Towards Identity as a Service (IDaaS)

Use cloud power to solve cloud era challenges

Microsoft France

Published: June 2016 (Updated: January 2017)

Version: 1.0a

Author: Philippe Beraud (Microsoft France)

For the latest information on Azure Active Directory, please see

http://azure.microsoft.com/en-us/services/active-directory/

Copyright© 2017 Microsoft Corporation. All rights reserved

Abstract: Organizations of any size require a single way to do identity, whether it will be for employees, partners, consumers, devices, “things”, etc. As of today, anything must be able to have a digital relationship – and connect – to anything else. After reviewing the main industry trends organizations have to cope with, the document explores the reasons why organizations of any size will increasingly use and rely on cloud services to solve cloud era problems, and thus why a new service-based model will emerge for identity combining more advanced capabilities with externalization of operations to achieve reduction in risk, effort and cost.

As such, through the analysis of both the business-to-employees (B2E), business-to-business (B2B), and business-to-consumers (B2C) scenarios, and their main characteristics as far as identity is at least concerned, the document discusses why Identity as a Service (IDaaS) – a service combining identity, security (and privacy), personalization and directory – will require that we move beyond the models of identity management that have guided our thinking to date, along with the possible (technical) paths. IDaaS will eventually manage everything from employees and customers to the Internet of Things (IoT).

This page is intentionally left blank.

Executive summary

Business means relations between entities by knowing and recognizing people, organizations, applications, devices, etc. so they can be allowed to (conditionally) access to information within and across organizations.

**There is no digital economy without identity. Ongoing digital relationships and connectivity with people and other entities are indeed fundamental to the success of today’s organizations.** Businesses need to know the names and characteristics of the digital and physical entities they interact with – when separated in cyberspace. They need to be able to authenticate these entities when interacting with them, to have a way to store information about them, to be able to “discover” that information, and do all this across organizational boundaries while preventing unauthorized access. Likewise, everyone (i.e. employee and *“*external*”* such as a partner or a consumer) needs these capabilities to work with current infrastructure and still lead in tomorrow’s technical environment. Identity is the foundational technology enabling this.

**Organizations require a single way to do identity, whether it will be for employees, partners, consumers, devices, things, etc. Anything must be able to have a digital relationship – and connect – to anything else.** Identity management, provisioning, role and access management, and authentication are key services both on-premises and through the (hybrid) cloud. With the “Bring Your Own Apps” (BYOA) for the cloud and Software as a Service (SaaS) applications, the desire to better collaborate a la Facebook with the “social” enterprise, the need to support and integrate with social networks, which leads to a “Bring Your Own Identity” (BYOI) trend, identity becomes a service where identity “bridges” in the cloud talk to on-premises directories or the directories themselves move and/or are located in the cloud. All organizations (i.e. greenfield organizations vs. IT-based organizations) will increasingly use and rely on cloud services to solve cloud era problems, but without abrupt changes and fork-lift upgrades. On-premises and cloud environments indeed fundamentally constitute a continuum.

**Identity as a Service (IDaaS) – a service combining identity, security, personalization and directory – will require that we move beyond the models of identity management that have guided our thinking to date.** A new service-based model will emerge combining more advanced capabilities with externalization of operations to achieve reduction in risk, effort and cost. High end security capabilities will become utilities available even to the smallest organizations, resulting in a democratization of the safe Internet. As illustrated with Microsoft’s ongoing investments in Azure Active Directory (as well as in other Microsoft services, products, and technologies), IDaaS will become in the forthcoming years the predominant way of connecting all the aforementioned entities and managing the related identity relationships.

IDaaS will transcend security perimeters, allowing applications and APIs to be integrated while running anywhere on any platform or hosting environment. It will provide a holistic control plane for on-premises and cloud-based identity systems (IS).  Moreover, IDaaS will unify provisioning, attribute management, personalization, authentication, authorization, real-time threat analysis, alerting, dashboards, auditing, and reporting for all these entities. IDaaS will be driven more by processes controlled through policies – workflows – than by administrators. This not only applies to automation of provisioning, but to the very way the service is hosted, where tenants will be able to require that actions by service administrators be limited, visible and subject to their approval.

Finally, IDaaS will support tenants with billions of entities, provide options for both geo-separation and geo-replication, guarantee automated failover between replicas, exceed a wide range of audit and compliance requirements, operate at greater than 5 9’s, employ hardware security modules for crypto, use TPM-based software deployment mechanisms, exclusively use multi-factor permission-based access for operator intervention and guarantee end-users detailed automated real-time audits of any operator actions impacting their tenant.

Table of Contents

[Notice 1](#_Toc454545545)

[Towards a new identity model 2](#_Toc454545546)

[Rationalization and externalization of IT 2](#_Toc454545547)

[API Economy 4](#_Toc454545548)

[Consumerization of IT 5](#_Toc454545549)

[Internet of Things 5](#_Toc454545550)

[The role of IDaaS for B2E 9](#_Toc454545551)

[Projecting employees’ identities to the cloud 9](#_Toc454545552)

[Providing identity “bridges” for the new world 11](#_Toc454545553)

[Towards a new model 11](#_Toc454545554)

[Illustrating these capabilities with Azure AD 13](#_Toc454545555)

[Handling the big shift towards B2B and B2C 17](#_Toc454545556)

[Managing identities at scale 17](#_Toc454545557)

[Enabling Business-to-Business (B2B) scenarios 18](#_Toc454545558)

[Enabling Business-to-Consumers (B2C) scenarios 21](#_Toc454545559)

[Further envisioning IDaaS 29](#_Toc454545560)

[Providing unified information access to the directory 29](#_Toc454545561)

[Providing unified automatic provisioning for users, groups and roles 30](#_Toc454545562)

[Registering and recognizing the identity of all the devices 30](#_Toc454545563)

[Granting context-aware conditional access 33](#_Toc454545564)

[Hardening operations to resist evolving cyber-threats 34](#_Toc454545565)

[Providing integrated management, altering, dashboard, etc. 38](#_Toc454545566)

[As a conclusion of this journey 39](#_Toc454545567)

[Appendix A. Seamlessly integrating with applications and APIs 41](#_Toc454545568)

[Embracing industry standard modern protocols and tokens 41](#_Toc454545569)

[Offering the best-of-breed support for well-established protocols and tokens 43](#_Toc454545570)

[Sustaining the most common primary scenarios 45](#_Toc454545571)

[Appendix B. Benefiting from Trust Frameworks and policies 46](#_Toc454545572)

[Leveraging the Trust Framework and the federation management foundation 46](#_Toc454545573)

[Articulating policies for identities experiences 48](#_Toc454545574)

[Terminology 50](#_Toc454545575)

[References 52](#_Toc454545576)

[Books 52](#_Toc454545577)

[Supplemental materials 52](#_Toc454545578)

# Notice

This document illustrates industry trends and foresees on that basis how adopted identity models will evolve towards Identity as a Services (IDaaS). It attempts to draw on that basis the main characteristics of IDaaS offerings and illustrates the envisioned directions with currently available capacities of Azure AD.

**Microsoft makes no commitments and no warranties, express or implied, with respect to the information provided here.**

# Towards a new identity model

As of today, four enormous waves of change are impacting organizations:

1. Rationalization and Externalization of IT,
2. API Economy,
3. Consumerization of IT,
4. Internet of Things.

These four “tsunamis” as industry trends are upon us or even already here. Technology and usage have caused a natural paradigm shift that is blurring the boundaries between business and private lives, physical world and digital world, within or outside the firewall, etc. And indeed, fear about security breaches is no longer a justification for enforcing rigid technology barriers. For example, IT is being forced to implement policies to guide employees while still allowing them to be creative.

**This boundary dissolution will consequently (if not already the case) shape the strategy for identity, security and privacy – leading ultimately to a new identity model.**

## Rationalization and externalization of IT

Economic pressures are changing the way we live and do business:

* The global economic contraction faced by every enterprise and government,
* The productivity imperative to “do more with less”, with a better agility and time to market.

IT-based organizations have no other choice than to become leaner, better focused, and more fit-to-purpose. Under such conditions, these organizations need breakthrough changes in order to survive and in many cases have to accomplish their digital transformation in some way or another.

This renewal must apply to ALL entities and systems of production and distribution - including IT - and the survivors will be the ones that specialize in what they do best and most efficiently.

Note Geoffrey Moore [Moore, December 2005] deeply delves on the differences between so-called "Core" and “Context" functions for an organization: “Core” refers to areas that businesses use to differentiate themselves from their competitors while “Context” corresponds to activities that help businesses achieve the status quo - think operational functions such as HR and Finance.

As far as IT is concerned, the economic benefits from combined cloud innovations can lead to:

* The obvious: new ways of delivering and operating the IT infrastructure and systems,
* The profound: new business processes as part of the above digital transformation.

As the economy indeed becomes progressively and increasingly digital, organizations must decide how to refactor, redistribute or even redefine business to accomplish the shift with the most efficiency. In this context, the cloud emerges as a major disruptive force shaping the nature of business and allowing dramatic global growth. **The cloud brings breakthrough change**, and thus represents (for incumbents) a major opportunity and plays a determining role.

An increasing number of people recognize the benefits of locating some set of their IT services in the cloud to reduce infrastructure and ongoing datacenter operational costs, maximize availability, simplify management, and take advantage of a predictable pricing model - provided that the resource consumption is also predictable, and the resource can be rapidly delivered to the market, can elastically scale in respect to the demand, and opens multichannel access for the business.

Many IT-based organizations have already begun to use both public and private cloud for their new applications (even whether IT likes it or not, which leads in such a situation to what is called the “Shadow IT”). And many have already switched to using finished cloud services for generic IT roles (for example Office 365, Salesforce.com, etc.). We are well into a new era of “hybrid deployment” in which progressively more IT functionality is hosted by cloud service providers at the same time that organizations retain IT assets running in on-premises datacenters.

Hybrid deployment requires that organizations increase their core infrastructure operational maturity in two main areas:

1. Improving the management of their on-premises IT landscape and traditional systems (servers, storage devices, network components, and other datacenter assets) by evolving towards a private cloud, i.e. an optimized and more automated way to provision and operate on-premises services.
2. Enhancing their service offerings by utilizing suitable public cloud services for lower-cost add-ons or replacements for existing IT assets. Such a dynamic is actually twofold:
3. When suitable and inexpensive “pay-as-you-go” (PAYG) alternatives exist for generic components, organizations can retire their expensive internal systems/applications/services (or parts of them), benefiting from cost reduction, agility, scalability, etc.
4. Organizations can cut the costs of new systems/applications/services by building them as cloud services and using other specialized cloud services as inexpensive building blocks that reduce their own labor.

The combination and interaction of the two approaches (private vs. public) provides the best strategy for the hybrid era and meets both the demands and the expectations of the businesses. A service request for a specific workload can be instantiated in either implementation, or moved from one to another, or can horizontally grow between the two implementations (cloud bursting for example).

As part as the rationalization and externalization/of IT, cloud economics creates a federated IT for organization with data and services in the Cloud.



**As far as identity is concerned, the above (with an increasingly multi-sourced hybrid cloud environment) implies that identity seamlessly work across the possible combinations for a specific workload with a mix of infrastructure, platforms, services and providers/operators, outside any perimeter, beyond direct organizational control.****This is all about (the ability of) projecting the employees’ identity to the cloud.**

Note The study “Hybrid environments Demand Coordinated IAM for both Security and Agility” [Forrester, May 2014] evaluates the identity challenges organizations are facing with hybrid cloud environments.

## API Economy

In the world of independent domains, IT-based organizations had to deploy every component required for business and IT solutions within their own environments. With the advent of the cloud, the federated IT as previously discussed, and along with the various Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) cloud offerings they can choose to procure some of these components as services and save the time and expense required to deploy (and even build) everything themselves.

As the ecosystem of cloud components materializes, all (incumbent) IT-based organizations - like of course new greenfield organizations for new comers - can build their own systems/applications/services (or parts of them) as cloud services using these building blocks.

Having done so, organizations can expose owned “specialized” services through simple RESTful web application programming interfaces (APIs) that allow them to be consumed in turn by other organizations, applications and services through notably a so-called open innovation move along with a focus on the ”three Cs to make the transition easier:

* Take steps to promote a **culture** around the values that APIs enable.
* Support a **community** of learning and innovation that reinforces these values.
* Make sure that the code is managed, secure, reliable, and scalable.“[[1]](#footnote-1)

“APIs have been elevated from a development technique to a business model driver and boardroom consideration.” [Deloitte, January 2015] Specialized services can (recursively) hook into other specialized services running anywhere else in the cloud using simple RESTful web APIs.



This enables organizations to focus on what they do best, avoid unnecessary development and maximize their competitiveness. *Appendix B. Seamlessly integrating with applications and APIs* presents the impact in terms of application’s architecture models.

In fact, the essence of “becoming digital” and entering the digital economy is to expose services as web APIs and relevantly leverage and consume the web APIs of specialized suppliers). Cloud platforms that stifle the openness of this interconnectivity will die from “synergy deficiency” compared to platforms that are open.

**This deep trend leads to the advent of the API Economy**[[2]](#footnote-2) **and governments and enterprises will flounder in the API economy without reusable identities protecting private data across their whole digital supply chain.** Systems run by different businesses must be able to reuse knowledge of identity and policy to adequately protect the private data they handle as it traverses multiple boundaries.

## Consumerization of IT

Devices have become cheaper and more affordable over the last few years and unsurprisingly proliferate: laptops, smartphones, slates, tablets, and hybrids. Same is true for both cellular and wireless networks that have become ubiquities. Social networks (Facebook, Google+, LinkedIn, Yammer, etc.) are changing how people get information and communicate. People want content and services to work seamlessly across all these devices and environments. They are becoming connected all the time: at home, at work and everywhere in between up to the point where personal and work communication can become indistinguishable.

As technology plays an increasingly important role in people’s personal lives, it is having a profound effect on their expectations for and use of technology in their work lives. People have access to powerful and affordable PCs, laptops, and tablets, are using mobile devices more and more, expect “always on” connectivity and are connecting with each other in new ways using social networks. Ultimately, they have more choice, more options, and more flexibility in the technology they use every day, and as that technology spills over into their professional lives, the line between personal and professional time is blurring. People want to be able to choose what technology they use at work, and they increasingly want to use that same technology in all aspects of their lives.

“Consumerization of IT” (CoIT) is the current phenomenon whereby consumer technologies and consumer behavior are in various ways driving innovation for information technology within the organization. As people become more comfortable with technology innovation in their personal lives, they expect it in their professional lives.

**Without any doubt, employees will demand – if not already the case - access with anything anywhere: i)** **from any location:** **at work, at home, or mobile, ii) from any device regardless of the fact they’re** **managed/unmanaged, corporate/personally owned, and** **with UI that meets the high standard set in the consumer world.**

This is also referred as to the mobility in the enterprise space. While CoIT has remarkable potential for improving collaboration and productivity, many organizations are grappling with the potential security, privacy and compliance risks of introducing consumer technologies into their environment. However, there are also many benefits to the CoIT trend that organizations can capitalize on with the right approach. Managing the CoIT challenge requires striking a balance between users’ expectations and an organization’s requirements.

People love their consumer technology because it makes it easier for them to connect with each other, access and share information, and collaborate. Those same benefits are there for the taking for businesses.

There is power in saying “Yes” to users and their technology requests in a responsible way – responsible meaning here that organizations will embrace these trends but also will ensure their (increasingly multi-sourced hybrid cloud) environment remains secure and well managed. Identity is certainly an enabler.

## Internet of Things

Internet of Things (IoT) is certainly a buzzword despite the fact that this term was initially proposed in1999 by Kevin Ashton[[3]](#footnote-3). Beyond the ambient noise and all the press buzz, IoT is still a difficult trend to define precisely: Is it about “the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure”[[4]](#footnote-4), “the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment”[[5]](#footnote-5), “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies”[[6]](#footnote-6), etc.?

