



Identity as a Service (IDaaS)

Go, change the world®

- Identity as a Service, or IDaaS companies supply cloud-based authentication or identity management to enterprises who subscribe.
- IDaaS companies supply cloud-based authentication or identity management to enterprises who subscribe. The X-as-a-service model in information technology is easy to understand.
- The X-as-a-service model in information technology is easy to understand. It means some feature is being delivered or served to a company through a remote connection from a third-party provider, as opposed to a feature being managed on site and by in-house personnel alone.
- Think of local email, such as Microsoft Outlook or Thunderbird, operating primarily on one's own computer versus cloud email, such as Gmail, being provided to users as a service through web connections. Identity, security, and other features can similarly be provided as a service.
- The goal of an Identity Service is to ensure users are who they claim to be, and to give them the right kinds of access to software applications, files, or other resources at the right times. If the infrastructure to make this happen is built on site, then the company has to figure out what to do every time a problem comes up.



Identity as a Service (IDaaS)

Go, change the world®

- If Bring Your Own Device (BYOD) employees are changing to different types of phones, for example, the local identity provisioning has to adapt immediately.
- It is much simpler to implement a centralized cloud-based system created by identity experts who have already solved such problems for hundreds of organizations.
- Services that provide digital identity management as a service have been part of internetworked systems from Day One. Like so many concepts in cloud computing, IDentity as a Service is a FLAVor (Four Letter Acronym) of the month, applied to services that already exist.
- The Domain Name Service can run on a private network, but is at the heart of the Internet as a service that provides identity authorization and lookup. The name servers that run the various Internet domains (.COM, .ORG, .EDU, .MIL, .TV, .RU, and so on) are IDaaS servers.
- DNS establishes the identity of a domain as belonging to a set of assigned addresses, associated with an owner and that owner's information, and so forth. If the identification is the assigned IP number, the other properties are its metadata.



Identity as a Service (IDaaS)

Go, change the world®

- An identity is a set of characteristics or traits that make something recognizable or known. In computer network systems, it is one's digital identity that most concerns us.
- A digital identity is those attributes and metadata of an object along with a set of relationships with other objects that makes an object identifiable.
- Not all objects are unique, but by definition a digital identity must be unique, if only trivially so, through the assignment of a unique identification attribute. An identity must therefore have a context in which it exists.
- This description of an identity as an object with attributes and relationships is one that programmer's would recognize.
- Databases store information and relationships in tables, rows, and columns, and the identity of information stored in this way conforms to the notion of an entity and a relationship or alternatively under the notion of an object role model (ORM) and database architects are always wrestling with the best way of reducing their data set to a basic set of identities.
- You can extend this notion to the idea of an identity having a profile and profiling services such as Facebook as being an extension of the notion of Identity as a Service in cloud computing.



An identity can belong to a person and may include the following:

- Things you are: Biological characteristics such as age, race, gender, appearance, and so forth.
- Things you know: Biography, personal data such as social security numbers, PINs, where you went to school, and so on
- Things you have: A pattern of blood vessels in your eye, your fingerprints, a bank account you can access, a security key you were given, objects and possessions, and more
- Things you relate to: Your family and friends, a software license, beliefs and values, activities and endeavors, personal selections and choices, habits and practices, an iGoogle account, and more.



Identity as a Service (IDaaS)

Go, change the world®

- To establish your identity on a network, you might be asked to provide a name and password, which is called a single-factor authentication method.
- More secure authentication requires the use of at least two-factor authentication; for example, not only name and password (things you know) but also a transient token number provided by a hardware key (something you have).
- To get to multifactor authentication, you might have a system that examines a biometric factor such as a fingerprint or retinal blood vessel pattern—both of which are essentially unique things you are.
- Multifactor authentication requires the outside use of a network security or trust service, and it is in the deployment of trust services that our first and most common IDaaS applications are employed in the cloud.
- Of course, many things have digital identities. User and machine accounts, devices, and other objects establish their identities in a number of ways.
- For user and machine accounts, identities are created and stored in domain security databases that are the basis for any network domain, in directory services, and in data stores in federated systems.
- Network interfaces are identified uniquely by Media Access Control (MAC) addresses, which alternatively are referred to as Ethernet Hardware Addresses (EHAs). It is the assignment of a network identity to a specific MAC address that allows systems to be found on networks.



