conclusion: **Identity and access management are in the scope of industry alliances along cloud-based services to ensure privacy and security. New joint working groups between industry associations and government organisations are in place working on specific aspects of IDM as well as AM. However some recommendations are missing, e.g. international well-defined and accepted technical standards on ID management, role management and life cycle management. Access management should include strong authentication and identity verification.**

4. Possible solution

To avoid misuse and attacks, a clear IDM/AM architecture is needed. This should define the access rights of a user to person-related databank systems, the validity of access rights of user, the rights of a user to read and write person-related data, the user's rights to transfer person-related data, the rights to store person-related data in different media and the right to work with person-related data.

An entire IDM/AC framework should capture all changes to the roles and responsibilities of a user in the cloud computing domain.

In the knowledge that Cloud computing services are not stopped at any border in Europe, it is evident that it is up to the EC to define and publish European guidelines on IDM/AM. This could avoid the harmonisation issues which we have witnessed in electronic-ID documents on a national level, where we have 15 national programmes running today and the EU Commission has paid, between 2009 and 2012, more than 100 Million Euros for interoperability, with systems such as LSP STORK, LSP epSOS, LSP PEPPOL, EESSI, LSP eCODEX, HPRO and SPOCS.

5. Benefit to Public, Enterprises and Citizens

A European guideline in the near future could increase the internal Market in Europe and increase the trust for citizens, enterprises and the public sector with regard to data protection and privacy. This could be part of the Digital Agenda for Europe as well as the European Cloud Computing Strategy. This is becoming even more important for the public cloud, because to the contrary to the private cloud, where companies may impose their own security rules, the public cloud needs to have a common policy of digital ID management.

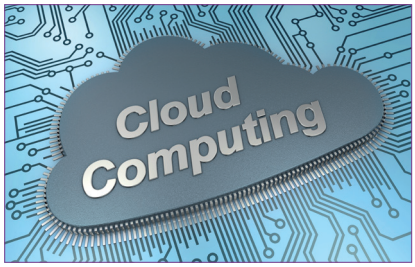
6. Risks

Missing EU guidelines and regulation foster national specific policies and guidelines in the 27 Member States, which deploys non-interoperability on security, privacy and data protection in Europe. Additional efforts are therefore required for interoperability on cross-border cloud services regarding data transferral, data storage, data management and identity and access management, such as that which is made for eID cross border with STORK_1 and which will be needed in the near future with STORK_2.

7. Call for Action

For growth and job creation of the European internal market, a flourishing cloud computer service is essential. For the reduction of administrative costs in the public domain, cloud services are also key. Many applications in the cloud domain deal with person-related data, where privacy and security are vital. International standards on electronic authentication and strong authentication in the digital world are available. The ICT network in Europe is growing, and more services are moving into the digital world.

Network complexity is growing. More and more users are involved.



For European users, a single identity cannot access multiple services. Their online experiences need to be separated into different domains in such a way as to retain their «privacy» in each field. On the other hand, managing multiple identities can be seen as a penalty, with federated identity seen as a service to reduce complexity.

For the ID providers, human behaviour analysis is perceived as a value, and this can be a threat to the user's privacy, if links are made between multiple domains, voluntarily separated by the user. EU legal authorities may enforce a rule to forbid the links between domains that may be used to identify persons without their consent.

It is similar to the CNIL approach in France where database contents cannot be linked together between domains (for example ministries), without previous declaration and agreement.

Legislation may also enforce the "Big Data" protection by allowing the consolidation of "anonymised" data only, and enforce the impossibility to retrieve individuals from these consolidated datasets.

EUROSMART believes identity and access management are fundamentals to privacy and security. The issue is even bigger in the public cloud, because in the private cloud, companies will have the possibility to impose their own security rules. Interoperability across EU and to the international world is requested. Pan-European interoperability of electronic identities based on 2-factor authentication where shown, e.g. in STORK and PEPPOL. The time is coming when a European guideline, as a holistic approach to privacy and security, should be defined. This should capture all relevant applications fields, like services in health, social, pensions, municipal, banking, insurance and even those of one's Internet provider. Many initiatives of the EU Commission are in the pipeline, such as the Digital Agenda for Europe, the European Cloud Computing Strategy and the proposed Regulation "on electronic identification and trusted services for electronic transactions in the internal market". Some synthesis is however missing.

EUROSMART recommends that attributes, credentials and strong authentication should be well defined, as should be the case for role management and life cycle management. The European Commission should define a comprehensive guideline on identity and access management to increase the confidentiality of cloud computing based services and their related privacy and security, in particular for the public cloud. The security of solutions shall be evaluated and certified according to Common Criteria (ISO 15408).