To attempt to formulate it differently, **IoT is a metaphor and really comes down to four basic areas**:

1. The **things** themselvesthat typically represent physical entities.
2. The **connectivity** those things have (or at least can have) to either the Internet (e.g. the cloud) or an organization in terms of central backend platform/system, each other or human beings.
3. The **data** those things acquire, collect (or can collect), and communicate information about the physical world.
4. The **analytics** that allows to extract from the data insights, i.e. meaningful information, and thus enabling people or machines to take decision(s) and/or action(s).

The above four key areas can apply to various domains, applications, and use case scenarios.

Note Everything is indeed becoming (or can be) connected and de facto a thing; the connectivity is also becoming considerably improved whether it’s wired, cellular, or wireless. Should be talked about ubiquitous connectivity? Likewise, capabilities are also unleashed with more and more powerful tiny microchips being released that are not only capable of connectivity but also able to run much more advanced software than ever before at a lower price.

Leading analysts are playing a numbers game trying to estimate the potential size and economic impact of IoT. According to the Gartner, “deployment of the IoT is certainly happening and the trend is growing. Approximately 3.9 billion connected things were in use in 2014 and this figure is expected to rise to 25 billion by 2020.”[[7]](#footnote-7) McKinsey Global Institute estimates that “the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025. At the top end, that level of value—including the consumer surplus—would be equivalent to about 11 percent of the world economy.”[[8]](#footnote-8) Regardless of what numbers you’re looking at, there are billions of things that have the ability to collect information and this number grows daily. This said, IoT isn’t necessarily about future predictions of billions of connected things.

For incumbent organizations, defining an IoT strategy is not necessarily about ripping and replacing technologies but should rather allow them - at their own terms – to build on the infrastructure they already have, to make use of what they already have, connect a wide range of (line-of-business (LOB)) things they already own, tap into the data that already exists, and gain the visibility they need.

IoT can make a difference to organizations’ businesses today starting with the things that matter the most by (in a non-exhaustive manner) **gaining better insights and agility, opening new business and game changing opportunities, and redefining customer service**. Furthermore, IoT opens up many profitable partnerships and more interactivity to the physical world. It will grow demands of (open) innovation and create opportunities in many sectors/industries (energy, manufacturing, retail, transport and mobility, health, etc.) as discussed in European Research Cluster (IERC) cluster book[[9]](#footnote-9).

As a result, it’s important to see IoT as not just a standalone strategy or, in terms of architecture, a set of dedicated services that work independently of the rest of an organization’s digital investments. **IoT has rather to be seen as part of a larger story that entails every aspect of on organization business and digital investment – of which IoT is just one (major) part.** “As in other technology waves, both incumbents and new players have opportunities. Digitization blurs the lines between technology companies and other types of businesses; makers of industrial machinery, for example, are creating new business models by using IoT links and data to offer their products as a service.”[[10]](#footnote-10)

Note By connecting line-of-business assets and other things, monitoring them, leveraging data analytics, etc. IoT isn’t fundamentally a new subject in itself. One can have in mind the waste machine-to-machine (M2M) implementations that already exist. This said, the most intense and promising phase has just started few years ago in parallel with the cloud that emerges as a major disruptive force in shaping the nature of business and digital investment of which IoT is just one (major) part. An increasing number of organizations will unsurprisingly find they need new capabilities to take full advantage of their existing things disseminated around the world. The cloud will appear as the most reliable and cost-effective way to obtain the capabilities they expect from IoT. Moreover, the cloud enables these organizations to scale the resulting IoT solution at any time whenever required to accommodate their business.

Note In a recent annual report, Jeff Immelt, CEO and Chairman General Electric, is convinced[[11]](#footnote-11) that “every industrial company will become a software company” as a result of such a transformation.

Beyond the above “shortly” expressed averred potential of IoT, security and privacy concerns are today top IoT adoption inhibitor for organizations[[12]](#footnote-12). “Security and privacy issues absolutely must be addressed. Internet of Things devices will not be used for critical tasks in, say, industrial or medical environments if connectivity protocols have not been established to prevent hacking, loss of intellectual property, or other potential breaches.”[[13]](#footnote-13)

Moreover, IoT security is unfortunately more complex than traditional IT security. Such a complexity is not only induced by the scale, all the heterogeneous/legacy systems to onboard, etc. but also due to physical/digital blur and its various consequences and impacts: greater risk of exposing privacy-sensitive information, reach of control, impact on human behavior (manipulation). It’s all the more so that a breach of security can eventually lead into a (major) safety breach…

Note Nitesh Dhanjani [Dhanjani, August 2015] explores how malicious attackers can abuse popular IoT devices. The discussion on how to uncover vulnerabilities in existing IoT devices represents a great opportunity to gain deeper insight into attackers’ tactics in such an asymetric paradigm.

In this context, and according to Gartner, **managing identities and access will be critical to the success of the IoT and there is growing importance for concept of Identity of Things (IDoT), which is a new extension to identity.** “The Identity of Things (IDoT) is a new component to identity management that encompasses all entity identities. These identities allow you to define relationships among the entities — between a device and a human, a device and another device, a device and an application/service, or a human and an application/service.” [[14]](#footnote-14)

It's only one piece of the puzzle but this certainly constitutes a solid starting point and a reliable foundation for future constructs. Likewise, old security approach needs to also be augmented and looking at the problem space from the threat modeling aspect provides more than an opportunity to better understand the threats that apply to IoT devices, data flow, storage, services, etc.

# The role of IDaaS for B2E

According to Wikipedia[[15]](#footnote-15), identity and access management (IAM) (a.k.a. identity management (IdM)) “describes the management of individual principals, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.”

The cloud is changing the way in which applications are written for an organization. Accelerated market cycles, multi-tenancy, pure cloud solutions as well as hybrid deployments, web programmability and the API economics, the rise of devices offer without any doubt new opportunities.

Whilst employees will continue to use many of today’s IT-approved applications, they (will) thus use progressively more cloud-based applications and APIs, starting with the Software as-a-Service (SaaS) applications but not only. There are no abrupt changes. Organizations simply progressively use cloud services to solve the cloud era problems they are faced with.

These changes present new challenges for the key services (both on-premises and in the cloud) that represent identity lifecycle management, provisioning, role and access management, authentication and security of users and devices requiring granular access. **The net result is to propel identity to first rank of importance.**

Key issues that require better identity capabilities for business-to-employee (B2E) include in a non-exhaustive manner:

* The “Bring Your Own Apps” (BYOA) for cloud and SaaS applications,
* The imperative of quickly becoming part of the API economy,
* The desire to better collaborate a la Facebook within the “social” enterprise where organizations more and more expect to experience themselves as social networks.

Let’s consider the first key issue where the employee identity has to be “projected” in some way or another to both the SaaS applications and the custom applications that organizations will consume or deploy in its forthcoming or already federated IT environment.

## Projecting employees’ identities to the cloud

As one can expect, usual on-premises authentication mechanisms such as Kerberos and NTLM no longer apply in a general manner in such a multi-sourced hybrid cloud environment since these applications outside the corporate network boundaries do not have most of the time connectivity to the on-premises identity systems (IS) infrastructure, for example an AD domain controller in a Microsoft “shop” (and/or in this context the operating systems underneath may not be domain-joined at all).

It’s all the more so with the mobility and the Bring Your Own Device (BYOD) trend where users will also often be themselves considered outside of the organization’s infrastructure perimeter. Furthermore, the modern applications to consider can by nature encompass multiple security realms. The aforementioned API economy and the “specialized” RESTful services reinforce this point.

Consequently, **the traditional IAM model devoted to a single security realm/domain no longer applies** for obvious reasons that we won’t cover in any further detail here.

Leaving aside the numerous SaaS applications that do not support identity federation, what can be referred as to **the first identity federation IAM model also has its own limits too**. Setting up outbound federation relationships for projecting “identities” outside the corporate network boundaries is the classic approach since early 2000 but complexity grows linearly when you have to manage a federation relationship with each (SaaS) application that belongs to your so-called federated IT.



Managing thousands of federation relationships becomes untenable. Beyond the number, this implies from a technical perspective to simultaneously support potentially various federation protocols imposed by the SaaS providers, the cloud providers, etc. along with their possible related profiles to accommodate diverse technical choices and capabilities to interoperate with the organization’s federation infrastructure on-premises.

Note Despite [Security Assertion Markup Language (SAML) 2.0](http://go.microsoft.com/fwlink/?LinkId=193996)[[16]](#footnote-16) and at a lower degree [WS-Federation (WS-Fed) 1.2](http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf)[[17]](#footnote-17) are today common well established standard protocols in this space, the devil is always in the details as one should say… and you generally have to overcome some quirks and peculiarities that pertain to specific providers’ implementation.

Note Former SAML 2.0 interoperability certification programs ran from [Liberty Alliance](http://www.projectliberty.org/liberty/liberty_interoperable)[[18]](#footnote-18) and later handled by the [Kantara Initiative](http://kantarainitiative.org/)[[19]](#footnote-19) (kan-TAR-a: swahili for "bridge"; arabic roots in "harmony") have contributed over the time to ease the interoperability. Such programs have been designed to test commercial and open source products against the SAML standard to assure base levels of interoperability between products in addition to the guidance of the available operational modes for the various SAML 2.0 implementations (see [Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf)[[20]](#footnote-20)).

In addition, you have to deals with all the SSL/TLS, signing, and encryption X509 certificates that such solutions leverage. It’s all the more so with the related trust chains: “*If federation is broken. It's PKI. If it is not PKI, there's a typo. If you typed it correctly (case counts!). It's PKI”.* (One should admit that DNS errors and network restrictions are also a common source of potential issues).

Once federation finally works with an application, the federation relationship has to be maintained over the time. For example, this supposes to monitor the (SaaS) application’s metadata if any and to automatically update your own trust definition information to reflect these current settings in your configuration. Such an operation allows to adequately in a timely fashion handle any certificate rollover for example. One should note that all of these considerations also apply from a cloud SaaS application provider too.

Furthermore, with identify federation, and beyond the above technical barriers, you have very limited user level visibility for the targeted applications whatever they are. The employees’ identity information - that is conveyed in the security token your on-premises IS infrastructure issues - is limited by definition to the acceptable size of the security token, potentially as per related specification.

These difficulties may lead organizations to design and deploy an external (LDAP-exposed) façade in the DMZ to the directories of their on-premises IS and directories so that “external” applications, at least the ones they own, can request the employees’ identity information they need to authorize and/or conduct the underlying functions. This can become very complex too and raise additional security considerations so that it’s appropriately hardened. Alternatively, an out-of-the-box (OOB) provisioning mechanism can be setup if supported by the considered applications but this also leads to additional complexity on a per application basis.

So, the above “old” model has also its limits with the federated IT landscape where identity has to seamlessly work across the possible combinations that may also vary over the time… (Thus, the topology should never be exposed to users.)

## Providing identity “bridges” for the new world

All the above plead for establishing more seamless “bridges” between from on-premises to cloud or vice versa, without friction, at any time. Thus identity becomes de facto a service where identity “bridges” in the cloud “talk” to on-premises IS and directories or the directories themselves move and/or are located in the cloud (see back in 2012 Gartner report 2013 Planning Guide: Identity and Privacy [Gartner, November 2012]).

The ability to operate synergistically with on-premises IS greatly eases the path for IT-based organizations to embrace the cloud without fork-lift upgrades: **on-premises and cloud identity systems are in fact a continuum**. The problems of transition and the requirements for information autonomy make integration with existing on-premises systems a hugely important issue in many market segments, and the evolution towards an integrated system, which prevents duplication of management and compliance, will become progressively more important as customers see coexistence with and migration to cloud systems as a strategic issue rather than a tactical one. This constitutes a prerequisite to allow the move from on-premises to cloud or vice-versa, without friction, at any time.

**All of the above plead that we move beyond the models of IAM that have guided our thinking to date.**

## Towards a new model

IT-based organizations (will) use cloud services and applications created by (cloud) ISVs, PaaS cloud platforms for LOB applications custom development, (as well as IaaS cloud environment for specific workloads to onboard the cloud for IT optimization reasons). (as already outlined, greenfield organization already live in a cloud era world.)

Hence organizations need a specialized service that appropriately handles in the above context identity as well as security and privacy for them – with an increased level of specialization and professionalization adequate to emerging cyber threats. About the key understanding this leads to is how you get more capability for less money. **This has to cut costs as well as deployment complexity – not increase them. “A new service-based model will emerge combining more advanced capabilities with externalization of operations to achieve reduction in risk, effort and cost.”[[21]](#footnote-21)**

Identity, like compute, storage and networking, is indeed an essential platform service. In the same way that identity played a critical role in the adoption of workgroup computing, identity services will play a critical role as organizations adopt the (hybrid) cloud, embracing the API economy, managing the BYOD trend, etc.

**Such a service-based model must leverage efficiencies of the cloud and automation to get efficiencies in identity.** Kim Cameron, Microsoft Chief Identity Architect, is convinced[[22]](#footnote-22) that “*organizations will find they need new identity management capabilities to take full advantage of the cloud. They will also find that the most reliable and cost-effective way to obtain these capabilities is through Identity Management as a Service – i.e. using the cloud to master the cloud.*”

Identity Management as-a-Service (IDaaS), will directly attack these problems – simplifying life for organizations and their users. IDaaS will:

* Offer ALL necessary high security identity capabilities (directory, outbound federation, inbound federation, (multi-factor) authentication services, access management for the cloud, mobile, and web, cloud provisioning, etc.) – while maintaining usability.
* Provide a business centric portal and automation features for configuring the above capabilities.
* Sustain easy-to-integrate/easy-to-customize identity experiences.
* And finally cut costs thanks to superior cloud economics.



Furthermore, to make that happens, and to merit and gain the organizations’ confidence, IDaaS vendors (will) have to heavily invest in:

* Third-party security certifications such as [ISO/IEC 27001:2013 standard](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534)[[23]](#footnote-23), i.e. one of the most recognized security benchmarks available in the world, SSAE 16 SOC 1 and SOC 2, etc.
* Compliance with industry regulations, privacy and data sovereignty (country-specific) laws that apply to such as Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), European Union Data Protection Directive (EUDPD 2003/58/EC) along with the European Union (EU) Model Clauses method, etc. to just name a few.

These requirements and capabilities for compliance, security, data sovereignty, privacy, etc. will drive almost all organizations to subscribe to IDaaS offerings that are cheaper, broader in scope, more unifying and more capable than the systems of today. Most organizations will certainly conduct a risk analysis, assess how the initially selected identity services offering fulfills their security, compliance, and risk management requirements. The [Cloud Controls Matrix (CCM)](https://cloudsecurityalliance.org/research/ccm/)[[24]](#footnote-24) and the [Security, Trust and Assurance Registry (STAR)](https://cloudsecurityalliance.org/star/)[[25]](#footnote-25) from the Cloud Security Alliance (CSA) can be leveraged to assess how an offering fulfills the security, compliance, and risk management requirements as defined by the CCM and what extend.

Note The CCM is a meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations in order to provide organizations with the needed structure, detail and clarity relating to information security tailored to cloud computing so that they can confidently evaluate an offering from a service provider.

Note The STAR program is a publicly accessible registry designed to recognize the varying assurance requirements and maturity levels of service providers and consumers, and is used by customers, service providers, industries and governments around the world. STAR consists of 3 levels of assurance, which currently cover 4 unique offerings: i) Self-Assessment, ii) STAR Attestation, iii) STAR Certification, and iv) STAR Continuous Monitoring. All offerings are based upon the succinct yet comprehensive list of cloud-centric control objectives in the CCM.

These organizations will also naturally review the provided service level agreements (SLA) (if any), the cost of the available subscriptions, the supported capabilities to that respect, etc. They will also assess the geographies in which these offerings are available, as well as a series of facts to further qualify the selected IDaaS vendors and their viability and relevancy over the time. This comprises their funding, their revenue, the number of customers they have along with their profiles, their number of employees, their locations, etc.

