Summary Report

Report # 1

"Security Challenges of Cross-Border Use of Cloud Services under Special Consideration of ENISA's Contributions"

COINS Summer School 2015 on Could Security

Prepared by:
Nabeel Ali Albahbooh

Ph.D. Student in Information Security Field
Norwegian Information Security Lab (NISLab)
Gjøvik University College (GUC), Norway
nabeel.albahbooh@hig.no

Course: IMT6003, COINS Summer School
Instructor: Dr. Hanno Langweg
hanno.langweg@hig.no

Submission Date: 21st September 2015

Table of Contents

1. Executive Summary

Cloud computing is an emerging concept and its main goal is to deliver on-demand services over Internet, from a remote location, rather than on user's desktop, laptop, mobile device, or even on an organization's servers. In other words, cloud computing is a combination of multiple computing entities, globally separated, but electronically connected. A service provider can deliver its applications, computing power and storage services via the web. Thus, cloud computing becomes a location and device independent, in a sense that it does not matter where data is hosted nor where processing is performed.

In general, cloud computing can be spilt into three types: infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), and each type composes of different assets as shown in Figure 1.

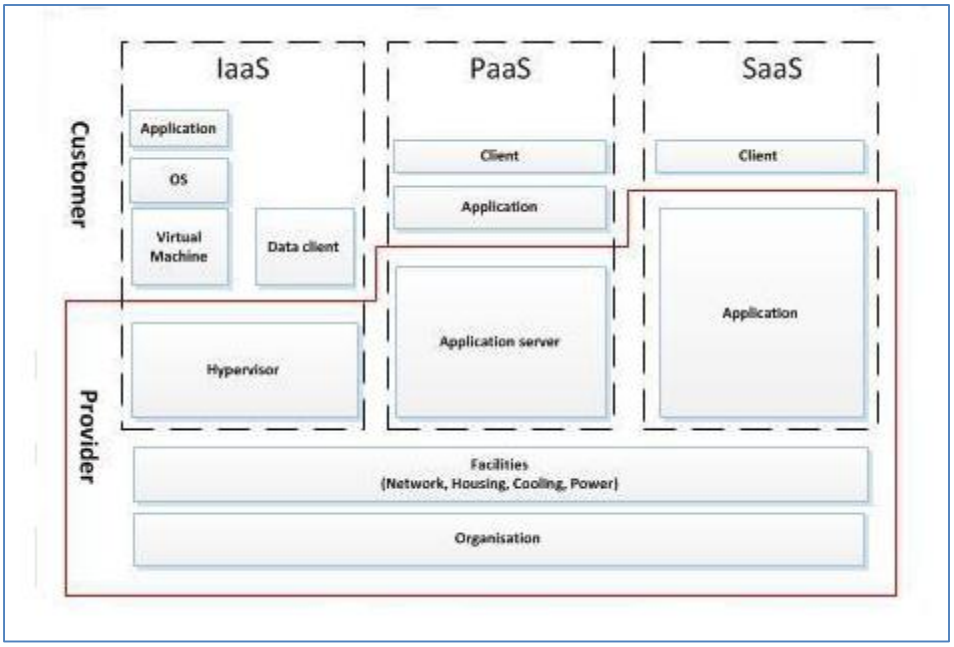

Figure 1: Cloud Types and Their Associated Assets [1]

The transfer of personal data across borders from one country to another leads to security challenges for cloud service providers as well as their users. These issues include agreeing on standards for the required data protection as well as the contractual rights granted to the cloud service providers. Furthermore, the required level of control and the clear of responsibilities in the context of cross-border cloud computing.

Cross-border clouds could be observed from two important aspects: privacy and data protection. The privacy refers to protection personal data while the data protection refers to aspect of privacy covering controls and countermeasures that govern the processing, storing or transferring of personal data. Moreover, other aspects might be considered such as: management/legal issues, interoperability, forensics, cryptography and authentication. However, due to the limitations of this report, we will focus only on cross-border cloud security aspects relevant to authentication.

