

# IT DEPENDS ON THE CONTEXT: HOW GOOD DOES AUTHENTICATION NEED TO BE?

Not only people but also apps and things access information today. That makes the issue of security more important than ever.

*by Martin Kuppinger*



The IT security directives of many companies state that content with a higher classification such as «confidential» may only be used with two-factor authentication. But in a world where more and more users are accessing applications, systems and therefore content with a wide variety of devices, such requirements have long since become inadequate.

## Security is no longer purely an issue internal to companies

The traditional focus of information security was on employees accessing internal systems. Yet the scenario has changed fundamentally in the last few years. Applications no longer run just in the internal data center but also in the cloud. More and more applications are not only being opened up to business partners but to customers as well. Long since has access not been just from desktop PCs but from numerous devices at many different locations, often over WLANs accessible to the public. Apps working over what are known as APIs (Application Programming Interfaces)

---

## About KuppingerCole

*KuppingerCole, founded in 2004, is a global analyst firm focusing on Information Security and Identity & Access Management (IAM). Governance, Risk Management and Compliance (GRC) is another core area of KuppingerCole research. KuppingerCole as an independent analyst group organizes conferences, seminars, workshops and webcasts in the fields of information security, IAM and GRC. It also hosts the European Identity & Cloud Conference, which has established itself as the main event for opinion leadership and best practices for Identity & Access Management, Cloud and Digital Risk in Europe.*

---

are increasingly being used as well. These APIs are gaining importance for integration into the Internet of Things (IoT) and for net-working business processes between companies.

## MORE AND MORE APPLICATIONS ARE NOT ONLY BEING OPENED UP TO BUSINESS PARTNERS BUT TO CUSTOMERS AS WELL.

In other words: There is more and more access as time passes, not only by people but also by things, apps and other systems. Information needs to be protected, even in this complex IT reality. Access needs to be adequately authenticated and authorized. Authentication has to determine whether the communication partner is the person, system or thing it purports to be. Authori-

zation is about the decision what system and information access to grant in concrete terms.

It is apparent that the basic differentiation between less critical with simple authentication, typically with a username and password, and critical with two-factor authentication is no longer sufficient in this environment. Things can and have to authenticate themselves differently than people, for whom in turn the device they are using is a factor in determining how authentication can actually be realized.

#### The balance of two aspects is decisive

How strong or weak authentication should be depends on the balance between two aspects. One aspect is the context in which access takes place: What device is being used? Where is it being used? Is the installed anti-malware current? What networks are being used? Are there any indications of abuse? We are talking about the risk associated with access. This risk may be greater or lesser, depending on the context.

### SO THERE IS NO RIGHT OR WRONG, BUT ONLY APPROPRIATE AUTHENTICATION.

The other aspect is the risk that is acceptable for an interaction or transaction. This requires a differentiated understanding of risk, which goes beyond the classification of documents, data or applications.

Furthermore, very different methods have to be supported depending on the access channel. When a user accesses a cloud service through an app, different methods and standards apply than when an employee accesses internal business applications from a notebook.

Authentication has to take the context into account. There is no right or wrong, strong or weak authentication, there is only appropriate authentication. Common two-factor authentication with a Smartcard or OTP Token may be insufficient for highly critical transactions.

#### High time to rethink the approach

Companies need to adapt their strategies, rules and implementation for authentication and authorization to the changed reality. Directives have to become more flexible and must be based on concrete risk. Practical methods to determine risk are needed. Various authentication methods have to be enabled to provide flexible support for different devices. Authorization needs to become variable. More or less may be permitted depending on authentication.

This requires new directives and concepts, but also flexible applications that integrate different authentication methods and standards in addition to supporting a broad range of use cases. It also means that applications must be able to work in a context and make their authorization decisions based on the authentication strength as well.

### IT IS HIGH TIME TO RETHINK AND MODERNIZE APPROACHES FOR THE OPTIMUM PROTECTION OF INFORMATION.

It is high time to rethink and modernize existing approaches for the optimum protection of information. This applies all the more since the risk of attacks has increased massively in recent years and no end to this trend is in sight. Where this journey to adaptive authentication and authorization under consideration of context information will lead was a topic avidly discussed at the European Identity Conference 2015 held in Munich, Germany this May (cf. [www.id-conf.com](http://www.id-conf.com)). ■

---

## Imprint

#### Publisher:

AdNovum Informatik AG  
Corporate Communication  
Röntgenstrasse 22  
8005 Zürich  
Phone +41 44 272 6111  
E-Mail [info@adnovum.ch](mailto:info@adnovum.ch)  
[www.adnovum.ch](http://www.adnovum.ch)

#### Responsibility and editing:

Andrea Duttwiler  
Feedback: [notitia@adnovum.ch](mailto:notitia@adnovum.ch)

#### Design and realization:

Comuniq, Zürich

#### Photography:

Gerry Nitsch, Zürich  
Printed on Balance Pure