## Illustrating these capabilities with Azure AD

Interestingly enough, the above discussed new model to lower the overall complexity of IAM in today’s world and benefit from cloud economics to cut costs already translate in [Azure Active Directory (Azure AD)](https://azure.microsoft.com/en-us/services/active-directory/)[[26]](#footnote-26).

Azure AD is Microsoft’s vehicle for providing IDaaS capabilities in a public/hybrid cloud for IT-based and greenfield organizations. Microsoft’s approach to IDaaS is deeply grounded in – and extends – the proven concepts of on-premises Active Directory (AD).

The foundational concept of on-premises AD is that **the content of the directory is the property of the organization deploying it and access to and use of that content is completely under the organization’s contro**l. This is also the fundamental concept behind Azure AD. Azure AD is NOT a monolithic directory of information belonging to Microsoft, but rather consists of millions of independent identity systems controlled by enterprise and government “tenants”. Each tenant’s information is owned and usable by the controlling organization - not by Microsoft.

Azure AD makes it easy at either regional or global scale to deliver a single sign-on (SSO) experience for:

* Microsoft services like Office 365, Dynamics 365, and Intune, as well as 3rd party pre-integrated SaaS applications thus eliminating the need for multiple usernames and passwords and limiting helpdesk calls and password resets.

Note To make the configuration even easier, thousands[[27]](#footnote-27) of cloud SaaS pre-integrated applications like ADP, Concur, Google Apps, Salesforce.com and others, regardless of the public cloud they are hosted on, are preconfigured via an application gallery. The SSO experience is either federation-based or password-based depending on the SaaS applications’ own capabilities.

* (Cloud-based) web applications and web APIs on Microsoft Azure or in other clouds such as Amazon Web Services (AWS) thanks to industry standard protocols support and outbound federation capabilities.
* Mobile applications thanks to standard modern protocols support (see *Appendix B. Seamlessly integrating with applications and APIs*).
* On-premises web applications as well thanks to Azure AD Application Proxy[[28]](#footnote-28) (and Kerberos transition protocol support).

Furthermore, Azure AD increasingly becomes a hybrid product with AD to (virtually) constitute at the end ONE single directory. Azure AD indeed includes Azure AD Connect[[29]](#footnote-29), a single and unified wizard that streamlines and automates the overall onboarding process for directory synchronization with on-premises AD (or other LDAP-based IS environments[[30]](#footnote-30)) (including a rich set of sync and write-back capabilities to the on-premises IS) and - if you want to - password (hash of) hash synchronization (PTS), pass-through authentication (PTA), or (federated cross-domain) single sign-on (SSO) to provide a seamless sign-in experiences for users.

Moreover, Azure AD Connect Health[[31]](#footnote-31) (for sync[[32]](#footnote-32), for Active Directory Federation Services (AD FS)[[33]](#footnote-33), and for Active Directory Domain Services (AD DS)[[34]](#footnote-34) in public preview as of this writing), a cloud based service, helps monitor and gain insight into health, performance, and both sync, login, and directory-related activities of your on-premises IS.

Azure AD provides a so-called “same sign-on” experience enabled by above password sync capability of Azure AD Connect that allows employees to sign in in the cloud with their on-premises password. If this experience isn’t sufficient and/or doesn’t fulfill the organizations security requirements, Azure AD supports integration with AD FS and other third-party security token services (STS)[[35]](#footnote-35) such Shibboleth2, PingFederate, SiteMinder, etc. to provide a federated SSO experience for corporate users while keeping user passwords on-premises. In addition, a pass-through authentication to AD is going to be introduced via a lightweight connector to deploy on-premises.

The ABC’s of this IDaaS offering embraces the following core principles:

* Nothing but open standards and connectivity to remove the technical barriers,
* Fully embrace all platforms and devices whatever they are,
* Remove any duplication of management effort (doubling administration would introduce new security vulnerabilities…),
* Use cloud signals and machine learning to harden and evolve both cloud and on-premises systems,
* Fully leverage cloud power, but respect organizational data boundaries, i.e. enforce a deep logical isolation between organizations’ information.

And **a commitment to one principle above all others: “The cloud is your cloud. It is an extension of your organization. You control and define it.”**

Last year, Gartner in their Magic Quadrant (MQ) for Identity Management as a Service (IDaaS) [Gartner, June 2015] has placed Azure AD after its only first year of availability in the “Visionaries” MQ. As of this writing, **Gartner has just released their MQ for IDaaS for 2016 [Gartner June 2016] and Azure AD Premium has been placed in the “Leaders” quadrant**, and positioned very strongly for our completeness of vision.



Important note The above graphic was published by Gartner, Inc. as part of the larger research document [Gartner June 2016] and should be evaluated in the context of the entire document. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

As Alex Simons, Director of Program Management, Microsoft Identity and Security Services Division, says, “we’re thrilled with the result. It really validates our vision of providing a complete solution for hybrid identity and access for supporting employees, partners and customers all backed by world class security based on Microsoft’s intelligent security graph. This result says a lot about our commitment in the identity and access management space but more importantly about our customers, implementation partners and ISV partners who have worked together with us. They have been awesome about sharing their time and energy every day, to make sure that the products and services we build meet their needs and are helping them position their companies to thrive in the emerging world of cloud and devices.

You might be surprised to know that Microsoft also is the only vendor in the Leader quadrant across Gartner’s Magic Quadrants for IDaaS, Cloud Infrastructure as a Service (IaaS), Server Virtualization, Application Platform as a Service, Cloud Storage Services, and as a leader across the data platform and productivity services. This really shows you why customers are choosing Microsoft across the full spectrum of cloud computing – our services are well integrated and also among the best available in their individual categories.

Our effort doesn’t stop here. We have a lot of hard work ahead of us and we are planning to deliver more innovative capabilities to further improve our position in the “leaders” quadrant*.*”[[36]](#footnote-36)

Considering the already impressive numbers (tenants, users, authentications per day, etc.) relating to the current adoption of IDaaS solutions – 10M directories, 750M users, above 1.3B enterprise authentications par days, etc. as far as Azure AD is concerned -, one can therefore predict with certainty that almost all organizations will subscribe to these (hybrid) services. They will leverage them to manage authentication and authorization of internal employees.

These IDaaS offerings will thus represent for greenfield organizations the best cloud-only solution but also provide connectivity with established IT-based organizations. Hence, **high end security capabilities will become utilities available even to the smallest organizations.** But in the outward looking world that is emerging so quickly it will be thus just as important to manage access to services by an enterprise’s supply chain, its customers (including individuals), its leads and prospects. In the same way, governments will benefit from these services when interacting with other government agencies, enterprises and citizens.

# Handling the big shift towards B2B and B2C

In addition to managing their employees (or civil servants) and mobile workforce access for the required SaaS and (cloud-based, hybrid, and on-premises) line-of-business (LOB) applications, IDaaS will help organizations manage their “external users”.

From an organization’s perspective, this population of “external users” represents all the people who interact with its online applications and (web) APIs, but who are not directly members of the organization itself. Consumers, customers, clients, citizens, retirees, partners, etc. are chief amongst them. Typical populations of these “external users” dwarf the size of an organization’s internal workforce.

Today, enterprises and governments struggle to manage the accounts, credentials and entitlements of their *huge populations* of “externals” that are not well served by existing on-premises IS.

## Managing identities at scale

Current best practices – maintaining local accounts and passwords – can lead to debilitating financial and personnel costs, and front-page security and privacy disasters. **The on-premises IS in place to sustain the above interactions indeed faces a multitude of challenges.**

This obviously starts with the security and privacy risks that must be adequately addressed when storing credentials and personally identify information (PII)/ or sensitive personal information (SPI) in various application databases.

From an implementation standpoint, IT-based organizations typically have to cope with heterogeneous stove-piped identity systems that are custom built, acquired from 3rd parties, part of legacy systems, etc. along with different data types and formats, different types of extensibility/states of modifications possible, different application platforms and systems (and even blurred system boundaries), etc.

Beyond the subsequent lack of a unified view, this usually results in high total cost of ownership (TCO) with not only the software licensing, maintenance, and upgrade costs implied with such an on-premises IS infrastructure but also with 7 x 24 operations and the support staff required to ensure the service.

This leads both to quality of service (QoS) challenges (given the absence of a high availability and/or disaster recovery infrastructure) and a lack of scalability (up to millions of these “external users”) since legacy systems have no elasticity when it comes to demand spikes.

Organizations need a specialized service that handles identity at the appropriate scale while assuring the necessary security and privacy. – This demands an increased level of specialization and professionalization adequate to emerging cyber threats (see section § Hardening operations to resist evolving cyber-threats later in this document). Once this will be understood, it will become obvious why organizations get more capability for less money by leveraging cloud capabilities.

**Unlike today’s identity systems, which focus primarily on employees, IDaaS will be equally adept at managing identity relationships with “externals” – an organization’s partners and customers. IDaaS will directly attack the above challenges – simplifying life for both IT-based and greenfield organizations and their “externals”.** Let’s look at how to do Business-to-Business (B2B).

## Enabling Business-to-Business (B2B) scenarios

Collaboration between organizations has become essential to the value organizations create. Many organizations take on projects that require partnering with other organizations to spread risk or assemble expertise. Many companies, including Microsoft, have extensive supply chains and partner networks made up of large and small organizations that are essential to delivering customer value.

IAM is at the core of each and every one of these collaborations: you need to give your business partners access to key applications and data, but you also need to make sure these assets don't end up in the hands of the wrong people.

### Why current models are flawed?

Traditionally, there have been two ways organizations have tried to solve this problem:

1. Inter-organization identity federation relationships.
2. Internally managed partner identities.

#### Inter-organization federation relationships

Setting up inter-organization federation relationships is the classic approach since early 2000 as already outlined but has problems:

* Most large IT-based organizations do business with many smaller organizations that don't have the expertise and can't afford the (on-premises) identity infrastructure required to setup and manage federation.
* Complexity grows linearly when you have to manage an inbound federation relationship with each partner. As discussed in section § Projecting employees’ identities to the cloud, managing thousands of federation relationships becomes untenable.



Once all the technical nitty-gritty details have been resolved, the technical barriers removed and the federation finally works with a partner, the federation relationship has to be maintained over the time to ensure a service level agreement (SLA) between your organization and the partner organization - an SLA that has also to be prior defined….

* With inbound identify federation, you have very limited user level visibility making compliance and audit challenging. As we already seen, the information conveyed as claims in the security token issued by the partner organizations is limited.

Note We use the term *claims* – rather than attributes which is a subset – because in the case of online transactions these are not facts that can be directly verified by the relying party; rather they are assertions, or claims about facts for which the relying party must develop sufficient confidence to grant the end user’s requested transaction.

Furthermore, this information also results from a prior business agreement between the two organizations that intend to collaborate, and have to respect and fulfill both the security and the privacy policies of the partner organization before releasing it. It’s thus by definition a tradeoff…

These difficulties lead many organizations to create directories of internally managed partner identities. Let’s consider this model.

#### Internally managed partner identities

This common practice has also its own security and management concerns in addition to the ones already outlined in section § Managing identities at scale:

* When partner accounts are managed by the organization, this is yet another set of usernames and passwords for partner users to remember and yet another set of identities for you to manage (provision, de-provision, reset passwords, etc.).

Beyond the possible need to manage a new directory for that specific purpose, this of course also implies additional processes (sign-up and cleanup at least), cost, and burden on both sides. One would say that some well-defined and controlled self-service solutions may contribute to reduce them over the time. This said, these self-service solutions if not already in place have to be de facto designed, implemented and rolled out. All of these lead to additional complexity too…

* These accounts in internally managed directories can easily provide too much access and thus put the whole organization at risk. Partner accounts indeed tend not be managed as closely as employee accounts. Therefore, they have become over the time the favored attack vector for hackers:

“*The hackers that carried out the massive data breach at Target Corp. appear to have gained access via a refrigeration contractor in Pittsburgh that connected to the retailer's systems to do electronic billing*.”

– Wall Street Journal[[37]](#footnote-37)

“*Criminals used a third-party vendor's user name and password to enter the perimeter of Home Depot's network.*”

– Home Depot[[38]](#footnote-38)

Once a partner account managed in the directory is compromised, attackers can move laterally to other accounts in the same identity store. So an exploited partner user puts the whole organization at risk…

* These accounts are disconnected from the partner's IS, so they are not disabled when partner employees change jobs or are terminated. Access continues long after a partner user has left his organization…

#### Towards an ideal cross-organization identity model

The ideal cross-organization identity model is one where each partner has the ability to manage their own employee identities, integrated into their existing IT systems, according to their own corporate security and privacy policies, in a way that works for their business while providing rich cross-organization visibility, and world class compliance and control.

**IDaaS will certainly help organizations of any size achieve this ideal** **in order to solve the IAM challenges that have emerged, as economic and competitive pressures drive commercial enterprises, to enable cross-organization collaboration wherever and whenever it makes senses for their business and competitively with the ambient credo to “do more with less, with a better agility and time to market”.**

IDaaS will help organizations manage their external users, and thus notably share resources with business partners that they work with every day and deliver applications to business.



IDaaS as the control plane will provide simplified management and security for partners and other external users accessing the organizations in-house LOB applications and other resources they provide. This unsurprisingly includes access to popular SaaS applications as well as other mobile, cloud, and on-premises applications.

As an illustration, Azure AD, which began as an IS for employees, extending on-premises AD into the cloud (and vice-versa in some areas) has evolved into a system designed to manage an organization’s relationships with its partners (and its consumers/citizens, see next section). The additional feature Azure AD B2B lets an organization enable access to its corporate resources from partner managed identities in a simpler and more secure manner by providing a simple sign up process regardless of what kind of IS your business partners have in place.

This feature allows to create cross-organizations relationships by inviting and authorizing users from partner organizations to access the authorized corporate resources. An email-verified process allows business partners with or without an existing Azure AD subscription to access these authorized applications and resources. (For business partners that don't already have Azure AD, and/or for partners with no IT infrastructure at all, Azure AD B2B collaboration has a streamlined signup experience to provide Azure AD accounts to your business partners.) This email-verified process enables a bulk invite and authorization of thousands of users at a time from partner organizations. The management burden is reduced as each business partners manage their own accounts while security is increased.

Complexity is also reduced as each organization federates once with Azure AD and each partner user is represented by a single Azure AD account. Azure AD creates and allows the organization to manage the trust relationships in the cloud, freeing that organization from the complexity of managing and maintaining over the time per-partner federation relationships.

Security is increased as access is lost when partner users are terminated from their organizations and unintended access is not granted by membership in internal directories. The organization’s business partners use their own login credentials, which frees you from managing user credentials in your directory for users as they join or leave their organization. Moreover, you control access policies within your organization where you can control and remove the authorization to access your corporate resources separately from the business partner's account lifecycle. Eventually, you have the ability to assign partner users to applications and to add partner users to security groups. This means for example that you can revoke access to your applications without having to ask the IT department (if any) of your business partner to do anything.

## Enabling Business-to-Consumers (B2C) scenarios

In addition to B2B scenarios, IDaaS will also take over management of relationships with individual consumers, customers or citizens to meet the growing needs of organizations looking to connect their "individuals” via consumer-facing applications.

In a research document [Gartner, June 2015], Gartner says that “B2C use cases have grown in importance as organizations look to replace a mixture of custom-developed IAM products and traditional on-premises IAM products”.

**IDaaS will certainly help organizations to solve the IAM challenges that have emerged, as economic and competitive pressures drive commercial enterprises, ISVs, educational institutions, and government agencies to shift their service delivery channels from face-to-face engagements to online web applications, web API, as well as native mobile applications.**

For that purpose, IDaaS will professionalize authentication, credential management, collection and storage of attributes, and privacy compliance – hardening operations to resist evolving cyber threats (see later in this document). This is primarily about reducing friction in B2C identity experiences, not aesthetics, although one should not be blind to the ease associated with beautiful user experiences (UX) that are key for B2C scenarios.

Note This refers to [emotional design](https://en.wikipedia.org/wiki/Emotional_Design)[[39]](#footnote-39) for the research on ease-of-use and aesthetics, and beyond that to UX design.

