v1.1 | 10 09 2019

Key Cloud Principles

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INDEX

SUMMARY

With over 10 million active users in the Netherlands, United Kingdom, Germany, France and US, Tools4ever is one of the Identity and Access Management market leaders. We serve a wide range of organizations varying in size from 300 to more than 200,000 user accounts.

Over the recent period, Tools4ever has migrated its HelloID offering from a hybrid model - in which we also offered private cloud and on-premise deployments - towards a cloud-only solution which runs on the Microsoft Azure cloud infrastructure. It is a step in our roadmap towards a cloud-only solution provider.

In this document we explain the drivers behind this migration, our approach and the customer benefits.

Drivers for the cloud-only migration

Cloud technology – and specifically Infrastructure-as-a-Service offerings as used by Tools4ever - has reached maturity. Gartner positions IaaS very close to the ultimate 'plateau of productivity' on their cloud computing technologies hype cycle, while cloud surveys from e.g. RightScale illustrate that today already 96% of all companies use the cloud. The majority adopted a public cloud strategy and public clouds are already in use at 92% of the companies. On average, organizations make use of 4.8 different cloud offerings over the full range of private, hybrid ad public services.

Also Tools4ever customers are rapidly migrating their IT landscape to the cloud. Often the key driver behind this is the wish to be more flexible and adaptive, but also cost-efficiency and a focus on core business operations are important drivers. As part of that strategy they also demand our Identity and Access Management solutions to be cloud based.

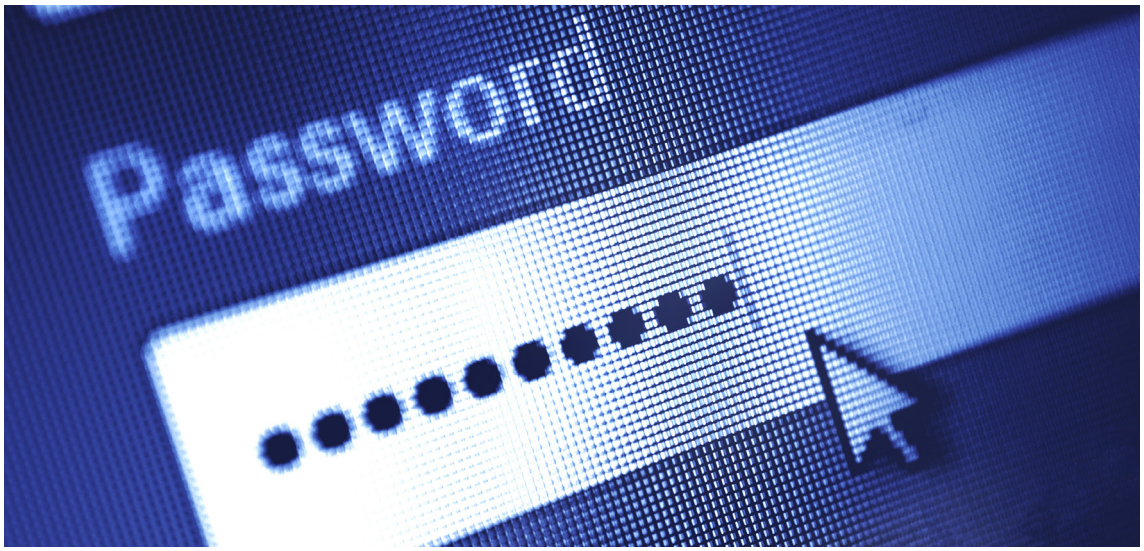
IaaS offerings offer advanced capabilities

Given these demands and our firm believe in cloud technology, we started upgrading our Identity Governance & Administration solutions from on-premise towards a cloud-enabled portfolio. HelloID was our first implementation of a 'cloud-first product'. It is fully designed, developed and tested for public cloud deployment, a milestone for Tools4ever.

Until recently we also supported HelloID for on-premise and private cloud installations. We experienced however that our Azure public cloud facilities increasingly outgrow today's on-premise and private cloud capabilities. Therefore, maintaining a combined on-premise and public cloud offering is no longer a sustainable option. Not from a professional solution management point of view and not from a customer point of view. It is therefore that we decided to discontinue the on-premise and private cloud offerings and focus all our expertise on accelerating the public cloud roadmap for HelloID.