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a center of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, ENISA facilitates contacts between the European institutions, the Member States and private business and industry actors.

This report explores the contributions of ENISA in regards to authentication security challenges in the context of cross-border clouds. In this report, we present some concepts relevant to Gov Cloud (discussed in Section 2) and CSSM (discussed in Section 3) that we believe they need to be considered while proposing any integration requirements between national and international clouds among different countries. The report shows that personal data protection, sharing critical information (explained in Section 4), security level of access and regulations are the major challenges that must be addressed and overcome to successfully design and implement a reliable, interoperable and secure cross-border authentication system. On the other hand, a better dialogue between governments, telecommunications operators and cloud service providers must be established to bridge the gap between various (or sometime overlapped) laws and regulations.

ENISA emphasis that a proposed cross-border system (described in Section 5) must be a heterogeneous with respect to technology; governed by two separate sets of laws; must not know all system participants [6].

2. Governmental Cloud (Gov Cloud)

ENISA defines a governmental cloud (Gov Cloud) as a centralized environment based on virtualization technologies, running services compliant with governmental and EU legislations on security, privacy and resilience. It uses a secure and trustworthy way to run services under public body governance. It builds and delivers services to state agencies, to citizens and to enterprises [2][5].

Before building a secure cross-border cloud between various EU countries, a secure Gov Cloud must be considered. Thus, ENISA proposes a logic security framework model for governmental clouds [2]. This framework is developed based on PDCA "Plan-Do-Check-Act) Deming model as depicted in Figure 2.