#### Using social accounts and local accounts

For consumers, social media is emerging as a key source of identity. Real world examples of this include organizations that have internet-centric business models. Consider music download sites such as Spotify that allow users to login using their Facebook identities make it far easier for users to sign up.

At the application level, this also constitutes the starting point to create and amplify user-generated content with a suite of social features that includes social sharing, comments, social activity feeds, live chat, and curated social content. All of the characteristics undoubtedly contribute to the user engagement.

Furthermore, usage of social identities appears to be expanding into more conservative areas; for example, the UK government has evaluated Facebook as part of the Identity Assurance (IDA) program[[40]](#footnote-40), a way of better enabling secure transactions between public sector bodies and citizens.

At the same time these changes present new challenges for the consumer-facing applications (both on-premises and in the cloud) that represent one more time identity lifecycle management, provisioning, role and access management, authentication and security of users and devices requiring granular access. The net result is to propel identity again to first rank of importance.

IDaaS will gives consumers, customers, etc. a choice between i) “Bringing their own Identities” (BYOI) by using one of their existing social accounts, such as Amazon, Facebook, Google+, Microsoft Account (MSA), LinkedIn, Twitter, etc. and ii) creating a new local account (arbitrary verified email address, username with password, username with verified phone number (see below), etc.).

Beyond local accounts, enabling BYOI ensures user adoption, given that there are millions of customer identities in use today from the aforementioned social identity providers and customers are more likely to remember a password they use daily rather than at most a few times a year.

#### Benefiting from the choices of authentications

Enabling BYOI for authentication to a relying party is only the first part of the solution. Clearly these social identities are self-asserted and of such low identity assurance that they are not sufficient to authorize access to valuable or sensitive information.

Hence to improve organizational security IDaaS will (have to) combine these social network credentials with information obtained from the customers themselves. To present verified attributes from authoritative sources in the context of the online transaction, the service will bundle support for commercial and government attribute verifiers that can verify the natural identity of users where that is a requirement. Furthermore, and as the stakes go up, IDaaS will do “step-up” using cell phones, recognition of a user’s hardware, and interaction with other devices as an additional authentication method when the use case warrants it.

Besides the various multifactor authentication mechanisms (MFA) supported out-of-the-box by IDaaS, IDaaS will provide a marketplace to open up for organizations the range of available solutions to accommodate (more) specific requirements.

IDaaS will relieve organizations of the need to limit their choices of authentication and risk evaluation mechanisms in a world where these will become increasingly diverse and evolve quickly, since IDaaS will have the resources to build in support for whatever is successful in the regional markets where customers live. It will do all this while using privacy enhancing technologies to remain compliant with government requirements and win public acceptance.

#### Towards a 100% policy driven identity model

IDaaS will be driven more by processes controlled through policies – workflows – than by administrators: relying on a 100% policy driven solution for digital interaction. As described hereafter, **IDaaS will morph into a flexible, policy-based, data-driven identity experience engine that orchestrates a series of actions in sequence as per executed policy.**

IDaaS will indeed act on behalf of a customer-facing application, i.e. a relying party, by automating and managing all the mechanisms through which it obtains digital identity information to enable that relying party to make at the “end of the dance” informed access control and personalization decisions about a transaction requested by a customer. Policies should be considered as a domain-specific language (DSL), i.e. “a computer language specialized to a particular application domain”[[41]](#footnote-41) with inheritance, “if” statements, polymorphism.

Product managers and business owners will be able to pick from a menu of friction-free identity experiences (sign-up, sign-in, self-service credential reset, etc.) applicable to specific scenarios, developing knowledge of customers incrementally.

Note We collectively refer to all the possible types of identity information that may be exchanged as part of the above identity experience as *claims*: claims about an end user’s authentication credential, identity vetting, communication device, physical location, personally identifying attributes, and so on.

It’s also due to the fact that IDaaS will be designed to simplify the exchange of all types of digital identity information in a consistent manner regardless of whether the underlying protocol is defined for user authentication or attribute retrieval. Likewise, the term *claims providers* can be used to collectively refer to identity providers, attribute providers and attribute verifiers when one doesn’t want to distinguish between their specific functions.

They will be able to easily reuse social network credentials and select a spectrum of identity services from high security (e.g. multi-factor authentication and verified attributes) to satisfy organizational “Know Your Consumer” (KYC) requirements up to high privacy by simplifying the process for a user to consent to release of her identity information, by preventing tracking and correlation of their online activities via “untraceable” and “unlinkable” security tokens and by avoiding unnecessary storage of a their personally identifying information by relying parties.

Note There continue to be attempts to solve these needs for strong identity assurance and verified attributes by creating attribute aggregators and/or registries. Such approaches can simplify the network interface for relying parties into a rich source of end user digital identity data. However, if aggregation services function primarily to monetize the delivery of personal identifiable information (PII), or just to simplify the direct retrieval of PII by relying parties – without sufficient involvement and protection of end users – the industry runs the risk of privacy breakdowns which will destroy consumer and citizen confidence. A user centric approach to attribute release and verification, along with its minimal disclosure technology, can mediate between relying parties and attribute sources to avoid unnecessary data aggregation.

Note Innovative technologies from research labs such [Microsoft U-Prove](http://www.microsoft.com/u-prove)[[42]](#footnote-42) allow users to minimally disclose certified information about themselves to protect the confidentiality of online user transactions against observation by 3rd party identity providers and attribute providers. An IDaaS can thus act on behalf of the end user to protect a person’s privacy and ensure consent is obtained for the release of personally identifying information to the application.

Considering the above, IDaaS will consequently have characteristics shaped by the importance of identity for both the protection of assets and the enhancement of relationships as we enter the era of the social enterprise. There is general agreement on the need to provide individuals and organizations with more “*secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation*”.

The identity experiences will thus encompass as series of actions in sequence in terms of authentication and information collection.

Note In the digital world, confidence can be based on trust in the source of a claim or correlation of claims from multiple sources. Both models must be facilitated under precise policy control. There are numerous scenarios in which a relying party requires claims that cannot be provided by a single source. For example, social identity providers almost never offer the kind of strongly vetted PII that is required to strongly identify an end user for access to valuable or sensitive information. Applications have historically relied on forms to gather this data, but self-asserted claims are not sufficient for authorizing access to sensitive resources. A modern (web) application could redirect the user’s browser to different authoritative sources. However, this would complicate application development and maintenance because at a protocol or API level there are significant differences between the interactions with all the claims providers involved in the transaction: identity providers vs. attribute providers or attribute verifiers.

These experiences will be defined as such through policies created through a flexible policy framework that provides granular control over identity experiences and behaviors for the relying parties.

Interoperability with existing relying party and (social) identity provider, attribute provider and attribute verifier infrastructures is maintained with support for industry standard protocols.

All of the above bring simplicity and confidence to the existing federation methods available today. **IDaaS will simplify and automate complex federation trust relationships setup – required to support re-use of digital identities across multiple contexts - in complex communities of interest as the ones that come along with more and more business-to-consumer scenarios. And it will shield relying parties from ongoing trust and connectivity reconfigurations (see section § Internally managed partner identities earlier in this document) as different claims providers and relying parties join or leave the community – through a policy-based, data-driven technology.**

This will require IDaaS to allow you to answer the following questions:

* *What are the legal, security, privacy and data protection policies that must be adhered to?*
* *Who are the contacts and what are the processes for becoming an accredited participant?*
* *Who are the accredited identity information providers (a.k.a. claims providers) and what do they offer?*
* *Who are the accredited relying parties [and optionally what do they require]?*
* *What are the technical “on the wire” interoperability requirements for participants?*
* *What are the operational “runtime” rules that must be enforced for exchanging digital identity information?*

To answer all these questions, IDaaS can leverage the Trust Framework construct, i.e. an internationally recognized policy construct that combines the contractual, security, privacy and compliance identity management policies subscribed to by members of a community of interest, with the configuration metadata to establish network connectivity between them for federated identity management.

As such, the Trust Framework construct provides the foundation to express policies that model an identity experience. The Appendix C. Benefiting from Trust Frameworks and policies further introduces this construct and details the notion of policies that can be articulated from this perspective.

Policies will have a consistent “developer” interface that allows a graphical and fully guided definition of the policies. Even more interestingly, policies are units of re-use for relying parties. In other words, such policies once created typically will constitute reusable identity experiences. Multiple policies of the same type may be thus designed. Product managers and business owners will be able to select any policy in any application at runtime and possibly to further customize it. This will allow them to balance privacy versus security concerns on an application by application basis by articulating suitable policies.



As an illustration, such a 100% policy driven vision without coding comes out already today in [Azure AD B2C](http://azure.microsoft.com/en-us/services/active-directory-b2c/)[[43]](#footnote-43). Azure AD B2C is "IDaaS for customers and citizens” designed with Azure AD privacy, security, availability, and scalability for customer/citizen Identity management (IAM).It’s a comprehensive, cloud-based, 100% policy driven solution where declarative policies encode the identity experiences as well as the relationships of trust and authority inside a Trust Framework (see above).

The Azure AD B2C service has been developed out of a broad dialog internationally and in conformance with requirements from a great many expert sources in government and industry, and is being exercised in multiple pilots globally. Because of its flexibility we believe it contributes to and helps provide the basis for interoperating IDaaS services world-wide.

Azure AD B2C constitutes the first version of such an identity experience engine for connecting your consumer-facing modern applications that can be integrated in any platform, and accessible from any device.



From an application perspective, and regardless of the protocol standard being used – all the widely used standards are supported -, such a “connection” will just redirect to the Azure AD B2C service specifying which policy to enforce and gets back the authenticated result of the identity experience as a set of claims with zero application complexity.

Azure AD B2C allows you to invoke the policy in an application using standard identity protocol requests to the service and the application will receive tokens with claims (customized by you) as responses. (See Appendix B. Seamlessly integrating with applications and APIs.) The identity experience engine operates as a pipeline and uses request/response claims exchanges to communicate with its internal components as well as with external entities. It enforces for regulating the assertion and consumption of claims.

Azure AD B2C is designed to abstract out the complexity of the intended interactions as per policy and make it easy for customer-facing applications to obtain the necessary claims while automatically complying with applicable security and privacy obligations. Azure AD B2C applies the related policy to decompose the request. Depending on the complexity of the request, Azure AD B2C may decompose it by farming out “pieces” of the request to separate claims providers, and initiating separate interactions with multiple claims providers. It may be necessary to ask the end user to approve specific claims providers or just to consent to release of the collective set of claims required.

Azure AD B2C provides today a unique value proposition.

#### Customizing the overall user experiences

**UI customization for the relating user experiences is key for any business-to-consumer solution.**

This indeed truly conditions the ability to delegate the identity part of the considered consumer-facing applications to IDaaS in order to not refrain people from authenticating themselves in something perceived as external/foreign. “IDaaS for customers” will be white-label solutions.

Hence IDaaS will allow to customize the look-and-feel of the above identity experience on the various pages that can be potentially served and displayed by the services via the above policies.

This can be achieved for example by crafting HTML5/CSS files as appropriate. (For security reasons, the use of JavaScript should be blocked for customization.) E.g. for that purpose, the aforementioned solution Azure AD B2C runs code in the consumer's browser and uses the modern and standard approach [Cross-Origin Resource Sharing (CORS)](http://www.w3.org/TR/cors/)[[44]](#footnote-44) to load content from a specific URL that you specify in a policy to point to the above HTML5/CSS files in lieu of providing a set of APIs you’ll have to code against. You can specify different URLs for different pages. Thank to this approach, the end users will then have consistent experiences between your application and the pages served by Azure AD B2C.

#### Entering the new world of digital marketing and gamification

IAM services for consumers may embrace some characteristics of the digital marketing solutions as such solutions enable to visualize, in terms of consumer insights, users’ data from a single dashboard using powerful tools to build audience segment and thus deliver relevant marketing campaigns. Thanks to their API-based integration path at the application level, they also allow, in terms of signals and conditional profiling, tracking onsite activities including purchase behaviors, ad clicks, etc. and on that basis building consumer rich profiles by capturing identity data.

These capabilities are definitely of interest in IDaaS. Consequently, one should therefore predict that IDaaS will notably (contribute to):

* Measure referral traffic tracking of consumer’s sites through intuitive reports.
* Helps to gain key insight into self-registration, syndication, engagement, etc.
* Provide powerful segmentation tools to visualize and segment consumer profile data.

Furthermore, to further frame the future of IDaaS in this space, these two offerings also include gamification capabilities. Generally speaking, gamification can be seen as a mean of improving consumer loyalty by rewarding consumer onsite behaviours through incentivizing users with points, badges and special offers for performing value actions on website or app.

In addition to the above characteristics, having gamification fully integrated into IDaaS will:

* Enable a seamless registration experience between gamification program and other consumer touch points.
* Allow to perform gamification actions directly to user identity to build to above consumer profiles.
* Link behavioural data to consumer profiles and reward most loyal and influential users.
* Provide insight into metrics on user behaviours and highlight top users, daily activities.
* Rank users by social loyalty and consumer engagement.

This will allow IDaaS to provide an even greater value proposition beyond all what have been discussed so far in the ability to limit the consumer churn for the organization.

**IDaaS will make B2B and B2C digital interactions for “externals” the everyday norm by eliminating technical complexity and operational overhead around interconnection and supporting Trust Frameworks as governance mechanisms defining policies that cap legal risk and guarantee compliance. Eventually, to help to amplify its power, relevancy, and utilization, IDaaS will offer above shortly discussed digital marketing and gamification capabilities.**

While much of the technology of an IDaaS will and must remain the same (e.g. directory), this will allow to accommodate many different requirements – thus the need for capabilities that interact but are honed to specific problems. E.g. for the aforementioned interactions, IDaaS will have to support tenants with billions of entities, provide options for both geo-separation and geo-replication, guarantee automated failover between replicas, operate at greater than 5 9’s among key characteristics.

In fact, this illustrates one key aspect: **the various capabilities of an IDaaS can be thought of as a continuum, so approaches as enabled by IDaaS need to be able to be mixed and deployed flexibly. Let’s further envision IDaaS at work, at home, and in spite of criminals.**

# Further envisioning IDaaS

**IDaaS will integrate identity management for people, organizations, (IoT) devices, applications, permissions, roles and groups – including the relationships between them.**

IDaaS is comprised of a series of identities capabilities. Aside the key capabilities already discussed so far, IDaaS will provide at least the capabilities discussed in the following sections, considering the relentless pace of innovation that occurs in this space.

## Providing unified information access to the directory

IDaaS will support an extensible schema for the directory to store any kind of entity information and expose a directory programming surface for storing, querying, and updating the directory, and thus sustaining the entities lifecycle management.

**Information about employees, partners, customers, devices and all the other entities it manages will be available to authorized applications of all kind anywhere through a RESTful graph-based API in lieu of classic “old-fashioned” LDAP.**

The approach of using standard RESTful interfaces to operate over a graph containing entities (nodes) and relationships/connections (arcs) between entities - often referred to as a graph interface - is already very common on the Internet nowadays. For example, much of the information in [Facebook](https://developers.facebook.com/docs/graph-api)[[45]](#footnote-45) is available in such a manner.

The directory part of IDaaS should be more than an inventory: the information on the relationships between entities is at least as important as the one that pertains to the entities. As such, a graph interface aims at providing a unified identity fabric for all object types and the connections of their instances to ultimately represent the network of things that IDaaS will have to embrace and model. The graph allows to follows the connections between entities. This is a graph that developers can use to connect their apps and services and create new compelling experiences.

Note For more information on networks and graphs, we advise reading the book entitled Networks, Crowds, and Markets: Reasoning About a Highly Connected World [Easley, July 2010].

Such a RESTful web API is by nature inter-vendor and can be extended at will to provide unified information access to the state of everything known by the organization.