Is a public cloud solution reliable and secure?

Although the cloud is widely adopted, it is still worthwhile to reconfirm the current maturity



level with respect to availability, reliability, security and data protection. Our cloud partner Microsoft Azure is internationally recognized as a global market leader and has deployed a cloud infrastructure that fully covers global and local demands. By leveraging their leading and well-structured topology of Geographies, Regions and Availability Zones, we can guarantee our customers the highest levels of data resilience. Today, the Azure public cloud is already used for many business-critical solutions like e.g. core banking applications.

Solutions which are certified and verified

The compliance of both Microsoft Azure and Tools4ever to international standards are documented where possible with the applicable certifications. As important is however our strict verification policy. Tools4ever considers pro-active and frequent testing of our security solutions as a cornerstone of our success.

We run an in-house program in which our own solutions are frequently tested on potential security flaws by our own experts. However, that is only our first line of prevention. In addition, we have our software solutions tested twice a year by top-class external ethical hackers of Deloitte, the international market leader in information security. These external tests keep us sharp, prevent the occurrence of blind spots and provide us with an extra pair of eyes. The external ethical hackers look at IT systems from the point of view of experienced cybercriminals, to recognize vulnerabilities that others might overlook. They use for example the NCSC ICT-B v2 guidelines and the OWASP Top 10 Application Security Risks of 2013 and 2017.

About this white paper

In this whitepaper we discuss our cloud strategy in more detail. We explain our vision on cloud maturity and security and translate that vision into the design, development and deployment of our solutions. Specific details about the architecture and design of the solutions - like HelloID - will be addressed in separate security white papers per solution.

In this white paper we elaborate on 4 questions:

1. What is the state of the cloud? How mature is the technology and what is the adoption level of cloud solutions?
2. How does our Infrastructure as a Service cloud provider (Microsoft Azure) guarantee business critical requirements in areas like reliability, security and data protection?
3. What design, development and operational principles does Tools4ever deploy to guarantee an optimized reliability, security and data protection for our IDaaS offerings that run on Azure?
4. How is the quality of the combined Azure/Tools4ever certified and verified by independent parties in the market?

CURRENT STATE OF THE CLOUD

Today, the cloud is widely adopted as the main IT deployment scenario. Still, executives do have concerns, which is logical at the brink of a transformation where the full IT landscape of companies is migrated from on-premise towards an external environment. An external IT environment managed by external staff while in parallel own IT resources are reduced. Concerns do include security and closely related to security, data management. Though, also vendor management raises concerns. Let's start with a summary of the current 'state of cloud', as well as the main challenges that customers do experience and foresee.

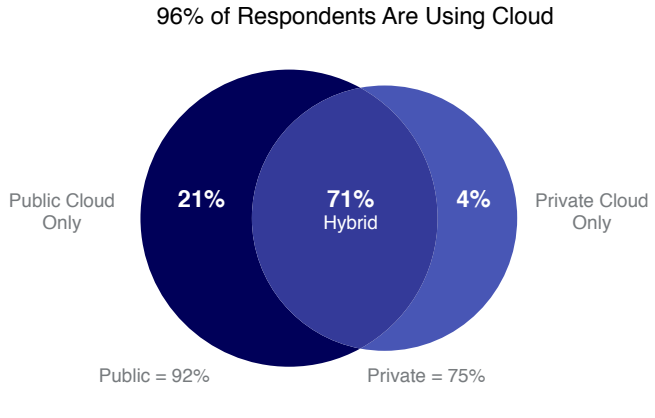
Current cloud adoption

One of the most commonly used indicators to define the 'maturity' of new technology, is the Gartner Hype Cycle. It shows the development path of technologies through several well-defined stages from the phase of innovation via a peak of inflated expectations and a subsequent disillusionment period to the phase in which a technology is widely accepted and delivering all promises. In the most recent Gartner Hype Cycle for cloud computing technologies [1], Infrastructure as a Service (IaaS) on which we deploy our security solutions was already about to reach the plateau of productivity.

