

---

## - Master-/Bachelorarbeit - Adaptive Authentication for the Cloud

---

### Background

Nowadays the growing usage of Cloud-related technologies has become evident. However, its [associated security issues are still a major “show-stopper”](#) in sensitive areas like e.g. eHealth and eGovernment. The necessity of creating secure and trusted Cloud services has resulted in a central question: [how to objectively and quantitatively measure the security of the mechanisms and procedures implemented by a Cloud Service Provider?](#)

On the other hand, security metrics have become an enabler for a new IT paradigm known as [“Adaptive Security” –AS-](#). An AS-enabled mechanism, is able to change its behaviour (e.g. secret-key length, encryption algorithm, firewall rules, ...) according to the measured security level, therefore allowing the system to protect itself from security attacks. Consequently, [authentication systems built under the AS principle \(a.k.a. AS-AuthN\)](#) are able to change their identification mechanism (e.g. from username/password to X.509 certificates), according to the incoming connection’s security- or risk-level. [AS-AuthN is a promising approach for Cloud-based Identity Management](#), which is nowadays a hot topic in academia and industry.

### Tasks

Within this topic it is expected to propose the security metrics and associated methods to enable an AS-AuthN service for the Cloud. As a proof of concept the candidate should develop a prototype of the proposed system using e.g. an open identity framework like [“Higgins” \(http://www.eclipse.org/higgins/\)](#). Based on the proposed metrics (e.g. IP geo-location, requested asset’s value, IP reputation, ...), the AS-AuthN should be able to “re-authenticate” the used based on available modules (e.g. X.509 certificates, Attribute-Based Credentials, etc.).

This work is expected to contribute to the state of the art technology being developed by the EU-funded project [ABC<sub>4</sub>Trust](#). Also, we offer to the candidate further involvement with specialized organizations, in particular the [Cloud Security Alliance](#).

### Prerequisite

- The candidate should have knowledge of IT security (preferably related with authentication and identity management).
- Because this topic involves the development of a proof-of-concept prototype, then the candidate should also have good Java programming skills (Web Services programming is a plus).
- Motivation to work within international work groups on Cloud security.
- The thesis has to be written in English
- Immediately

### Start

### Contact

**Dr. Jesus Luna , Dipl.-Wirtsch.-Inform. Hamza Ghani**

{jluna|ghani}@deeds,informatik.tu-darmstadt.de

06151–16 - 5359/3414

S2|02 E206