Note Developers can build on this simple direct URL based access and may take advantage of the sophisticated filtering and metadata operations that are available today via the [ISO/IEC DIS 20802 Open Data Protocol (OData)](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=69208)[[46]](#footnote-46) standard.

OData is a very rich protocol, and not all of it is applicable to a directory – An IDaaS directory may support only a subset. Such directory will publish it schema and the attributes that can be used in filter expressions for scale and performance reasons. Built on standards such as HTTP, JSON and AtomPub, OData is a web protocol for unlocking and sharing data - freeing it from silos that exist in some software applications today. The OData protocol supports serialization in multiple popular formats, including JSON and Atom/XML.

The [AD Graph API](https://msdn.microsoft.com/library/azure/hh974476.aspx)[[47]](#footnote-47) available in Azure AD constitutes an illustration of such an API and a query model for applications of all kind to access an Azure AD directory tenant.

## Providing unified automatic provisioning for users, groups and roles

If IDaaS will constitute by nature a natural continuum with the on-premises IS systems, and can be ultimately perceived as one unified system for identities, IDaaS will have to ease in turn the provisioning of the SaaS applications organizations subscribe to in terms of identities, their attributes, and related supported roles.

This implicitly supposes that the considered SaaS applications expose some APIs to externally drive the provisioning. Unlike previous industry failed attempts to standardize common API set and/or markup language in this space, such as Directory Services Markup Language (DSML) in the late 90’s, and after an observation period, the [Cross-domain Identity Management (SCIM) 2.0](http://www.simplecloud.info/)[[48]](#footnote-48) standard specification is gaining popularity and will certainly have a major role to play as an open API for managing identities and provisioning workloads. Such an API will facilitate the IDaaS directory sync fabric to automatically provision (selected) identities into the targeted workloads, provided that those applications are also SCIM-based for their provisioning part.

To make that happens, the (SaaS) application must support SCIM right out-of-the-box. A SCIM-based façade will have to be built to translate between IDaaS SCIM endpoint and whatever API, interface, or mechanism the application supports for user provisioning. Once configured, IDaaS will send requests to create, modify and delete assigned users and groups to the configured SCIM-based provisioning endpoint, which can then honor those requests, and translate them into operations upon the identity store used by the application. This also implies to potentially do some mappings between the way such an information is represented in IDaaS and the way it is expected to be defined in the application.

## Registering and recognizing the identity of all the devices

IDaaS will provide unique value as a single IS for many kinds of entities – and their interrelationships. For example, its graph of users, their computers, their mobile devices, and the applications available to them is essential in Corporate-Owned Personally-Enabled (COPE)/BYOD scenarios.

### Registering the user’s devices

**IDaaS will be able to automatically register and recognize the identity of all the devices organizations interact with – not just Corporate-Owned Business-Owned (COBO) devices, but also the ones brought in by employees and partners, or used by consumers: a mobile device world.** For that purpose, IDaaS will have to interact with cloud-based (or on-premises) Enterprise Mobility Management (EMM) solutions.

Note Mobile Device Management (MDM) has evolved over the time to EMM that encompasses MDM, Mobile Application Management (MAM), and Mobile Content Management (MCM) capabilities.

The identity registration of these devices in IDaaS will further pilot their enrollment and their state into the MDM/EMM solutions with notably in a non-exhaustive manner:

* The enforcement of applicable security policies in terms of device’s configuration lockdown along with the deployment of possibly any required agent technologies that will keep track of system status and will monitor patch levels and vulnerability data,
* The provisioning of the adequate cryptographic key materials not only to sustain network-based authentication through the layer 2 802.1x protocol (supported by Extensible Authentication Protocols (EAP) like LEAP, PEAP, and TLS) but also to later generate health attestation with the check for anti-virus signatures, patches, and worms, etc. thanks to above agent(s) or other kind of attestations depending on the scenarios to sustain.

Note The MDM/EMM solutions can leverage for that purpose the [Open Mobile Alliance (OMA) Device Management (DM) specifications](http://openmobilealliance.org/about-oma/work-program/device-management/)[[49]](#footnote-49) that define as set of protocols and mechanisms allowing to deliver configuration parameters to a device.

* The controlled deployment of applications for the MAM dimension.

As implicitly suggested and to make that happens, IDaaS will have to expose for that purpose at least a RESTful web API for the devices’ registration in the IDaaS directory. Registration will result in generating a device ID, associating the user of the device with the device itself, issuing key material to prove the association, etc.

To provide a smooth integrated flow for the devices’ enrollment with the aforementioned solutions, IDaaS will use a fabric underneath to orchestrate the interaction. Hence, this fabric will expect and deeply rely on some web APIs expose in turn by the above MDM/EMM solutions, and these solutions may in turn report devices’ compliance to IDaaS based on another API... This is another illustration of the API economy with smooth and loosely-coupled integration. This is typically the approach adopted by Azure AD today[[50]](#footnote-50).

### Registering IoT devices

The same cross-object dynamics will distinguish IDaaS in the world of small, connected things and devices, commonly called IoT devices, which are transforming organizations, and will play an increasingly strong role in the computing ecosystem.

Beyond aforementioned users’ devices, IDaaS will provide integrated IAM of the ever-increasing number of IoT devices owned by organizations, from light switches, cameras, doors and sensors to robots and manufacturing equipment, and even beyond. “Existing ideas and approaches to identity management will not be entirely effective for the IoT.”[[51]](#footnote-51)

Knowledge of these IoT devices combined with knowledge of the people in their proximity, will be the basis of the control plane for intelligent buildings and physical security. Their management depends on knowing their interrelationships with users, organizations, software upgrades and service gateways. This requirement, and the scale of IoT will play dramatically to IDaaS’s strength. As stressed in the introduction, there is growing importance for concept of Identity of Things (IDoT), which is a new extension to identity, and IDaaS will “incorporate IDoT's relationship concepts into identity data and policy planning to support the scale and flexibility required by business moments using the IoT.” [Gartner, February 2015]

IDaaS vendors will ensure that their ISes embrace and play well with these IoT devices, building gateways, protocols (with the rest of the industry and at the standardization level) and infrastructure that are appropriate for the small computational power (RAM, CPU, network) that is common on these resource-constrained devices. This endeavor starts with the provisioning of these identities: “Discovery of devices, provisioning new and existing devices, authentication services for those devices and protecting data from them will account for at least 50% of the remaining security spend in organizations. [...] Protecting the endpoints will be very challenging without a means to initialize devices or their proxies with security configurations. It is also important to be able to communicate security updates to those devices. These concerns will dominate much of the IoT security markets with network segmentation between 2015 and 2020.” [Gartner, December 2015]

Note [GSMA IoT Security Guidelines](http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/)[[52]](#footnote-52) refer to currently available solutions, standards and best practice.

When discussing the IoT device provisioning, this is generally a multistep bootstrap process that occurs over the time with for instance at the very beginning a default (factory) pre-configuration and activation. This can encompass - as part of the overall process – in a non-exhaustive manner:

* The application of specific security profiles,
* The activation/deactivation of high-level services of the IoT device.
* The network integration with the setup of a global-ready (embedded) SIM card (eUICC),
* The provisioning of the correct operator settings for the considered country where the IoT device is activated.

Note As far as the latter is concerned, integration/support with related mobile enabled M2M industry standards will be certainly considered. We more specifically think of specifications like [GSMA Embedded SIM Specification](http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/SGP-02-v3-0.pdf)[[53]](#footnote-53) for the remote ‘over the air’ provisioning of M2M devices (that now includes profile interoperability) and [ETSI TS 103 383 v12.5.0 (2014-08)](http://www.etsi.org/deliver/etsi_ts/103300_103399/103383/12.05.00_60/ts_103383v120500p.pdf)[[54]](#footnote-54) - that closely relate to another flavor of device’s identity - in addition to the [OMA LightweightM2M v1.0](http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0)[[55]](#footnote-55).

System-controlled unique id and attributes, the credentials in the forms of cryptographic key materials along with all the descriptive metadata about the IoT device, - like its model and serial number, data schemas for data emitted by it, and schemas for configuration parameters controlling device behaviors, as well operations and parameters for the control actions it can execute, or what events it can observe – will be part of the registration process.

Note The [JSON Web Key (JWK)](https://tools.ietf.org/html/rfc7517)[[56]](#footnote-56) standard for the key containers used for binary secrets or RSA keys eases the definition of the key material while JSON documents provides a seamless support for metadata information.

Considering the above, a suitable provisioning API will have to encompass all the possible interaction with the IDaaS directory thanks to the previously discussed graph-based API as well as with any third-party APIs like the ones provided today as an illustration by Jasper.

Such an API will have to expose for purpose a series of verbs/operations to sustain the complete lifecycle of the IoT device like:

* “Register” to register the it in IDaaS,
* “Unregister” to remove it from IDaaS,
* “Activate” to activate it from a previously deactivated state,
* “Deactivate” to deactivates it from a previously activated state (which includes revoking access),
* “Update” to notably updates its key material and/or its metadata information over the time,
* “Reset Credentials” for a full reset of all IoT device’s credentials and tokens.

In terms of credentials and key materials, one will also certainly observe the “resurgence” of Public-key infrastructure (PKI) with its ability to represent identities in a cross-platform, multiprotocol approach. IDaaS will include or interact with lightweight “PKI-as-a-service” to issue, manage and revoke certificates for IDoT on demand and at scale.

Albeit the resource-constrained and more than diverse nature of many IoT devices makes it unfeasible for any one authentication method to address all types of IoT devices, IDaaS will also (help to) handle IoT device authentication with (a set of) standardized protocols in replacement of proprietary, ad hoc, and highly customized authentication mechanisms that may exist today.

Note [OAuth 2.0](http://tools.ietf.org/html/draft-ietf-oauth-v2)[[57]](#footnote-57) [[58]](#footnote-58) or specialized profiles that derive from such as [User-Manager Access (UMA)](https://docs.kantarainitiative.org/uma/draft-uma-core.html)[[59]](#footnote-59) already represent good candidates. Nevertheless, the game is completely open at this stage and there is room for innovation...

In this context, contextual data that originates natively on the IoT devices or that is obtained through interaction with other entities will certainly contribute providing adaptive authentication approaches and beyond that conditional access.

## Granting context-aware conditional access

**IDaaS will be able to combine its knowledge of users and contextual factors like location with knowledge of a user’s devices – including their health – (or its knowledge of IDoT and IoT devices in the specific context of IoT) to determine whether (or how much) step-up is required to protect a given resource’s access.**

It will transcend the well mastered for years’ network-centric security perimeters that have vanished, thus allowing applications to be integrated while running anywhere on any platform or hosting environment. In today federated IT and mobile world, data is the new de-facto security perimeter, identity the “gate”, and IDaaS will provide a holistic control plane for on-premises and cloud-based identity systems.

IDaaS will provide Claim Based Access Control (CBAC) for conditional access. Further, because it provides integration of authentication and authorization capabilities, it will be able to efficiently combine contextual factors (who, when, where and on what device) and concrete authorization requirements (which groups, roles and/or permissions) to leverage more intelligence to make access decisions and to construct fine-tuned authentication claims appropriate to modern applications and APIs. For example, from a device perspective, if a device is jail-broken, doesn’t have the right version of software/OS installed on it, or is unknown, access to all corporate applications and data can be blocked.



**IDaaS’s multi-tenant architecture allows cross-company permissioning problems to be solved that cannot be addressed by federating on-premises systems without undue disclosure of information.**

Furthermore, in this context, it will unify not only provisioning, attribute management, personalization, authentication, authorization, but also real-time threat analysis, alerting, dashboards, auditing, and reporting for all these entities.

## Hardening operations to resist evolving cyber-threats

With cyber-security attacks continuing to make headlines, it’s well established that security is already a top priority of organizations and consumers, and will remain top of mind. At the same time, the old security boundaries of network and device are no longer appropriate for the scenarios that people want solved. In other words, if cybersecurity used to mean building a bigger moat and a bigger wall, the new era computing environment extends far beyond the “organization’s four walls” …

### Assuming breach

The federated IT landscape has dramatically changed the security posture. “Sanctioning cloud-based services requires a new approach to security - one that “assumes breach“ - and accounts for the limitations of endpoint and perimeter defenses. […] To “assume breach” requires a shift in mindset from prevention alone to adaptation.”[[60]](#footnote-60)

This implies to admit the disturbing fact that security breaches are inevitable: digital (layers of) defenses whatever they are will be vulnerable one day if not already... Accepting such a mindset doesn’t mean to capitulate. On the contrary, this means that you have taken the first step towards mitigating the risks in the digital age[[61]](#footnote-61). *What is then the plan B? What is the plan to detect an intrusion? How to react to this type of incident?*

This implies that we move from a simple “Protect and Recover” model to a new security strategy and a more holistic posture that will encompass at least through 3 main phases: “Protect”, “Detect” and “Respond” as illustrated hereafter.

Note The risk-driven [NIST Framework for Improving Critical Infrastructure Cybersecurity](http://www.rsaconference.com/videos/machine-learning-and-the-cloud-disrupting-threat-detection-and-prevention)[[62]](#footnote-62) comprises 5 phases: “Identify”, “Protect”, “Detect”, “Respond”, and “Recover”.



In the evolving world drawn so far, **identity becomes the new and critical control plane**. **Identity is the foundation of security assurances for all information assets in the organization**. Security will be based on users’, (IoT) devices’, etc. identity, that these entities are really who they purport to be, and on centralized conditional delegation and authorization mechanisms for assets and resources, whatever they are.

Unsurprisingly and consequently, modern cyber-attackers will actively target IDaaS – as they already do today with on-premises directories - to get intellectual property and corporate assets wherever they are located. As a consequence, and to adequately contribute to organizations’ defense in depth approaches, IDaaS must have an outstanding level of security and usability to satisfy both modern scenarios and modern security requirements, and to accelerate organizations’ ability to protect, detect and respond to cyber incidents, and to ultimately help organizations adopting this new security posture.

### Building an intelligent security graph

**IDaaS will employ real-time cyber-threat analysis, taking a wide range of signals from different sources as inputs in the cloud and elsewhere.** As cyber-attacks keep getting more and more sophisticated and increasingly automated, IDaaS vendors (will) indeed need to evolve their ability to get real-time insights and predictive intelligence across the networks so they can stay a step ahead of the cyber-threats. IDaaS must be able to correlate its security data with its threat intelligence data to know good from bad. And IDaaS must leverage the industry and partners to ensure a broad, comprehensive approach. These three things align with the approach IDaaS should bring to security for its customers – a holistic, agile security platform, informed by insights from an intelligent security graph and integration with partners and the industry as a whole.

Leveraging existing and new broad and deep security signals will allow IDaaS to rapidly recognize and faster respond to entirely new modern day threats. Tapping into the immense data and signals from cloud to datacenter to endpoints, IDaaS will be able to build an intelligent security graph, formed by trillions of signals from billions of sources, that can learn from one area and apply across the platform combined with machine learning and behavioral-based approaches to profile behaviors and evaluates the activity of user and other entities, reveal trends and attack patterns, and eventually detect anomalies, suspicious activities and advanced attacks.

“By understanding how users behave and tracking legitimate processes, organizations can enlist user and entity behavior analytics (UEBA) to spot security breaches.”[[63]](#footnote-63) Intelligence will become central to detect malicious and abusive behavior that otherwise will go unnoticed. As outlined above, IDaaS will thus extensively leverage data science, and in particular machine learning, for threat prevention, detection and eventually investigation.

Note Machine learning will allow to mainly achieve two outcomes in order to tackle with different identity-based threats that IDaaS will have to consider and understand, to harden and evolve both cloud and on-premises systems, and ultimately to raise the security bar: i) next-generation of identity-based threats detection and response, and ii) simplified security, operations or policies management for protection.

As part of their sophistication, cyber-attacks use data science too as they masquerade their activities as noise, and learn quickly from mistakes. Machine learning will help IDaaS to respond to these recent developments by strengthening rule-based detections.