This analysis is backed by quantitative analyses of the current cloud deployment. The current situation with respect to the adaptation and use of cloud solutions is well-described in the annual State of the Cloud Report from RightScale [2]. Researchers surveyed 997 technical professionals across a broad cross-section of organizations about their adoption of cloud computing. Main conclusion could be that it is not so much if companies are adopting cloud, but how many cloud solutions they will use in parallel.

96% of the respondents indicated that their organization make use of cloud services. These can be private clouds, publics clouds and hybrid deployments in which both types are combined. Public cloud adoption increased to 92% and private to 75%. Many respondents indicated that their public cloud strategy has top priority.

This is not restricted to specific niche applications or basic tools with limited integration demands, like email or storage. Today, also core business applications with substantial integration requirements like complex ERP and CRM solutions are delivered from the cloud.



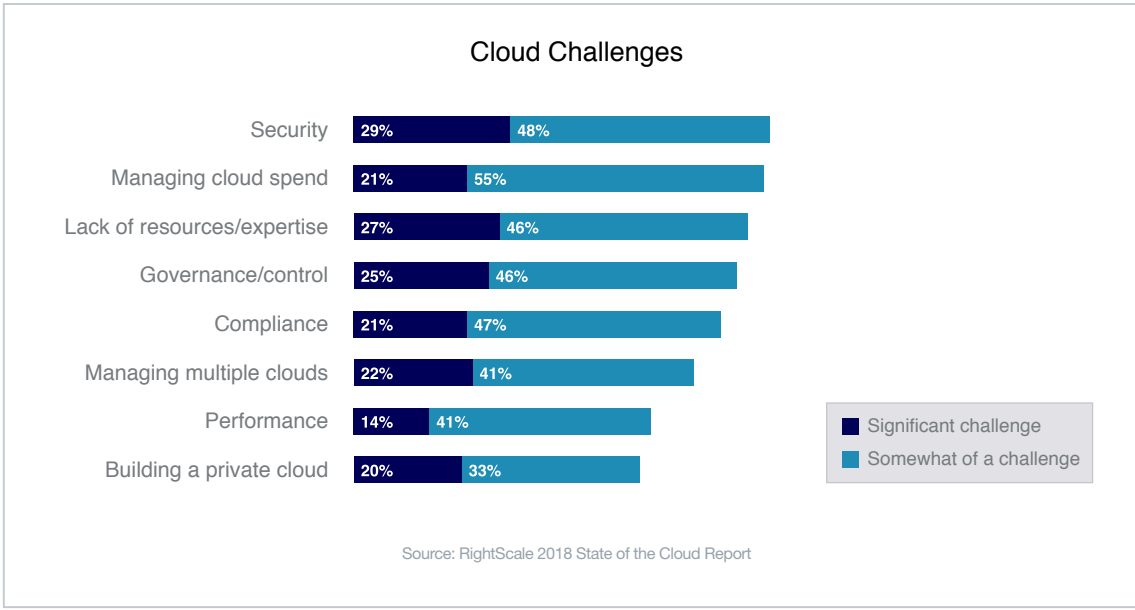
Source: RightScale 2018 State of the Cloud Report

From single cloud to multi-cloud

So, it is no longer a question if the market is adopting the cloud. In 2018 the question is more how many cloud services are used. According to the cloud survey, organizations on average leverage 4.8 clouds across both public and private. In an average company, 3.1 cloud environments are used to run applications, the other 1.7 are used for experimenting.

Key challenges for cloud deployment

The fact that the cloud is now widely adopted, does not mean that cloud migrations are without challenges.



As expected, security is a top challenge for the respondents of the survey. There is however an important observation. First, although security and other topics are mentioned as challenges, the majority sees them as 'a' challenge, not a significant challenge. They are considered hurdles which can be taken. Certainly at larger organizations with more cloud experience and knowledge, security is often considered less of a problem compared to topics like cost management and resourcing.