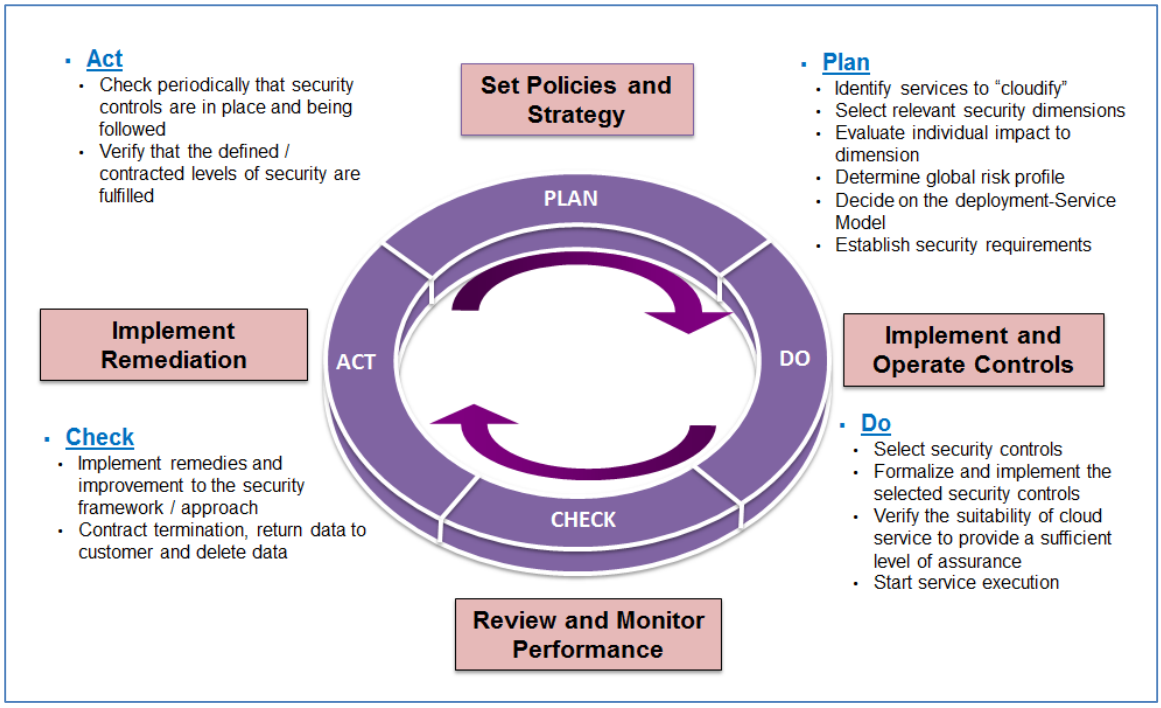

Figure 2: Gov Cloud Security Framework based on PDCA Model

3. Cloud Certification Scheme Metaframework (CCSM)

ENISA proposes a Cloud Certification Schemes Metaframework (CCSM) that maps detailed security requirements used in the public sector to describe security objectives in existing cloud certification schemes. CCSM provides more transparency about certification schemes and to help customers with procurement of cloud computing services. It is based on 29 documents with Network and Information Security (NIS)

requirements from 11 various EU countries (United Kingdom, Italy, Netherlands, Spain, Sweden, Germany, Finland, Austria, Slovakia, Greece and Denmark). It covers 27 security objectives, and maps these to 5 cloud certification schemes [3]. The main concept of CCSM is explained in Figure 3.