Supervised machine learning models will be trained by presenting them with malicious and benign examples. The model will then generalize the examples into an algorithm. This will greatly contribute to reduce triage of burden by prioritizing alerts: combining independent alert streams and providing informed scoring, each alert combining by nature multiples points: *Is the sequence of (API) calls unusual for this account? Is the IP address unusual? Does the time of access look normal? etc.*

Security expertise will be required to develop highly tuned models using a wealth of analyzed examples. This indeed supposes incorporating security analyst (and user) feedback to improve the signals to provide interpretable results and be informed why the machine learning feels it is anomalous. Since attackers - once blocked - will slightly change their behavior in order to go under the radar, developed models will react to these changes automatically to quickly adapts to moving “targets”.

Conversely, unsupervised machine learning models will work in the absence of examples

Note Threat detection demonstrates the impact of network effect. The more organizations using a service, the more inputs and cloud signals there are for detection of anomalous behavior. For example, an IP address failing authentication at numerous different organizations or other suspect patterns can become a signal informing real-time threat evaluations and accuracy is likely to rise dramatically with larger sets of input data.

Thanks to the cyber-threats detection capabilities, IDaaS will allow the identification of attackers and whom they are attacking, dynamically up-level defenses of attacked resources, etc., and of course notify the organizations that are under attack.

**In addition, IDaaS will be designed to withstand professionalized insider and outsider cyber-attacks, using cryptographic data protection to manage the risks related to storage of information and provision of access to applications.**  IDaaS will employ hardware security modules for crypto, use TPM-based software deployment mechanisms, and exclusively use multi-factor permission-based access for operator intervention.

### Towards a risk-based and adaptive policies driven IDaaS

It will do this without increasing complexity for neither application developers nor administrators. As already discussed with aforementioned policies for collaboration and agility (see section § Towards a 100% policy driven identity model), IDaaS will be driven more by processes controlled through policies – workflows – than by administrators. This not only applies to automation of provisioning, but to the very way the service is hosted, where tenants will be able to require that actions by service administrators be limited, visible and subject to their approval.

Moreover, making effective security configuration decisions is broadly speaking not easy. It requires both security experience and expertise and it’s all the more so with the federated IT world introduced earlier. Hence, to help organizations achieve greater security in the cloud but also on-premises, IDaaS will allow organizations of any size to opt in to use of mechanisms that reason over the information in their IS, and benefit from the wisdom of other organizations.

IDaaS will not only provide these organizations with better security insights but will also make suggestions and actionable recommendations about how to improve security, operations or policies. For example, a system could discover patterns in granting access to certain resources to employees with given characteristics and suggest automation or review of the granting of that privilege. Similarly, IDaaS will be able to use corporate policies to reason in a holistic way about what access to give people employing different unmanaged devices in varying locations and possibly in proximity to each other.

The ultimate goal will aim at helping organizations to both assess and know what their security performance is and what to do or what will be automatically done in order to address their own pain points in the cloud and on-premises.

These suggestions and recommendations will unsurprisingly be based on machine learning models too that will compare them for purpose to a reference group with similar needs, deployments’ configuration, activities, security logs, etc. without evidently compromising privacy for those organizations. Eventually, IDaaS will have to be conformant to privacy and security profiles mandated by regulators as introduced before.

As an illustration, Azure AD Identity Protection[[64]](#footnote-64) is a capability announced last year at the RSA Conference 2016 that provides a consolidated view into suspicious sign-in activities and potential vulnerabilities and with notifications, remediation recommendations and risk-based policies helps protect organizations’ business. By:

* Gathering and analyzing signals from billions of authentications and malicious attacks against every Microsoft on-line, enterprise and consumer, service all over the world,
* Using user behavioral analysis, advanced machine learning technologies along with data from Microsoft Security Response Center (MSRC), Microsoft Digital Crime Unit (DCU), Microsoft Malware Protection Center (MMPC), Office 365 Advanced Threat Protection[[65]](#footnote-65), and other data sources,

the service detects suspicious activities for end user and privileged (admin) identities based on signals like brute force attacks, leaked credentials, sign-ins from unfamiliar locations, infected devices, to protect organizations in real-time against from compromised accounts, identity attacks, and configuration issues. More importantly, based on these suspicious activities, it provides a consolidated view into identity threats and vulnerabilities through notifications, analysis, recommended remediation and by automate future responses: a user risk severity is computed and risk-based conditional access policies can be configured and automatically protect the identities of an organization.

Note For more information, see RSA 2016 session’s webcast [Machine Learning and the Cloud: Disrupting Threat Detection and Prevention](http://www.rsaconference.com/videos/machine-learning-and-the-cloud-disrupting-threat-detection-and-prevention)[[66]](#footnote-66).

This is a really important example on how identities of organizations can be effectively protected for current and future cyber-threats automatically, based on a well-calculated risk score without the need of constantly monitor alerts and notifications to manually act.

All of the above will require huge investments for IDaaS vendors that will have to be funded in one way or another. Albeit other IDaaS vendors already claim to offer risk-based or adaptive policies and remediation actions, no one else (at least for the moment) gathers, analyses and acts on the number and strength of signal that the above service does. As of this writing, Microsoft operates over 200 online and cloud services from a common set of infrastructure. Moreover, Microsoft services are used by over one billion customers, 20 million businesses and are delivered in over 90 markets around the world. The size of infrastructure required by these services allows Microsoft to make investments in security development and operations that are much larger than many enterprises and public sector organizations are unable to make on their own.

This said, and nevertheless, no single company can solve the security challenges that organizations already face today, which is why, as stressed before, the security ecosystem, and all of security partners, are key to such an approach. IDaaS built-in security technologies will work in tandem with those of the security ecosystem, to deliver the above drawn holistic, agile security platform.

## Providing integrated management, altering, dashboard, etc.

**IDaaS will allow integrated management, alerting, dashboard, auditing and reporting of both SaaS applications and custom line-of-business applications regardless of where they are hosted to avoid duplication of management effort.** (Doubling administration would introduce new security vulnerabilities…)

IDaaS will guarantee organizations detailed automated real-time audits of any operator actions impacting their tenant.

As already introduced, one can foresee that LOB project managers and application developers will use simple self-service portals to control the identity experiences of their employees, partners, and consumers. Compliance and risk management specialists will have a governance portal to configure corporate policies, enforcement, metrics and reports. And an IT portal will provide those responsible for the system with holistic system management, the ability to configure synchronization, dashboards and alerts.

# As a conclusion of this journey

Relentlessly turning this vision of IDaaS into reality - for let say 2020 - is not a destination but a journey for IDaaS vendors. Hence one can see success in the market for IDaaS depending on the ability of an IDaaS to execute well on a whole series of fronts beyond delivering the capabilities consistent with the vision discussed throughout this document.

We’ve started this journey with B2E interactions and the ability to project employee’s identities in the cloud to benefit from the cloud economy. As of now, the existing on-premises IT systems world is already becoming like just yet another cloud from an IDaaS perspective and for some organizations that want to. We may have already reached a paradigm shift between projecting identities to the cloud back in the early days of the identity federation and controlling and managing everything from employees and customers to the Internet of Things (IoT) from the cloud. Periodic events like the [Cloud Identity Summit](https://www.cloudidentitysummit.com/en/index.html)[[67]](#footnote-67), the [European identity & Cloud conference](https://www.id-conf.com/)[[68]](#footnote-68), the [RSA Conference](http://www.rsaconference.com/)[[69]](#footnote-69), etc. to name a few, represent more than an opportunity to see how this will evolve over the time. Perhaps most important in the long term is the [network effect](https://en.wikipedia.org/wiki/Network_effect)[[70]](#footnote-70) produced by an IDaaS in scale.

Note The concept of a network effect is well known in technology ecosystems. The core concept is that more scale in an ecosystem results in more value of that ecosystem to customers. When a business is able to harness this effect, it creates a “flywheel” where success reinforces success. Platforms that build a network effect create a powerful strategic moat that is difficult for competitors to dislodge.

An example would be the simplification of B2B interactions. If enough organizations participate in an IDaaS, it becomes absolutely simple for a person in one organization to give people from other organizations access to applications and resources. They are all wired to the same infrastructure. The more organizations there are in the service, the earlier these capabilities pay off for customers, creating a virtuous cycle. This is similar to the “friends” phenomenon in social networks. Another example would be threat detection that also demonstrates the impact of network effect. The more organizations using a service, the more inputs there are for detection of anomalous behavior.

There are a great many instances where network effect will be primary and that this will have a huge impact on the market as far as IDaaS is concerned. IDaaS vendors like Microsoft and others will concentrate on features exhibiting the network effect to maximize the impact and differentiation attainable with scale. Hence, the above journey will be paved and informed by the requirements and issues encountered in delivering IDaaS at scale and to a wide variety of customers. Furthermore, this will also require to pay deep attention to the fundamentals of reliability, privacy and security while delivering the above capabilities as a service through consistent execution and strategic staying power.

As far as Microsoft is concerned, because of the success of Office 365, its IDaaS already serves more than six million organizations and requires all the capabilities outlined in this document in order to properly steward Office 365 and other services such as Azure going forward. Microsoft’s explosive growth means that the company had to focus intensely on scale, operational robustness, defense from cyberattack and international compliance very early in the product cycle. These investments may not “visible” as features but are fundamental to the decisions customers will make about who operates their cloud identity infrastructure tomorrow. Because Office 365, Azure and all of Microsoft’s other consumer and enterprise services use Azure AD as their foundation, Microsoft’s interests in having the best IDaaS align completely with those of its customers.

# Appendix A. Seamlessly integrating with applications and APIs

In today’s world, as notably a result of the API economy (see eponym section § API Economy earlier in this document), modern applications live in an environment that includes a broad spectrum of mobile and native clients, server to server communication, and web APIs, in addition to traditional browser-and-website interactions.

## Embracing industry standard modern protocols and tokens

Interoperability with above modern applications is maintained as of today with support for industry standard modern protocols, and notably the OpenID Connect 1.0 protocol and the OAuth 2.0 protocol.

Through such standards, IDaaS will be designed to address new requirements that accompany the requirements of the modern applications.

OAuth 2.0 is more than gaining popularity in the Internet as an authorization protocol for accessing information. This is the primarily protocol for authorization and delegated authentication. Generally speaking, using OAuth 2.0, an application can gain access (with consent from the resource owner – which could be the end user or the administrator user) to impersonate the user, or users in his organization to access the resource. OAuth 2.0 is specified through the [OAuth 2.0 Authorization Framework](http://tools.ietf.org/html/rfc6749)[[71]](#footnote-71) and the [OAuth 2.0 Bearer Token Usage](http://tools.ietf.org/html/rfc6750)[[72]](#footnote-72) normative documents.

Specialized profiles that derive from OAuth 2.0 are currently being developed for IoT devices that don’t necessary “speak” HTTP. This includes in a non-exhaustive manner:

* [OAuth 2.0 Bearer Token Usage over the Constrained Application Protocol (CoAP)](https://tools.ietf.org/html/draft-tschofenig-ace-oauth-bt-01)[[73]](#footnote-73),
* [IETF Working Group’s draft standard for Object Security for CoAP](https://datatracker.ietf.org/doc/draft-selander-ace-object-security/?include_text=1)[[74]](#footnote-74),
* [The OAuth 2.0 Internet of Things (IoT) Client Credentials Grant](https://tools.ietf.org/html/draft-tschofenig-ace-oauth-iot-01)[[75]](#footnote-75).

OpenID Connect (OIDC) 1.0 defines an identity layer on top of OAuth 2.0 and represents the state of the art in modern authentication protocols. It’s a suite of lightweight specifications that provide a framework for identity interactions via REST like web APIs. It is based on OAuth 2.0. As such, [OpenID Connect Core 1.0](http://openid.net/specs/openid-connect-core-1_0.html)[[76]](#footnote-76) describes the core functionalities, and notably the request and responses messages for the supported flows, namely the authorization code flow, the hybrid flow and the implicit flow.

In addition, the [Response Type Encoding Practices](http://openid.net/specs/oauth-v2-multiple-response-types-1_0.html)[[77]](#footnote-77) and [Form Post Response Mode](http://openid.net/specs/oauth-v2-form-post-responsemode-1_0.html)[[78]](#footnote-78) normative specifications provide guidance on how to control which tokens should be returned in response to an authentication request and the HTTP mechanism that should be used to vehicle them.

Furthermore, OpenID Connect 1.0 provides:

1. A JSON configuration document (*openid-configuration.json*) as per [OpenID Connect Discovery 1.0](http://openid.net/specs/openid-connect-discovery-1_0.html)[[79]](#footnote-79) specification. This metadata information in JSON format provides configuration information such as the OAuth 2.0 endpoint locations, the signing key and issuer values to validate, etc.
2. Check session and sign-out endpoints, which allows a performant way to check if the current user session is active, thus to manipulate session, and notably how to handle distributed sign-out. These capacities are described in [OpenID Connect Session Management](http://openid.net/specs/openid-connect-session-1_0.html)[[80]](#footnote-80). In addition, as far as the latter is concerned, the [OpenID Connect HTTP-Based Logout 1.0](http://openid.net/specs/openid-connect-logout-1_0.html)[[81]](#footnote-81) draft specification deals with sign-out implementation through a more traditional mechanism (without the use of an iframe).
3. Dynamic registration capabilities with OIDC providers for client thanks to [OpenID Connect Dynamic Client Registration](http://openid.net/specs/openid-connect-registration-1_0.html)[[82]](#footnote-82).

Note Innovation is taking place as a rapid pace in this space and one should refer to the latest additions of the protocol to have a good understanding of what it provides and embraces as a whole. The various OIDC specifications are available on the [OpenID web site](http://openid.net/developers/specs/)[[83]](#footnote-83).

Note The OpenID Foundation has recently launched a certification program for OpenID Connect 1.0 implementations. For more information, see the article [The OpenID Foundation Launches OpenID Connect Certification Program](http://openid.net/2015/04/17/openid-connect-certification-program/)[[84]](#footnote-84). Having an OpenID Connect certification program provides confidence that certified implementations will "just work" together. This represents another important step on the road to widely-available secure interoperable digital identity for all the devices and applications that people use. Microsoft is proud to be a key contributor to the development of OpenID Connect 1.0 and now of its certification program.

Many of the tokens issued via the OIDC and OAuth 2.0 protocols are implemented with the JSON Web Token (JWT) format. As described in the [eponym standard](http://tools.ietf.org/html/rfc7519)[[85]](#footnote-85), JWT is a compact token format that is especially apt for REST-based development. JWT use is growing, and products supporting the format are increasingly common in the industry. The JWT format leverages the [JSON Web Signature (JWS)](https://tools.ietf.org/html/rfc7515)[[86]](#footnote-86) and [JSON Web Algorithms (JWA)](https://tools.ietf.org/html/rfc7518)[[87]](#footnote-87) specifications.

## Offering the best-of-breed support for well-established protocols and tokens

Beyond the above standard modern protocols, former identity federation protocols continue to relevantly respond to the traditional browser-and-website interactions (and potentially beyond). Considering the already existing (and potentially huge) investment of IT-based organizations in these protocols, IDaaS cannot afford not embracing them as well. There are part of the landscape and will remain here for a long time. (This said, one should confess that they are no longer the recipient of innovation for the industry.)

This translates by the support of the two following standards widely established and adopted: i) SAML 2.0, and ii) WS-Federation (WS-Fed) 1.2. These two protocols use SAML security tokens.

SAML 2.0, as a token format and a protocol, is very popular in the public sector with government agencies as well as with enterprises and educational institutions. SAML 2.0 is a suite of specifications and, as such, comprises a set of normative and non-normative documents. SAML 2.0 essentially defines XML-based **assertions** and **protocols**, **bindings**, and **profiles**.

The critical aspects of SAML 2.0 are covered in detail in the following four normative documents:

1. [Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)[[88]](#footnote-88) (SAMLCore), the core specification.
2. [Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)[[89]](#footnote-89) (SAMLBind), which maps the SAML messages onto the standard messaging or communication protocols.
3. [Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)[[90]](#footnote-90) (SAMLProf), the use cases or the “*How-to*” in regards to the use of SAML in various situations.
4. And [Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0](http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf)[[91]](#footnote-91) (SAMLConform), the operational modes for the SAML 2.0 implementations.