An expert view on cloud security

This is backed by the confidence of experts that the cloud indeed ís secure. In the opinion of Gartner's security practice, security issues with respect to cloud services have mainly to do with human processes around them :

> *"The challenge exists not in the security of the cloud itself, but in the policies and technologies for security and control of the technology. In nearly all cases, it is the user — not the cloud provider — who fails to manage the controls used to protect an organization's data" [3]*

Gartner even quantifies this by stating that through 2022 they expect at least 95% of cloud security failures will be the customer's (i.e. the customer of the cloud provider) fault. They also claim that through 2020, public cloud Infrastructure as a Service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centers.

It is an observation we at Tools4ever can support from a qualitative point-of-view. For example, systems managers have high-level authority, they have the technical knowledge and they even know the technical access details like the IP address of SQL clusters. The impact of a simple mistake or a vindictive ex-employee could be disastrous. Something for which cloud service provider are in general better prepared than in-house IT departments.

Also relevant is the McAfee Cloud Security Survey [4], where already 83% of 1400 interviewed IT decision makers confirmed that they store sensitive data in the public cloud.

Security services are moving to the cloud

Even more interesting is what analysts say about the delivery of security services from the cloud. During Gartner's Security and Risk Management Summit in June 2018, Gartner research vice president Peter Firstbrook discussed several security trends [5]. One of the trends he highlighted was the fact that security itself moves to the cloud. Firstbrook explained that enterprise security organizations are overloaded by the maintenance burden of legacy security solutions. At the same time, cloud-based security products appear to be more agile. They can adopt new detection methods and security services faster than on-premise solutions.

It is something Tools4ever experienced first-hand in our co-operation with our cloud infrastructure partner Microsoft Azure. Until recently we also supported HelloID for on-premise and private cloud installations. We experienced however that our Azure public cloud facilities increasingly outgrow today's on-premise and private cloud capabilities. Therefore, maintaining a combined on-premise and public cloud offering is no longer a sustainable option. Not from a professional solution management point of view and not from a customer point of view. It is therefore that we decided to discontinue the on-premise and private cloud offerings and focus all our expertise on accelerating the public cloud roadmap for HelloID.

Conclusions

If one message is clear from the market, it is that cloud already years ago passed the phase of inflated expectations and unproven claims. Cloud services reached maturity and are used for mission critical IT services. Looking at the top challenges that executives defined, topics like security are considered challenges, but certainly not as show-stoppers. The migration of applications towards the cloud is in other words not an Elon Musk type of Mars-journey. It is the journey of a skilled driver throug Europe. It certainly requires the right materials, the right skills and the right planning. But given these preparations, it is one of the most reliable journeys on earth.

TOOLS4EVER CLOUD PARTNER: MICROSOFT AZURE

HelloID is hosted on Microsoft's Azure cloud computing platform. This platform can be used to host many types of services including webservers, databases, virtual machines and many more. Tools4ever has a long-standing Microsoft Gold Partnership and has built up specific security experience working with the Microsoft product suite. Microsoft has decades-long experience building enterprise software and running some of the largest online services in the world.

Microsoft Azure positioned as Cloud Infrastructure market leader worldwide

Under the leadership of Satya Nadella, Microsoft has made an impressive transformation towards a leading cloud player. In the most recent Gartner Magic Quadrant for Cloud Infrastructure as a Service, Microsoft is listed for the 5th consecutive year as one of market leaders worldwide, together with AWS and 'new entrant' Google [6]. Today, 90% of Fortune 500 companies make use of the Microsoft Cloud. For the well-known Office 365 service of course, but also for business-critical applications.

An example of a company which transferred their business-critical assets to Azure is Geneva-based Temenos AG [7]. Temenos provides banking software to 3,000 firms across the globe, including 41 of the top 50 banks. They daily processes transactions of more than 500 million banking customers. Temenos was listed in July 2017 as a Market Leader in the Magic Quadrant for Global Retail Core Banking. In the banking market of course strict security and compliance requirements are in place. The Temenos chief enterprise architect John Schlesinger explains:

> *"This is a traditionally on-premises industry in terms of core banking applications, but our view is that by 2020, all new core banking projects will be on infrastructure-as-a-service (IaaS) platforms, if not software-as-a-service platforms."*

He also confirms that from a security and compliance point of view, the Azure proposition is fully prepared for the extreme demanding financial business processes:

"From a security point of view, I think Azure is a demonstrably more secure environment than most banks' datacenters," and "From the compliance point of view, we already have the regulators in Europe allowing core banking on the Dublin datacenter."