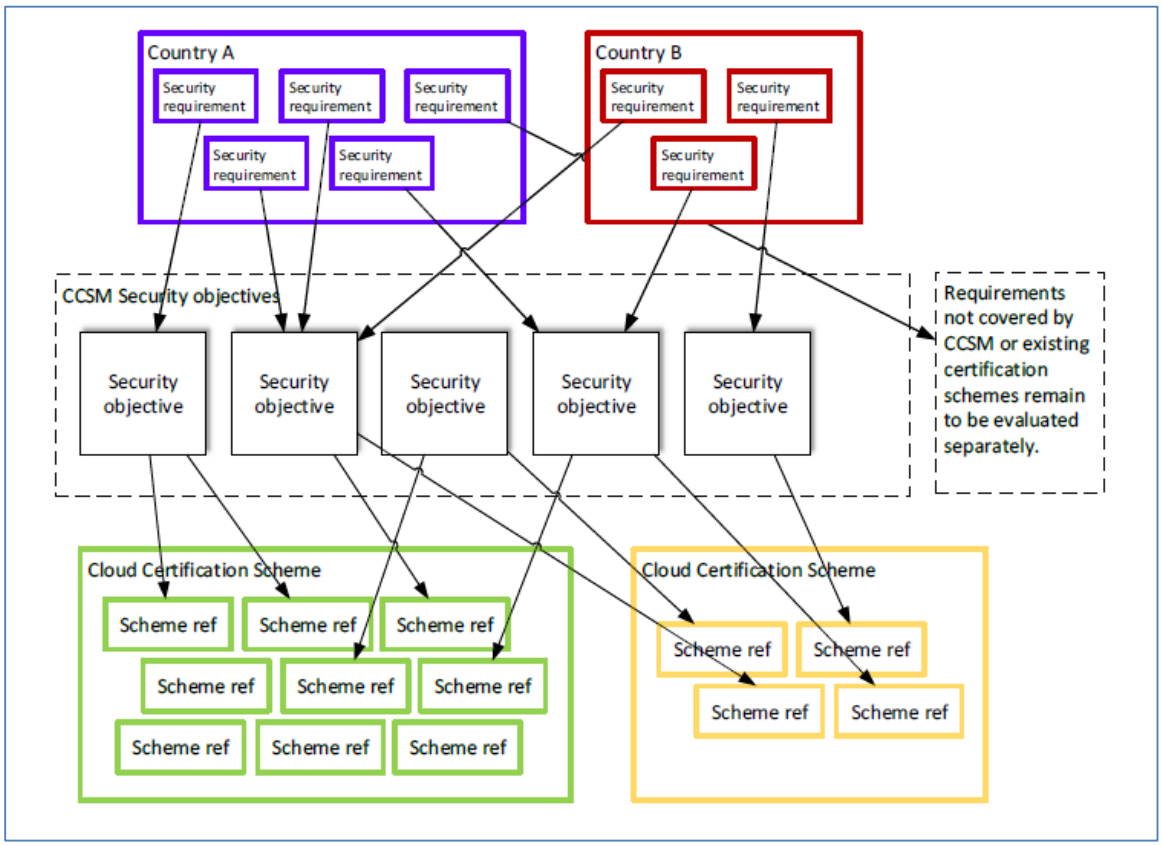

Figure 3: CCSM High Level Concept [3]

CSSM sets the requirements from both a customer side and a cloud server provider side. A customer needs to perform a due-diligence by checking the security requirements that meet the security objectives of the provider. On the other hand, a provider must fulfil the security objectives that are high-level goals without any technical explanations (e.g., an availability of 99.9%). Moreover, a provider needs to implement appropriate security measures "controls" in order to accomplish the required security objectives [3].

For simplifying the CCSM implementation, ENISA recently publishes the CCSM as an online tool to help customers with cloud security when buying cloud services.

4. Sharing Critical Information in Cross-Border Clouds

ENISA has published an intensive report about the challenges with sharing critical information (i.e., incident reports) between different clouds within EU countries. There is a couple of challenges with cross-border sharing of incidents. There is big concern relevant to legislative and regulatory concerns as some countries do not allow exporting data beyond their national borders. Furthermore, when a customer purchases a service from one country that is implemented using systems in a third country. In this case, it can be difficult to determine where such incidents should be reported. The jurisdiction might not be well understood by various countries. Another issue is that some incidents might affect national security in a certain country; and thus a trust across-borders becomes a problematic. On the other hand, the existing regulatory for each country introduces burdens on the integration between various national and international systems [4].

5. Authentication in Cross-Border Clouds

EU countries have started to look for an integrated and trusted authentication system that could be used as a cross-border solution. This solution provides public eGovernment services beyond national borders and extended to numerous group of national users. However, an intensive study needs to be carried out in order to assess and identify the security risks exist with such a solution, and then propose appropriate mitigations accordingly.

5.1 Authentication Model

Any proposed authentication model for cross-border clouds must consider the following aspects [6]:

- Establish a legal and contractual framework
- Identify EU citizens through appropriate credentials
- Authenticate system participants among different EU countries
- Provide secure and reliable online connections

- Solve the incompatibility issues between different and complex technologies
- Establish and agree on a common security policy

ENISA proposes a generic authentication model that could be used accord borders as illustrated in Figure 4.