The term SAML Core, in relationship with the SAMLCore core specification, refers to the general syntax and semantics of SAML assertions (a.k.a. tokens) as well as the protocol used to request and transmit those assertions from one system entity to another. Most of the time, the SAML assertion you may have to consider will be the so-called "bearer" assertion, a short-lived bearer token (i.e. without a proof of possession). Such an assertion may include both an authentication statement and an attribute statement.

A SAML 2.0 protocol describes how certain SAML elements (including assertions) are packaged within SAML request and response elements, and gives the processing rules that SAML entities such as an identity provider (IdP) must follow when producing or consuming these elements. For the most part, a SAML protocol is a simple request-response protocol. It is important to keep in mind that a SAML protocol always refers to what is transmitted, and not how (the latter is determined by the choice of binding). In the context of this document, the most interesting SAML protocols are the Authentication Request Protocol, and the Artifact Resolution Protocol,

A SAML 2.0 binding determines how SAML requests and responses map onto standard messaging or communications protocols. In other words, it’s a mapping of a SAML protocol message onto standard messaging formats and/or communications protocols. SAML 2.0 completely separates the binding concept from the underlying profile (see below). The SAML 2.0 standard defines several bindings:

* HTTP Redirect (GET) binding,
* HTTP POST binding,
* HTTP Artifact binding,
* Etc.

In the parlance of SAML, A SAML 2.0 profile is a concrete manifestation of a defined use case or the “*How-to*” using a particular combination of assertions, protocols, and bindings, assertions. Indeed, it describes in detail how SAML 2.0 assertions, protocols, and bindings combine to support the considered use case, and to solve the specific related problems. The SAML 2.0 standard defines an important number of profiles:

* Web Browser SSO profile,
* Artifact Resolution profile,
* Enhanced Client or Proxy (ECP) profile,
* Etc.

The most important one is certainly the web Browser SSO profile since this is the primary SAML use case for web SSO and federation. One should also note that these profiles support various possible deployment models. The operational modes are of particular interest for IDaaS in terms of interoperability references.

Finally, WS-Fed offers a simplified path for web Browser SSO. It’s described in [Web Services Federation Language (WS-Federation) Version 1.2](http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html)[[92]](#footnote-92). The WS-Fed protocol provides a federation metadata document format that encompasses the one defined for SAML 2.0. The general syntax and semantics of metadata are defined in the aforementioned specification.

As already outlined, **federation metadata document is also of particular interest for IDaaS to automate the relationships and maintain them over the time**.

## Sustaining the most common primary scenarios

Taking into account the above landscape and the potential innovation areas, IDaaS will provide (or even already provides) a support for the following primary scenarios:



1. **Web browser to web application**. A user needs to sign in to a web application (written in .NET, PHP, Java, Ruby, Node.js, etc.) that is secured by IDaaS. For that purpose, the application typically issues an OIDC authentication request to the service, and obtain in return an ID token.
2. **Web application to web API**. A web application needs to get resources from a web API secured by IDaaS. The application performs in this case a combined OIDC and OAuth 2.0 flow, and acquires tokens using authorization codes and refresh tokens. The OAuth 2.0 authorization code flow will be typically used for that purpose.
3. **Single Page Application (SPA).** A single page application (primarily written in JavaScript, and often using dedicated frameworks like AngularJS, Durandal, Ember.js, etc.) that uses the service preview to secure its web APIs back end. The OAuth 2.0 implicit flow will be typically used for that purpose.
4. **Mobile and native application to web API**. A mobile or native application that runs on a device needs to authenticate a user to get resources from a web API that is secured by the service. The OAuth 2.0 authorization code flow will be typically used for that purpose.
5. **Daemon or server side processes to web API**. A daemon application or a server side process with no web user interface needs to get resources from a web API secured by the service. Such applications can authenticate and get tokens using an application’s identity (rather than using a user’s delegated identity) with the OAuth 2.0 client credentials flow.
6. **Standalone web APIs.**

# Appendix B. Benefiting from Trust Frameworks and policies

## Leveraging the Trust Framework and the federation management foundation

As outlined in section § Towards a 100% policy driven identity model earlier in this document, the Trust Framework (TF) construct should be understood as a written specification of the identity, security, privacy, and data protection policies to which participants in a community of interest must conform.

Federated identity provides a basis for achieving end user identity assurance at Internet scale. By delegating identity management to 3rd parties, a single digital identity for an end user can be re-used with multiple relying parties.

Identity assurance indeed requires that both identity and attribute providers adhere to specific security, privacy and operational policies and practices. Absent the ability to perform direct inspections, relying parties must develop trust relationships with the identity providers and attribute providers they choose to work with. As the number of consumers and providers of digital identity information mushrooms, it becomes untenable to continue pairwise management of these trust relationships, or even the pairwise exchange of the technical metadata required for network connectivity. Federation hubs have achieved only limited success at solving these problems.

TFs are the linchpin of the Open Identity Exchange (OIX) Trust Framework model[[93]](#footnote-93) where each community of interest is governed by a particular TF specification.

Note The Open Identity Exchange (OIX) is a non-profit trade organization of market leaders from competing business sectors e.g. the internet (Google, PayPal, etc.), data aggregation (Equifax, Experian, etc.), and telecommunications (AT&T, Verizon, etc.) driving the expansion of existing online services and the adoption of new online products. OIX helps develop and register trust frameworks: pre-negotiated sets of business, legal, and technical agreements that provide stakeholders with mutual assurance that their online transactions can be trusted. OIX members form a global center of excellence for the identity trust layer of online transactions sharing domain expertise, joint research, and pilot projects to test real world use cases.

Such a TF specification defines:

* The security and privacy metrics for the community of interest with the definition of:
  + The levels of assurance (LOA) offered/required by participants, i.e. an ordered set of confidence ratings for the authenticity of digital identity information.

Note As notably defined in NIST [SP800-63-2 Electronic Authentication Guideline](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)[[94]](#footnote-94), LOA represents confidence in how strongly the asserted identity corresponds to the real-world identity along a scale from 1 to 4, in terms of no confidence, some confidence, high confidence and very high confidence. Other standards than the NIST SP800-63-2 adopt a similar approach such as the [ISO/IEC 29115:2013](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138)[[95]](#footnote-95) standard.

* + The levels of protection (LOP) offered/required by participants, i.e. an ordered set of confidence ratings for the protection of digital identity information handled by participants in the community of interest. (LOP will be used as illustrating a corollary to LOA for measuring privacy protection on a graduated scale; but there is no corresponding standard specification for LOP at this time).
* The description of the digital identity information offered/required by participants.
* The technical policies for production and consumption of digital identity information, and thus for measuring LOA and LOP. These written policies typically include the following categories of policies:
  + Identity proofing policies: *how strongly is a person’s identity information vetted?*
  + Security policies: *how strongly are information integrity and confidentiality protected?*
  + Privacy policies: *what control does a user have over personal identifiable information (PII)?*
  + Survivability policies: continuity and protection of PII if a provider ceases operations.
* The technical profiles for production and consumption of digital identity information. These profiles:
  + Scope interfaces for which digital identity information is available at specified LOA.
  + Describe technical requirements for on-the-wire interoperability.
* The descriptions of the various roles that participants in the community may perform along with the qualifications required to fulfill these roles.

Thus a TF specification governs how identity information is exchanged between the participants of the community of interest: relying parties, identity and attribute providers, and attribute verifiers.

In the parlance of this OIX TF model, a TF specification is constituted as one or multiples documents that serve as a reference for the governance of the community of interest regulating the assertion and consumption of digital identity information within the community. This means a documented set of policies and procedures, designed to establish trust in the digital identities used for online transactions between members of a community of interest. **A TF specification defines the rules for creating a viable federated identity ecosystem for some community**.

As of today, there is widespread agreement on the benefit of such an approach and there is no doubt that trust framework specifications will facilitate the development of digital identity ecosystems with verifiable security, assurance and privacy characteristics, such that they can be reused across multiple communities of interest.

Note In terms of identity assurance, the aforementioned Kantara Initiative runs a [Trust Framework Provider (TFP) program](https://kantarainitiative.org/idassurance/)[[96]](#footnote-96). As the premier TFP aligned with the [National Strategy for Trusted Identities in Cyberspace (NSTIC)](http://www.nist.gov/nstic/)[[97]](#footnote-97) program in the US, this programs approves identity and attributes providers.

For that reason, the aforementioned 100% policy driven Azure AD B2C service leverages specification as its core as the basis of its data representation for a TF to facilitate interoperability. Azure AD B2C represents a TF specification as a mixture of human and machine readable data: some sections of this model (typically those more oriented towards governance) are represented as references to published security and privacy policies documentation along with the related procedures if any, while other sections describe in detail the configuration metadata and runtime rules to facilitate operational automation.

## Articulating policies for identities experiences

In terms of implementation at the IDaaS level, the above TF specification will typically consist in a set of “policies” that allow complete control over identity behaviors and experiences.

E.g. Azure AD B2C allows you to author and create your own TF through such declarative policies that can define and configure:

* The document reference(s) defining the federated identity ecosystem of the community that relates to the TF. They are links to the TF documentation.
* The (predefined) operational “runtime” rules, a.k.a. the “user journeys” that automate and/or control the exchange and usage of the claims. These user journeys are associated with a LOA (and a LOP). A policy may therefore have user journeys with varying LOAs (and LOPs).
* The identity and attribute providers, a.k.a. the claims providers, in the community of interest and the technical profiles they support along with the (out-of-band) LOA/LOP accreditation that relates to them.
* The integration with attribute verifiers, a.k.a. the claims providers.
* The relying parties in the community (by inference).
* The metadata for establishing network communications between participants. These metadata along with the technical profiles will be used in the course of a transaction to plumb “on the wire” interoperability between the relying party and other community participants.
* The protocol conversion if any (SAML 2.0, WS-Fed, OAuth 2.0, and OIDC).
* The authentication requirements.
* The “step-up” authentication method orchestration if any.
* A shared schema for all the claims available and mappings to participants of a community of interest.
* All the claims transformations - along with the possible data minimization in this context - to sustain the exchange and usage of the claims.
* The blinding and encryption.
* The claims storage.
* Etc.

Thus they govern how identity information is exchanged between a relying party, identity and attribute providers, and attribute verifiers. They control which identity and attribute providers are required for a relying party’s authentication and what level of privacy is required.

These policies constitute the machine readable portion of the TF construct in Azure AD B2C with all the operational details (claims providers’ metadata and technical profiles, claims schema definition, claims transformation functions, and user journeys, etc.) filled in (for a specific community of interest) to facilitate operational orchestration and automation.

They are assumed to be “living documents” in Azure AD B2C since there is more than a chance that their contents will change over time with respect to the active participants declared in the policies, and also potentially in some situations to the terms and conditions for being a participant.

Federation setup and maintenance are vastly simplified by shielding relying parties from ongoing trust and connectivity reconfigurations as different claims providers/verifiers join or leave (the community represented by) the set of policies.

Interoperability is another significant challenge as additional claims providers/verifiers have to be integrated, since relying parties are unlikely to support all of the necessary protocols. Azure AD B2C solves this problem by supporting industry standard protocols and by applying specific “user journeys” to transpose requests when relying parties and attribute providers do not support the same protocol.

Users journeys include protocol profiles and metadata that will be used to plumb “on the wire” interoperability between the relying party and other participants. There are also operational “runtime” rules that will be applied to identity information exchange request/response messages for enforcing compliance with published policies as part of the TF specification. The idea of user journeys is key to the customization of customer experience and sheds light on how the system works at the protocol level.

On that basis, relying party applications and portals can, depending on their context, invoke Azure AD B2C passing the name of a specific policy and get precisely the behavior and information exchange they want without any muss, fuss or risk.

# Terminology

**Community of interest**: grouping of organizations which agree to specific terms and conditions for the exchange of digital identity information to improve trust, security and privacy of online transactions.

**Trust Framework**: internationally recognized policy construct that combines the contractual, security, privacy and compliance identity management policies subscribed to by members of a community of interest, with the configuration metadata to establish network connectivity between them for federated identity management.

**End user**: person who is attempting to perform an operation at a relying party that requires authentication, and possibly the evaluation of attributes as authorization data.

**Relying party (RP)**: (aka Service Provider) organization that offers online applications or resources to end users, and relies upon authentication results and attributes about end users to make access control decisions.

**Identity assurance**: confidence that the digital identity of a party to an online transaction corresponds to the asserted real-world identity of that party. Identity assurance can apply to both the end user and relying party.

**Level of assurance (LOA)**: measure of identity assurance specifically applied to end users. As notably defined in NIST [SP800-63-2 Electronic Authentication Guideline](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)[[98]](#footnote-98), LOA represents confidence in how strongly the asserted identity corresponds to the real-world identity along a scale from 1 to 4, in terms of no confidence, some confidence, high confidence and very high confidence. Other standards than the NIST SP800-63-2 adopt a similar approach such as the [ISO/IEC 29115:2013 “Information technology - Security techniques - Entity authentication assurance framework”](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45138)[[99]](#footnote-99) standard.

**Level of protection (LOP)**: measure of confidence in the privacy protection provided for identity information that is disclosed between participants in a community of interest. LOP will be used in this document as illustrating a corollary to LOA for measuring privacy protection on a graduated scale; but there is no corresponding standard specification for LOP at this time.

**Attribute**: data item that describes any characteristic that might be evaluated to identify an end user or make an access control decision. In addition to “traditional attributes” (e.g. name, address, group memberships) we include characteristics of the end-user’s i) authentication credential (e.g. type or strength), ii) human identity proofing, ii) device or iv) location.

**Claim**: assertion about a fact that cannot be directly verified by the relying party, and for which the relying party must develop sufficient confidence to grant the end user’s requested transaction.

**Identity provider**: organization that performs an end user authentication operation, and upon success provides at least one attribute it maintains about that subject, a digital identifier. It may declare the LOA associated the authentication event. It may also return other attributes about the end user.

**Attribute provider**: organization that provides attributes about a specific end user. An attribute provider does not provide information about any current authentication operation as does an IdP.

**Attribute verifier**: organization that accepts a set of attributes about an end-user, and confirms that they match a dataset in some authoritative system of record (e.g. drivers’ licenses, credit ratings). An attribute verifier may provide additional information about the dataset (e.g. SSN refers to a deceased person).

**Digital identity information providers**: or just providers, is a collective reference to identity providers, attribute providers and attribute verifiers.