Microsoft Azure global infrastructure and cloud security

Security is built into the Microsoft Cloud from the ground up, starting with the Security Development Lifecycle, a mandatory development process that embeds security requirements into every phase of the development process. The Microsoft Cloud is protected at the physical, network, host, application, and data layers so that their online services are resilient to attack. Continuous proactive monitoring, penetration testing, and the application of rigorous security guidelines and operational processes further increase the level of detection and protection throughout the Microsoft Cloud.

An essential element is the international topology of the Azure cloud. Azure is organized in Geographies, each of which consists of two or more Regions. Each Geography is a discrete market that preserves data residency and compliance boundaries (e.g. GDPR). So, customers with specific data-residency and compliance needs, can keep their data and applications close. Microsoft may replicate data to other Regions within that Geography for data resiliency but will not replicate or move customer data outside that Geography.

Geographies are not just defined at a supra-national level. In Europe, there are also smaller, independent geographies defined at several countries. France, United Kingdom and Germany Geographies within the Azure hierarchy. Azure Germany is a so-called sovereign offering, a physically and logically separate instance of services with a dedicated network between Germany datacenters. It is designed to meet the strictest EU data protection laws, under control of a German Data Trustee (T-Systems International GmbH, a subsidiary of Deutsche Telecom) and is only available for customers and partners in the EU and the European Free Trade Association (EFTA). And in the France Geography, the availability, resiliency, and business continuity are fully organized within France, using 2 Regions (France Central and France South).

Within a Geography, a **Region** is a set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. Most Azure services enable customers to specify the Region where their customer data will be stored. Microsoft may replicate this data to other Regions within the same Geography for data resiliency. As such, Geographies are fault-tolerant to withstand complete region failure through their connection via the dedicated high-capacity networking infrastructure.

54 regions worldwide **140** available in 140 countries

* Two Azure Government Secret region locations undisclosed

Finally, some regions (West Europe, North Europe and France Central) contains multiple **Availability Zones**. Availability Zones are physically separate locations and made up of one or more datacenters equipped with independent power, cooling, and networking. Availability Zones allow customers to run mission-critical applications with high availability and low-latency replication. For example, the France Central Region offers three availability zones.

Tools4ever by default offers its services via two Geographies, Europe and US. Other Geographies are available on request.

TOOLS4EVER SECURE CLOUD DEVELOPMENT AND OPERATIONS

So, cloud technology is mature and fully deployed at most businesses in Europe. Often for business-critical applications, including security and identity solutions. Cloud services today deliver the appropriate level of security and cloud maturity is such that security is most of the time in better hands with cloud providers than with isolated security team.

By partnering with Microsoft, we can leverage the top-ranked cloud capabilities of a partner which meets the highest standards for cloud services, security and data protection. But that doesn't mean that for our Identity-as-a-Service offerings, running on the Azure datacenters in Europe, we can sit on our hands. The central position of our solution in the customer's IT landscape forces us to also bring our own Tools4ever security design, development and deployment standards to the highest level.

In this chapter we explain which key principles we used by designing, developing and operating our IDaaS propositions.

The Tools4ever security design, development and deployment principles

The way we design, develop and maintain our solutions is based on a set of key principles, which we describe below. Foundation for our approach are the Security by Design Principles as defined by OWASP.