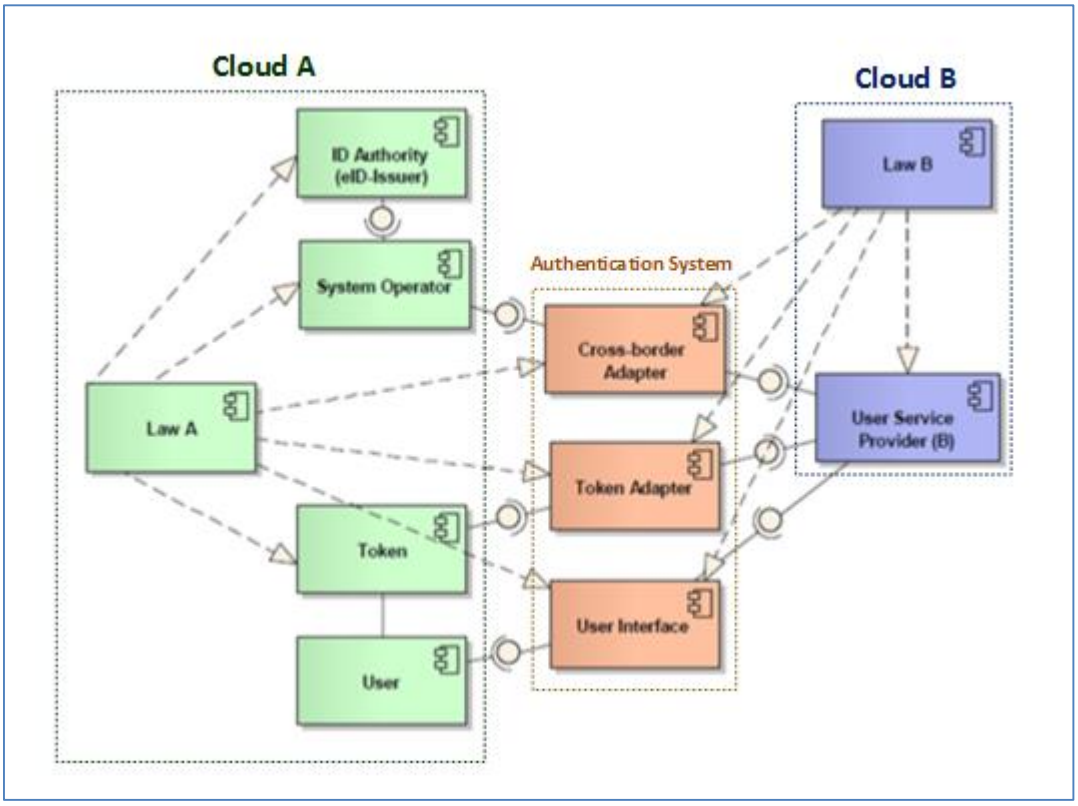

Figure 4: A generic Authentication Model for Cross-Border Clouds [6]

Cloud A reside in a country different than Cloud B. Let us assume that a user in Cloud B would like to access a service in Cloud A using his local credentials. The user service provider in Cloud B does not have a direct contractual agreement with system operator in Cloud A. The law in Cloud B governs only the local user service provider and cannot be enforced in any components of Cloud A (e.g., system operator). Both Cloud A and Cloud B have their own specific business rules.

Form the above assumptions, it is clearly that both Cloud A and Cloud B might deploy incompatible technologies with overlapping security policies. Furthermore, since each cloud has its own regulations, many security aspects need to be considered including cross-border data protection, liability and insurance. Therefore, a middle authentication system must be placed between Cloud A and Cloud B that plays a role of a cross-border

interpreter. In principle, it resolves the incompatibility burdens between different cloud setups.

Obviously, the authentication system consists of three main components: a cross-border adapter, a token adapter and a user interface. Table 1 summarizes the main function of each component [6].

No.	Component	Function
1	Cross-Border Adapter	It performs a middleware that proxies an authentication request from different countries. It translates data formats and business rules wherever necessary.
2	Token Adapter	It Interfaces a token from one country with a user service provider from another country. It establishes the compatibility of the token with the user service provider's systems.
3	User Interface	It provides a suitable interface between user service provide in a country with a user requesting a service in another country.

Table 1: Authentication System Components and their Functions

5.2 Security Challenges

There are some security challenges that need to be assessed for the proposed cross-border authentication system. These challenges can be dived into two main categories: technical security risks and legal issues.

In the technical security risks, there are some issue such as:

- **Personal Data** – Different types of credentials and their reliability may lead to falsified personal data and fraudulent tokens. Also, untrusted user service providers or cross-border adapters could withdraw, cache and misuse personal data.
- **Different Security Levels** – Different technical infrastructures, authentication protocols and procedures could led to a number of security vulnerabilities.
- **Attacks** – Various attacks such as man-in-the middle (MITM), illegal tracking of a user's location or behavior and denial of service (DoS).

On the other hand, there are some legal issues such as:

- **Personal Data** – The interpretation and implementation of data protection directive may differ between countries. Also, the restrictions on personal data transfer across borders may differ between countries (e.g., national IDs or more personal data is transferred than required).
- **Legal Obligations** – The liability insurance and damages in the context of legal obligations may differ between countries. Also, the liability of agencies may create complicated regulations.
- **Regulations** – National regulations may disallow authentication across borders (e.g., the usage or verification of the certificates in cross-border transactions).