8. Glossary

AM	Access Management
ANSSI	Agence Nationale de la Sécurité des Systèmes d´Information
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Ministry)
BIVEE	Business Innovation and Virtual Enterprise Environment. Coordinator: Telemetry Association Ltd, South Stoke, UK;
CIP	Competitiveness and Innovation Program
CLOUD4all	Cloud platforms Lead to Open and Universal access for people with Disabilities and for All. Coordinator: Technosite, Madrid, Spain;
CNIL	Commission Nationale de l'Informatique et des Libertés
CSA	Cloud Security Alliance
CSA	Coordination and Support Action
CSP	Cloud Service Provider
DAE	Digital Agenda Europe
DNI	Documento Nacional de Identidad (Spain)
EC	European Commission
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
EU	European Union
FP	Framework Program
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies

IDM	Identity Management
IP	Integrated Project
ISO	International Standardization Organization
LSP	Large Scale Pilot
mOSAIC	Open Source API and platform for multiple Clouds. Coordinator: Seconda Universita di Napoli, Italy;
NIST	National Institute for Standarization and Technology (USA)
NOVI	Network innovations Over Virtualized Infrastructure; Coordinator: National Technical University of Athens, Greece;
NPO	Non Profit Organization
NSTIC	National Strategy for Trusted Identities in Cyberspace
OASIS	Open Advancing Standards for the Information Society
OIX	Open Identity Exchange
PEPPOL	Pan-European Public Procurement Online
PaaS	Platform as a Service
PII	Personally Identifiable Information
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SECFUNET	Security for Future Networks. Coordinator: Laboratoire d'informatique de Paris, France;
STORK	Secure Identity Across Borders Linked
STREP	Specific Target Research Projekt
TCLOUDS	Trustworthy Clouds Privacy and Resilience for Internet-scale Critical Infrastructure. Coordinator: Technicon, Graz, Austria;
UMA	User Managed Access

9. Appendix

Cloud computing related public funding projects of EC - status 12/2011

Cloud4SOA, Cloud-TM, Contrail, CumuloNimbo, FI-WARE, I2Web, INDENICA, MOSAIC, OPTIMIS, SLA@SOI, SRT-15, VISION Cloud, Webinos, EuroCloud, Release, IOLanes, iCargo, ADVENTURE, BIVEE, BUTLER, CALIPSO, ebbits, ExtremeFactories, GloNet, iCORE, IoT6, IoT@Work, IoT-A, MSEE, NEFFICS, OpenIoT, CLOUD4all, Sim-e-Child, VPH-Share, p-medicine, GAMES, FIT4GREEN, ALL4GREEN, COOLEMALL, POLYSYS, GALACTICO, PLATON, NAVOLCHI, FIREFLY, SAIL, GEYSERS, TRILOGY, EGI-InSPIRE, StratusLab, VENUS-C, EDGI, SIENA, TCLOUDS,SECFUNET, PASSIVE, ANIKETOS, SPACIOS, NOVI, iCity, EPIC, BONFIRE, OFELIA, OPENLAB.
This list may not be exhaustive and many new programs should be launched.

Authors

Didier Chaudun
Detlef Houdeau
Jean-Marc Lambert
Ingo Liersch

About Eurosmart

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, developing Smart Security standards and continuously improving quality of security applications.

Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers who work into dedicated working groups (communication, marketing, security, electronic identity).

Members are largely involved in research and development projects at the European and international levels.

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry".

Eurosmart members are companies (Austria Card, EM Electronic Marin, FNMT-RCM, Gemalto, Giesecke & Devrient, Infineon Technologies, Inside Secure, LFoundry, Morpho, NedCard, NXP Semiconductors, Oberthur Technologies, Prooftag, Renesas Electronics, Samsung, STMicroelectronics, Toshiba), payment systems (GIE Cartes Bancaires, Mastercard), laboratories (CEA-LETI), research organisations (Fraunhofer AISEC), associations (Smart Payment Association, Mobismart, Danish Biometrics) and independent experts (Michel Koenig, Jonas Andersson).

EUROSMART
The Voice of the Smart Security Industry

Contact us:

EUROSMART
Rue du Luxembourg 19-21
B-1000 Brussels
Tel. (+32) 2 506 88 38
Fax. (+32) 2 506 88 25
Email : eurosmart@eurosmart.com
Visit our website ! www.eurosmart.com