1	**Minimize attack surface area**	Our aim for secure development is to reduce the overall risk by reducing the so called 'attack surface area'. Every feature that is added to an application adds a certain amount of risk to the overall application.
2	**Establish secure defaults**	By default, we deliver a user experience which is maximally secure. It is up to the application user – within his or her mandate - to reduce the default level of security as configured in our applications.
3	**Principle of Least privilege**	Accounts by default have the minimal privilege required to perform the necessary business processes. This covers not just user rights but also resource permissions like CPU limits, memory, network, and file system permissions.
4	**Principle of Defense in depth**	Even when one control would be reasonable, we prefer more controls to approach risks in different fashions. This principle can make severe vulnerabilities extraordinarily difficult to exploit and more unlikely to occur.
5	**Fail securely**	An application may fail to process transactions for a variety of reasons. However, the result of such a fail determines whether an application is secure or not. If a user authorization check fails, but as a result assign admin rights to that user, this is an example of insecure failing.
6	**Don't trust services by default**	Third party partners will typically have differing security policies and posture than we. So, we don't use implicit trust of externally run systems and treat all external systems in a similar fashion.
7	**Separation of duties**	This is an essential fraud control and is part of our process flows as implemented in the solutions. For example, administrators should typically not be users of the application.
8	**No security by obscurity**	In our vision security of key systems should not just rely on hiding details. We consider this as a weak security control
9	**We keep security simple**	Our approach favors straightforward and simple code over overly complex approaches. No double negatives and complex architectures when they are not necessary
10	**Fix security issues correctly**	Once a security issue has been identified, it is important to develop a test for it, and to understand the root cause of the issue. When design patterns are used, it is likely that the security issue is widespread amongst all code bases, so developing the right fix without introducing regressions is essential.

How exactly we implemented these principles in our solutions, can be reviewed by your experts in the security white paper of each individual solution. However, they all are based on this foundation.

We are extremely proud that our efforts to design, develop and deploy truly secure solutions are recognized by peer industry experts. In 2017, Tools4ever won the Cybersecurity Excellence Awards in the Network Access Control category. Holger Schulze, founder of the 350,000-member Information Security Community on LinkedIn, which organizes the awards program explained:

> *"With more than 450 entries, the 2017 awards are highly competitive. All winners and finalists reflect the very best in leadership, excellence and innovation in today's cybersecurity industry."*

Our solutions are also tested twice a year by the security experts of Deloitte, as described in the next chapter.

Security and privacy. By design and by default

For many customers, a migration to the cloud does not only mean a move from an existing, trusted on-premise deployment to a new shared environment which they have to 'learn to trust'. It also means changes in the way they work. In the on-premise situation staff often had direct access to the solution database.

At Tools4ever we therefore receive questions and requests which often cover the full '180 degrees'. Some customers are concerned what happens if an unauthorized person could access the database (For example: "can someone access my cloud data and reset or export them using a Powershell script?"). At the same time we receive requests to provide direct customer access to cloud data and functionality.

We deal with these mixed demands in the following way, following our key design principles:

- We only open access to those functions and data which are indeed relevant for our customers (we 'minimize the attack surface').
- We offer a highly secured API for customers who needs direct access. Some solution providers don't offer API's for security reasons, but the simple truth is that every company sooner or later may come in the position where an API is required to support their business processes. So, question for Tools4ever is not if we offer an API (we do). It is how we protect this API.
- By default all security levels are set at their highest and at the same time the least necessary privileges are established. Also, we use in-depth security mechanisms. 2FA is supported and access to business-critical functions can be restricted to specific IP addresses.
- With respect to access procedures we maintain internally Tools4ever a strict separation of duties. We also advise this approach to our customers.

No one can guarantee that a solution is 100% safe. Such a guarantee would only be a proof of incompetence in an era where even security and intelligence organizations suffer from security breaches. What we can guarantee is that we leveraged the powerful arsenal of Microsoft Azure security tools to the maximum to provide our customers with an optimal reliable and secure identity solution.

CLOUD SERVICE VERIFICATION AND CERTIFICATION

The deployment of secure cloud solutions starts with using the right principles, technologies and partners, as we addressed in the previous chapters. However, for our customers this needs as much as possible verification and certification. Verification in which our cloud solutions are independently tested against clear security requirements and verification whether we comply with relevant standards are. Verification and certification are therefore important elements of the Tools4ever cloud security policy.