# References

## Books

* [Bertocci, January 2016]: Vittorio Bertocci, January 2016, Modern Authentication with Azure Active Directory for Web Applications, ISBN 978-0735696945, MS Press, https://www.microsoftpressstore.com/store/modern-authentication-with-azure-active-directory-for-9780735696945
* [Dhanjani, August 2015]: Nitesh Dhanjani, August 2015, Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts, ISBN 978-1-4919-0233-2, O’Reilly, http://shop.oreilly.com/product/0636920033547.do
* [Easley, July 2010]: David Easley, Jon Kleinberg, July 2010, Networks, Crowds, and Markets: Reasoning About a Highly Connected World, ISBN 978-0521195331, Cambridge University Press, http://www.cambridge.org/gb/knowledge/isbn/item2705443
* [Moore, December 2005]: Geoffrey Moore, December 2005, Dealing with Darwin, ISBN 978-1591841074, http://www.dealingwithdarwin.com/theBook/introduction.php

## Supplemental materials

* [Deloitte, January 2015]: Deloitte, January 2015, API economy from systems to business services, http://dupress.com/articles/tech-trends-2015-what-is-api-economy/
* [Forrester, May 2014]: Forrester, May 2014, Hybrid environments Demand Coordinated IAM for both Security and Agility, https://azureinfo.microsoft.com/CO-Azure-CNTNT-FY15-07Jul-HybridEnvDemandCoordinatedIAM-Registration-Page.html?ls=Media&lsd=UKPaidProgramme
* [Gartner, November 2012]: Gartner, November 2012, 2013 Planning Guide: Identity and Privacy, http://www.gartner.com/id=2221415
* [Gartner, February 2015]: Gartner, February 2015, The Identity of Things for the Internet of Things, https://www.gartner.com/doc/2975217/identity-things-internet-things
* [Gartner, June 2015]: Gartner, June 2015, Magic Quadrant for Identity and Access Management as a Service, Worldwide, https://info.microsoft.com/Gartner-Magic-Quadrant-EMS.html?ls=Website
* [Gartner, December 2015]: Gartner, June 2016, Predicts 2016: Security for the Internet of Things, ttp://www.gartner.com/reprints/microsoft?id=1-2X78PVU&ct=160127&st=sb
* [Gartner, June 2016]: Gartner, June 2016, Magic Quadrant for Identity and Access Management as a Service, Worldwide, https://info.microsoft.com/EMS-IDaaS-MQ-2016.html[)](https://info.microsoft.com/EMS-IDaaS-MQ-2016.html).
* [KuppingerCole, June 2014]: KuppingerCole, June 2014, Leadership Compass Cloud User and Access Management, Report No.: 70969, https://azure.microsoft.com/files/leadership-compass.pdf
* [McKinsey, June 2015]: McKinsey Global Institute, June 2015, The Internet of Things: Mapping the value beyond the hype, http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Business%20Technology/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking\_the\_potential\_of\_the\_Internet\_of\_Things\_Executive\_summary.ashx

|  |
| --- |
| The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.  This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.  Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.  Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.  © 2017 Microsoft Corporation. All rights reserved.  The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.  Microsoft, list Microsoft trademarks used in your white paper alphabetically are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.  The names of actual companies and products mentioned herein may be the trademarks of their respective owners. |

1. Don't Get Ubered: APIs Hold Key to Digital Transformation: http://www.forbes.com/sites/danwoods/2015/10/19/dont-get-ubered-apis-hold-key-to-digital-transformation/ [↑](#footnote-ref-1)
2. Why The API Economy Is Exploding: http://www.forbes.com/sites/tomtaulli/2015/11/30/why-the-api-economy-is-exploding/ [↑](#footnote-ref-2)
3. Internet of Things: http://en.wikipedia.org/wiki/Internet\_of\_Things [↑](#footnote-ref-3)
4. Ibid [↑](#footnote-ref-4)
5. The Internet of Things: http://www.gartner.com/it-glossary/internet-of-things/ [↑](#footnote-ref-5)
6. Overview of the Internet of things: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559 [↑](#footnote-ref-6)
7. Mass Adoption of the Internet of Things Will Create New Opportunities and Challenges for Enterprises: https://www.gartner.com/doc/2994817/mass-adoption-internet-things-create [↑](#footnote-ref-7)
8. Unlocking the potential of the Internet of Things: http://www.mckinsey.com/insights/business\_technology/the\_internet\_of\_things\_the\_value\_of\_digitizing\_the\_physical\_world [↑](#footnote-ref-8)
9. Internet of Things: From Research and Innovation to Market Deploy: http://www.internet-of-things-research.eu/cluster\_book.htm [↑](#footnote-ref-9)
10. Unlocking the potential of the Internet of Things: http://www.mckinsey.com/insights/business\_technology/the\_internet\_of\_things\_the\_value\_of\_digitizing\_the\_physical\_world [↑](#footnote-ref-10)
11. GE Software Annual Report Highlights the Industrial Internet and GE Predictivity: https://www.gesoftware.com/news-events/featured-stories/annual-report-highlights-industrial-internet-and-ge-predictivity-0 [↑](#footnote-ref-11)
12. What Securing the Internet of Things Means for CISOs: https://www.gartner.com/doc/2706521/securing-internet-things-means-cisos [↑](#footnote-ref-12)
13. The Internet of Things: Sizing up the opportunity: http://www.mckinsey.com/insights/high\_tech\_telecoms\_internet/the\_internet\_of\_things\_sizing\_up\_the\_opportunity [↑](#footnote-ref-13)
14. Ibid [↑](#footnote-ref-14)
15. Identity management: https://en.wikipedia.org/wiki/Identity\_management [↑](#footnote-ref-15)
16. Security Assertion Markup Language (SAML) 2.0: http://go.microsoft.com/fwlink/?LinkId=193996 [↑](#footnote-ref-16)
17. Web Services Federation Language (WS-Federation) Version 1.2: http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.pdf [↑](#footnote-ref-17)
18. Liberty Interoperable certification program: http://www.projectliberty.org/liberty/liberty\_interoperable [↑](#footnote-ref-18)
19. Kantara initiative: http://kantarainitiative.org/ [↑](#footnote-ref-19)
20. Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf [↑](#footnote-ref-20)
21. Identity Management as a Service: http://www.identityblog.com/?p=1205 [↑](#footnote-ref-21)
22. Ibid [↑](#footnote-ref-22)
23. ISO/IEC 27001:2013 “Information technology -- Security techniques -- Information security management systems – Requirements”: http://www.iso.org/iso/home/store/catalogue\_tc/catalogue\_detail.htm?csnumber=54534 [↑](#footnote-ref-23)
24. Cloud Controls Matrix (CCM) v3.0.1: https://cloudsecurityalliance.org/research/ccm/ [↑](#footnote-ref-24)
25. CSA Security, Trust and Assurance Registry (STAR): https://cloudsecurityalliance.org/star/ [↑](#footnote-ref-25)
26. Azure Active Directory: https://azure.microsoft.com/en-us/services/active-directory/ [↑](#footnote-ref-26)
27. Azure Active Directory Marketplace: https://azure.microsoft.com/en-us/marketplace/active-directory/ [↑](#footnote-ref-27)
28. Publish applications using Azure AD Application Proxy: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-application-proxy-publish [↑](#footnote-ref-28)
29. Integrating your on-premises identities with Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect [↑](#footnote-ref-29)
30. Coming later this CY’17 [↑](#footnote-ref-30)
31. Monitor your on-premises identity infrastructure and synchronization services in the cloud: https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health [↑](#footnote-ref-31)
32. Using Azure AD Connect Health for sync: https://docs.microsoft.com/fr-fr/azure/active-directory/connect-health/active-directory-aadconnect-health-sync [↑](#footnote-ref-32)
33. Using Azure AD Connect Health with AD FS: https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health-adfs [↑](#footnote-ref-33)
34. Using Azure AD Connect Health with AD DS: https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health-adds [↑](#footnote-ref-34)
35. Azure AD federation compatibility list: https://docs.microsoft.com/fr-fr/azure/active-directory/connect/active-directory-aadconnect-federation-compatibility [↑](#footnote-ref-35)
36. #AzureAD a leader in the 2016 Gartner IDaaS MQ!: https://blogs.technet.microsoft.com/enterprisemobility/2016/06/07/azuread-a-leader-in-the-2016-gartner-idaas-mq/ [↑](#footnote-ref-36)
37. Target Breach Began with Contractor's Electronic Billing Link: http://www.wsj.com/articles/SB10001424052702304450904579367391844060778 [↑](#footnote-ref-37)
38. Home Depot: Someone's WEAK-ASS password SECURITY led to breach: http://www.theregister.co.uk/2014/11/07/home\_depot\_megabreach/ [↑](#footnote-ref-38)
39. Emotional design: https://en.wikipedia.org/wiki/Emotional\_Design [↑](#footnote-ref-39)
40. UK Cabinet Office Web site, Identity assurance: enabling trusted transactions: http://www.cabinetoffice.gov.uk/resource-library/identity-assurance-enabling-trusted-transactions [↑](#footnote-ref-40)
41. Domain-specific language: https://en.wikipedia.org/wiki/Domain-specific\_language [↑](#footnote-ref-41)
42. Microsoft U-Prove: http://www.microsoft.com/u-prove [↑](#footnote-ref-42)
43. Azure Active Directory B2C: http://azure.microsoft.com/en-us/services/active-directory-b2c/ [↑](#footnote-ref-43)
44. Cross-Origin Resource Sharing W3C Recommendation 16 January 2014: http://www.w3.org/TR/cors/ [↑](#footnote-ref-44)
45. Facebook Graph API: https://developers.facebook.com/docs/graph-api [↑](#footnote-ref-45)
46. ISO/IEC DIS 20802-1 “Information technology -- Open data protocol (OData) v4.0 -- Part 1: Core”: http://www.iso.org/iso/home/store/catalogue\_tc/catalogue\_detail.htm?csnumber=69208 [↑](#footnote-ref-46)
47. AD Graph API: https://msdn.microsoft.com/library/azure/hh974476.aspx [↑](#footnote-ref-47)
48. System for Cross-domain Identity Management (SCIM) 2.0: http://www.simplecloud.info/ [↑](#footnote-ref-48)
49. OMA Device Manage Working Group: http://openmobilealliance.org/about-oma/work-program/device-management/ [↑](#footnote-ref-49)
50. Azure Active Directory integration with MDM: https://msdn.microsoft.com/windows/hardware/commercialize/customize/mdm/azure-active-directory-integration-with-mdm [↑](#footnote-ref-50)
51. The Internet of Things Identity Crisis – A Gartner Q&A with Earl Perkins: http://www.gartner.com/smarterwithgartner/the-internet-of-things-identity-crisis-a-gartner-qa-with-earl-perkins/ [↑](#footnote-ref-51)
52. GSMA IoT Security Guidelines: http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/ [↑](#footnote-ref-52)
53. GSMA Remote Provisioning Architecture for Embedded UICC Technical Specification Version 3.0 30 June 2015: http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/SGP-02-v3-0.pdf [↑](#footnote-ref-53)
54. ETSI TS 103 383 V12.5.0 (2014-08) Smart Cards; Embedded UICC; Requirements Specification (Release 12): http://www.etsi.org/deliver/etsi\_ts/103300\_103399/103383/12.05.00\_60/ts\_103383v120500p.pdf [↑](#footnote-ref-54)
55. OMA LightweightM2M v1.0: http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0 [↑](#footnote-ref-55)
56. JSON Web Key (JWK): https://tools.ietf.org/html/rfc7517 [↑](#footnote-ref-56)
57. RFC 6749 The OAuth 2.0 Authorization Framework: http://tools.ietf.org/html/rfc6749 [↑](#footnote-ref-57)
58. RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage: http://tools.ietf.org/html/rfc6750 [↑](#footnote-ref-58)
59. User-Managed Access (UMA) Profile of OAuth 2.0: https://docs.kantarainitiative.org/uma/draft-uma-core.html [↑](#footnote-ref-59)
60. How SaaS Adoption Is Changing Cloud Security: http://www.darkreading.com/perimeter/how-saas-adoption-is-changing-cloud-security-/a/d-id/1316015 [↑](#footnote-ref-60)
61. Assumption of breach: How a new mindset can help protect critical data: http://searchsecurity.techtarget.com/tip/Assumption-of-breach-How-a-new-mindset-can-help-protect-critical-data [↑](#footnote-ref-61)
62. NIST Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [↑](#footnote-ref-62)
63. Detect Security Breaches Early by Analyzing Behavior: http://www.gartner.com/smarterwithgartner/detect-security-breaches-early-by-analyzing-behavior/ [↑](#footnote-ref-63)
64. Azure AD Identity Protection: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection [↑](#footnote-ref-64)
65. Exchange Online Advanced Threat Protection Service Description: https://technet.microsoft.com/en-us/library/exchange-online-advanced-threat-protection-service-description.aspx [↑](#footnote-ref-65)
66. Machine Learning and the Cloud: Disrupting Threat Detection and Prevention: http://www.rsaconference.com/videos/machine-learning-and-the-cloud-disrupting-threat-detection-and-prevention [↑](#footnote-ref-66)
67. Cloud Identity Summit: https://www.cloudidentitysummit.com/en/index.html [↑](#footnote-ref-67)
68. European identity & Cloud conference: https://www.id-conf.com/ [↑](#footnote-ref-68)
69. RSA Conference: http://www.rsaconference.com/ [↑](#footnote-ref-69)
70. Network effect: https://en.wikipedia.org/wiki/Network\_effect [↑](#footnote-ref-70)
71. RFC 6749 The OAuth 2.0 Authorization Framework: http://tools.ietf.org/html/rfc6749 [↑](#footnote-ref-71)
72. RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage: http://tools.ietf.org/html/rfc6750 [↑](#footnote-ref-72)
73. The OAuth 2.0 Bearer Token Usage over the Constrained Application Protocol (CoAP): https://tools.ietf.org/html/draft-tschofenig-ace-oauth-bt-01 [↑](#footnote-ref-73)
74. Object Security of CoAP (OSCOAP): https://datatracker.ietf.org/doc/draft-selander-ace-object-security/?include\_text=1 [↑](#footnote-ref-74)
75. The OAuth 2.0 Internet of Things (IoT) Client Credentials Grant: https://tools.ietf.org/html/draft-tschofenig-ace-oauth-iot-01 [↑](#footnote-ref-75)
76. OpenID Connect Core 1.0 incorporating errata set 1: http://openid.net/specs/openid-connect-core-1\_0.html [↑](#footnote-ref-76)
77. OAuth 2.0 Multiple Response Type Encoding Practices: http://openid.net/specs/oauth-v2-multiple-response-types-1\_0.html [↑](#footnote-ref-77)
78. OAuth 2.0 Form Post Response Mode: http://openid.net/specs/oauth-v2-form-post-responsemode-1\_0.html [↑](#footnote-ref-78)
79. OpenID Connect Discovery 1.0 incorporating errata set 1: http://openid.net/specs/openid-connect-discovery-1\_0.html [↑](#footnote-ref-79)
80. OpenID Connect Session Management 1.0 - draft 25: http://openid.net/specs/openid-connect-session-1\_0.html [↑](#footnote-ref-80)
81. OpenID Connect HTTP-Based Logout 1.0 - draft 03: http://openid.net/specs/openid-connect-logout-1\_0.html [↑](#footnote-ref-81)
82. OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 1: http://openid.net/specs/openid-connect-registration-1\_0.html [↑](#footnote-ref-82)
83. OpenID Specifications & Developer Information: http://openid.net/developers/specs/ [↑](#footnote-ref-83)
84. The OpenID Foundation Launches OpenID Connect Certification Program: http://openid.net/2015/04/17/openid-connect-certification-program/ [↑](#footnote-ref-84)
85. RFC 7519 JSON Web Token (JWT): http://tools.ietf.org/html/rfc7519 [↑](#footnote-ref-85)
86. RFC 7515 JSON Web Signature (JWS): https://tools.ietf.org/html/rfc7515 [↑](#footnote-ref-86)
87. RFC 7518 JSON Web Algorithms (JWA): https://tools.ietf.org/html/rfc7518 [↑](#footnote-ref-87)
88. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf [↑](#footnote-ref-88)
89. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf [↑](#footnote-ref-89)
90. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf [↑](#footnote-ref-90)
91. Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf [↑](#footnote-ref-91)
92. Web Services Federation Language (WS-Federation) Version 1.2 OASIS Standard: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html [↑](#footnote-ref-92)
93. OIX Trust Framework Model: see http://openidentityexchange.org [↑](#footnote-ref-93)
94. NIST SP800-63-2 Electronic Authentication Guideline: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf [↑](#footnote-ref-94)
95. ISO/IEC 29115:2013 “Information technology - Security techniques - Entity authentication assurance framework: http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=45138 [↑](#footnote-ref-95)
96. Kantara Initiative Trust Framework Provider program: https://kantarainitiative.org/idassurance/ [↑](#footnote-ref-96)
97. National Strategy for Trusted Identities in Cyberspace**:** http://www.nist.gov/nstic/ [↑](#footnote-ref-97)
98. NIST SP800-63-2 Electronic Authentication Guideline: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf [↑](#footnote-ref-98)
99. ISO/IEC 29115:2013 “Information technology - Security techniques - Entity authentication assurance framework”: http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=45138 [↑](#footnote-ref-99)