5.3 Protection Requirements

The Business Impact Analysis (BIA) is an analytical process that aims to identify and highlight the violation of scope assets' Confidentiality, Integrity and Availability and the violations' impact on data from operational, financial, reputational and legal points of view.

Determining the protection requirements of the assets by analysis of the sensitivity of the data that the asset processes, stores and transmits as well as the critically of the data. Separate scales are assigned for each asset as described in Table 2:

Scale	Description
High	The impact of any loss or damage can attain catastrophic proportions.
Medium	The impact of any loss or damage may be considerable.
Low	The impact of any loss or damage is limited and calculable.

Table 2: Protection Requirements Scale

In the context of a cross-border authentication system, there are 9 assets need to be protected with a minimum value and least impact: personal data, application data, token, ID authority, system operator, user service provider, cross-border adapter, token adapter and user interface. These assets are subject to the following major damage scenarios:

- Confidentiality
    - Abuse of personal data for non-system purposes
    - Misuse of person-related data has effect on social or financial standing

- Integrity
  - Identity theft
  - Impaired performance of duties due to false data
  - Falsification of person-related data has effect on social or financial standing
- Availability
  - Impaired performance of duties
  - Increased cost of performance of duties
  - Unavailability of service has effects on social or financial standing of individual

ENISA assessed the above assets in terms of confidentiality, integrity and availability respectively as described in Table 3 [6].

No.	Asset	Confidentiality	Integrity	Availability
1	Personal Data	Medium	Low	Low
2	Application Data	Low	Low	Low
3	Token	Medium	Low	Low
4	ID Authority	High	High	Medium
5	System Operator	Medium	Low	Low
6	User Service Provider	Medium	Low	Low
7	Cross-Border Adapter	Medium	Low	Low
8	Token Adapter	Medium	Low	Low
9	User Interface	Medium	Low	Low

Table 3: Assessment of Protection Requiremens for Assets

An ID authority is the source of the electronic identity based on the person's personal data. It can be a health insurance register or a civil register which establishes the root of all personal data for the application.

We notice that the ID authority is considered as the most sensitive asset within the cross-border authentication system. It has the highest scale "High" in terms of confidentiality and integrity. The confidentiality concern of ID authority refers to disclosure of large amounts of personal data of registered persons would cause significant, nation-wide loss of reputation. If the integrity of the registers is corrupted, severe issues of liability may arise and trust in the system may be catastrophically compromised. For the availability, however, it has the "Medium" scale which means that the acceptable

downtime is up to 24 hours. Longer downtime may impair the reputation and the performance of duties significantly.

Moreover, we notice that all assets have the lowest scale "Low" in terms of integrity and availability (except ID authority). A "Medium" scale was assigned to the confidentiality of all assets (excluding application data = "Low" and ID authority = "High"). This means that more protection requirements need to be considered for the confidentiality aspects of all assets rather than the integrity and availability.

We must note that the assessment of the protection requirements for each asset will solely depend on the application type that needs to be accessed and its criticality requirements.

6. References

[1] ENISA, "Cloud Security Guide for SMEs, Cloud Computing Security Risks and Opportunities for SMEs", April 2015.

[2] ENISA, "Security Framework for Governmental Clouds, All Steps from Design to Development", February 2015.

[3] ENISA, "Cloud Certification Schemes Metaframework", November 2014.

[4] ENISA, "Cloud Security Incident Report, Framework for Reporting about Major Could Security Incident", December 2013.

[5] ENISA, "Good Practice Guide for Securely Deploying Governmental Clouds", November 2013.

[6] ENISA, "Security Issues in Cross-Border Electronic Authentication, Risk Assessment Report", February 2010.