Deloitte Security Scan

At Tools4ever, we consider pro-active and frequent testing of our security solutions as a cornerstone of our success. Since we develop advanced Identity & Access Management solutions, we have a large number of security experts within our own ranks. They are not only active in developing our security solutions and products. We also run an inhouse programs in which our own solutions are tested on potential security flaws by our own experts on a regular basis.

However, that is only our first line of prevention. We also have our software solutions tested twice a year by top-class external ethical hackers of Deloitte. By selecting Deloitte for this, we have opted for guaranteed independent and highly qualified security experts of the market leader in information security. Gartner positioned Deloitte first globally in Security Consulting Services for the sixth consecutive year in its July 2018 report titled, Market Share: Security Consulting Services, Worldwide, 2017 [8].

Such external tests keep us sharp, prevents the occurrence of blind spots and provide us with an extra pair of eyes.

The test consists of a large number of attempts by professional ethical hackers to attack the HelloID solution. These ethical hackers have been trained to look at IT systems from the point of view of an experienced cybercriminal, to recognize vulnerabilities that others might overlook. They use for example the NCSC ICT-B v2 guidelines and the OWASP Top 10 Application Security Risks of 2013 and 2017.

The tests cover the full range of potential vulnerabilities. From system reports providing too much details, to the presence of cross-site scripting (XSS) vulnerabilities. Besides the well-known black box tests, the testers go further and execute also so-called grey box tests. A grey box test looks for security weaknesses in specific parts of HelloID, using inside information about the design and operation of the software. Finally, we look at the possibilities for authorized users within the system. Do they have ‘unintended’ possibilities which go beyond what’s necessary for their role? Very important of course, because we already know for a long time that fraud and cybercrime often take place from within organizations.

Certification

A crucial element in cloud services is the compliance with international standards. Both for the correct integration with IT systems in other domains, as well as to be assured that the latest views I areas like security, privacy and availability are adopted.

Tools4ever has an active compliance and certification policy. A recent example is our HelloID OpenID certification. This certification confirms the high quality of the OpenID Connect implementation as part of our HelloID Identity as a Service. As such, it provides additional confidence to our customers about the quality of our services.

Our cloud IaaS provider Microsoft Azure maintains the largest compliance portfolio [9] in the industry both in terms of breadth (total number of offerings), as well as depth (number of customer-facing services in assessment scope). Compliance covers major globally applicable standards and certifications. In addition, Microsoft offers compliance to both industry specific, and region/country specific standards and certifications.

SOURCES

1	**Gartner**, “Hype Cycle for Cloud Computing,” August 2017. [Online]. Available: https://www.gartner.com/doc/3772110/hype-cycle-cloud-computing-.
2	**RightScale**, “State of the Cloud 2018,” 2018.
3	**Gartner**, “Is the cloud secure,” March 2018. [Online]. Available: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/.
4	**McAfee**, "Navigating a Cloudy Sky; Practical Guidance and State of the Cloud Security," April 2018. [Online]. Available: https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html.
5	**Gartner**, "Gartner Top 6 Security and Risk Management Trends For 2018," 4 Juni 2018. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-5-security-and-risk-management-trends/.
6	**Gartner**, May 2018. [Online]. Available: https://azure.microsoft.com/en-us/resources/gartner-iaas-magic-quadrant/.
7	**Microsoft Azure**, "Core Banking Software Provider Moves Flagship Offering to the Cloud and Opens New Markets," September 2017. [Online]. Available: https://customers.microsoft.com/en-us/story/core-banking-software-provider-moves-flagship-offering.
8	**Deloitte**, "Deloitte positioned first by Gartner in market share for Security Consulting Services worldwide for sixth consecutive year," 5 october 2018. [Online]. Available: https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-ranked-1-gartner-in-security-consulting-for-5th-consecutive-year.html.
9	**Microsoft**, “Microsoft Azure compliance offerings,” 29 october 2018. [Online]. Available: https://gallery.technet.microsoft.com/Overview-of-Azure-c1be3942.

TOOLS4EVER

IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER BV

Adres Amalialaan 126c
3743 KJ Baarn
Nederland

Telefoon +31 (0) 35 54 832 55
Website tools4ever.nl

Informatie info@tools4ever.com
Sales sales@tools4ever.com