Identity as a Service (IDaaS)

Go, change the world®

- The manner in which Microsoft validates your installation of Windows and Office is called Windows Product Activation and creates an identification index or profile of your system, which is instructive.
- **During activation, the following unique data items are retrieved:**
 - A 25-character software product key and product ID
 - The uniquely assigned Global Unique Identifier or GUID
 - PC manufacturer
 - CPU type and serial number
 - BIOS checksum
 - Network adapter and its MAC address
 - Display adapter
 - SCSCI and IDE adapters
 - RAM amount
 - Hard drive and volume serial number
 - Optical drive
 - Region and language settings and user locale



Identity as a Service (IDaaS)

Go, change the world®

- From this information, a code is calculated, checked, and entered into the registration database.
- Each of these uniquely identified hardware attributes is assigned a weighting factor such that an overall sum may be calculated. If you change enough factors NIC and CPU, display adapter, RAM amount, and hard drive—you trigger a request for a reactivation based on system changes.
- This activation profile is also required when you register for the Windows Genuine Advantage program. Windows Product Activation and Windows Genuine Advantage are cloud computing applications, albeit proprietary ones.
- Whether people consider these applications to be services is a point of contention.



Networked identity service classes *Go, change the world®*

- To validate Web sites, transactions, transaction participants, clients, and network services various forms of identity services—have been deployed on networks.
- Ticket or token providing services, certificate servers, and other trust mechanisms all provide identity services that can be pushed out of private networks and into the cloud.
- Identity protection is one of the more expensive and complex areas of network computing. If you think about it, requests for information on identity by personnel such as HR, managers, and others.
- By systems and resources for access requests; as identification for network traffic; and the myriad other requirements mean that a significant percentage of all network traffic is supporting an identification service.
- Literally hundreds of messages on a network every minute are checking identity, and every Ethernet packet contains header fields that are used to identify the information it contains.
- As systems become even more specialized, it has become increasingly difficult to find the security experts needed to run an ID service. Identity as a Service or the related hosted (managed) identity services may be the most valuable and cost effective distributed service types you can subscribe to.



Networked identity service classes *Go, change the world®*

- Identity as a Service (IDaaS) may include any of the following:
 - Authentication services (identity verification)
 - Directory services
 - Federated identity
 - Identity governance
 - Identity and profile management
 - Policies, roles, and enforcement
 - Provisioning (external policy administration)
 - Registration
 - Risk and event monitoring, including audits
 - Single sign-on services (pass-through authentication)
- The sharing of any or all of these attributes over a network may be the subject of different government regulations and in many cases must be protected so that only justifiable parties may have access to the minimal amount that may be disclosed.
- This level of access defines what may be called an identity relationship



Identity system codes of conduct

Go, change the world®

- Certain codes of conduct must be observed legally, and if not legally at the moment, then certainly on a moral basis. Cloud computing services that don't observe these codes do so at their peril. In working with IDaaS software, evaluate IDaaS applications on the following basis:
- **User control for consent:** Users control their identity and must consent to the use of their information.
- **Minimal Disclosure:** The minimal amount of information should be disclosed for an Intended use.
- **Justifiable access:** Only parties who have a justified use of the information contained in a digital identity and have a trusted identity relationship with the owner of the information may be given access to that information.
- **Directional Exposure:** An ID system must support bidirectional identification for a public entity so that it is discoverable and a unidirectional identifier for private entities, thus protecting the private ID.
- **Interoperability:** A cloud computing ID system must interoperate with other identity services from other identity providers.
- **Unambiguous human identification:** An IDaaS application must provide an unambiguous mechanism for allowing a human to interact with a system while protecting that use against an identity attack.
- **Consistency of Service:** An IDaaS service must be simple to use, consistent across all its uses, and able to operate in different contexts using different technologies.



IDaaS interoperability

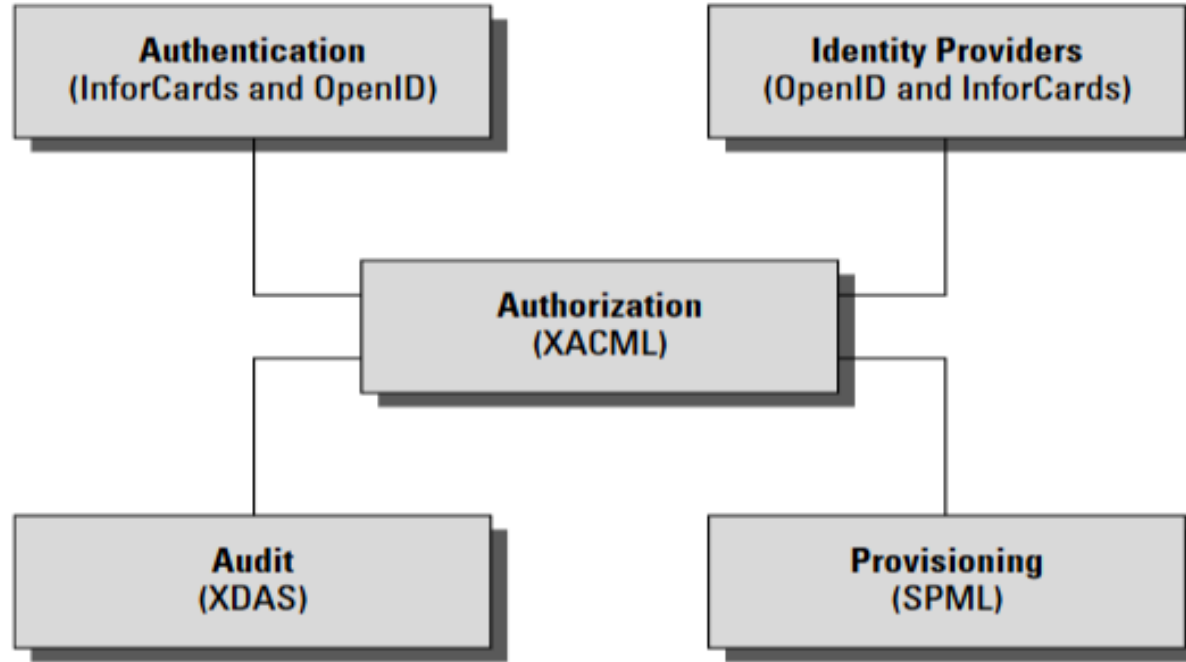
- Identity as a Service provides an easy mechanism for integrating identity services into individual applications with minimal development effort, by allowing the identification logic and storage of an identity's attributes to be maintained externally.
- Cloud computing IDaaS applications must rely on a set of developing industry standards to provide interoperability. The following are among the more important of these services:
- **User centric authentication** (usually in the form of information cards): The OpenID and CardSpace specifications support this type of data object.
- **The XACML Policy Language:** This is a general-purpose authorization policy language that allows a distributed ID system to write and enforce custom policy expressions.
- **XACML can work with SAML;** when SAML presents a request for ID authorization, XACML checks the ID request against its policies and either allows or denies the request.
- **The SPML Provisioning Language:** This is an XML request/response language that is used to integrate and interoperate service provisioning requests. SPML is a standard of OASIS's Provision Services Technical Committee (PSTC) that conforms to the SOA architecture.
- **The XDAS Audit System:** The Distributed Audit Service provides accountability for users accessing a system, and the detection of security policy violations when attempts are made to access the system by unauthorized users or by users accessing the system in an unauthorized way.



IDaaS interoperability

Go, change the world®

Open standards that support an IDaaS infrastructure for cloud computing





IDaaS interoperability

- The Identity Governance Framework (IGF) is a standards initiative of the Liberty Alliance (<http://www.projectliberty.org/>) that is concerned with the exchange and control of identity information using standards such as WS-Trust, ID-WSF, SAML, and LDAP directory services.
- The Liberty Alliance was established by an industry group in 2001 with the purpose of promoting open identity interchanges through policy standards that applications can use to enforce privacy as well as to allow privacy auditing.
- In 2009, this group released its Client Attribute Requirements Markup Language (CARML) and a set of IGF Privacy Constraints that forms the basis of the open source project called Aristotle ([http://www.openliberty.org/wiki/index.php/ ProjectAris](http://www.openliberty.org/wiki/index.php/ProjectAris)), which has as its goal the creation of an API for identity interchange.



User authentication

- OpenID is a developing industry standard for authenticating “end users” by storing their digital identity in a common format. When an identity is created in an OpenID system, that information is stored in the system of any OpenID service provider and translated into a unique identifier.
- Identifiers take the form of a Uniform Resource Locator (URL) or as an Extensible Resource Identifier (XRI) that is authenticated by that OpenID service provider. Any software application that complies with the standard accepts an OpenID that is authenticated by a trusted provider.
- A very impressive group of cloud computing vendors serve as identity providers (or OpenID providers), including AOL, Facebook, Google, IBM, Microsoft, MySpace, Orange, PayPal, VeriSign, LiveJournal, Ustream, Yahoo!, and others.
- The OpenID standard applies to the unique identity of the URL; it is up to the service provider to store the information and specify the forms of authentication required to successfully log onto the system.
- Thus an OpenID authorization can include not only passwords, but smart cards, hardware keys, tokens, and biometrics as well. OpenID is supported by the OpenID Foundation (<http://openid.net/foundation/>), a not-for-profit organization that promotes the technology.



User authentication

- These are samples of trusted providers and their URL formats:
- Blogger: <username>.blogger.com or <blogid>.blogspot.com
- MySpace: mspace.com/<username>
- Google: <https://www.google.com/accounts/o8/id>
- Google Profile: [google.com/profiles/<username>](https://www.google.com/profiles/<username>)
- Microsoft: accounts.services.passport.net/
- MyOpenID: <username>.myopenid.com
- Orange: openid.orange.fr/username or simply orange.fr/
- Verisign: <username>.pip.verisinglabs.com
- WordPress: <username>.wordpress.com
- Yahoo!: openid.yahoo.com
- After you have logged onto a trusted provider, that logon may provide you access to other Web sites that support OpenID.
- When you request access to a site through your browser (or another application that is referred to as a user-agent), that site serves as the “relying party” and requests of the server or server-agent that it verify the end-user’s identifier.



User authentication

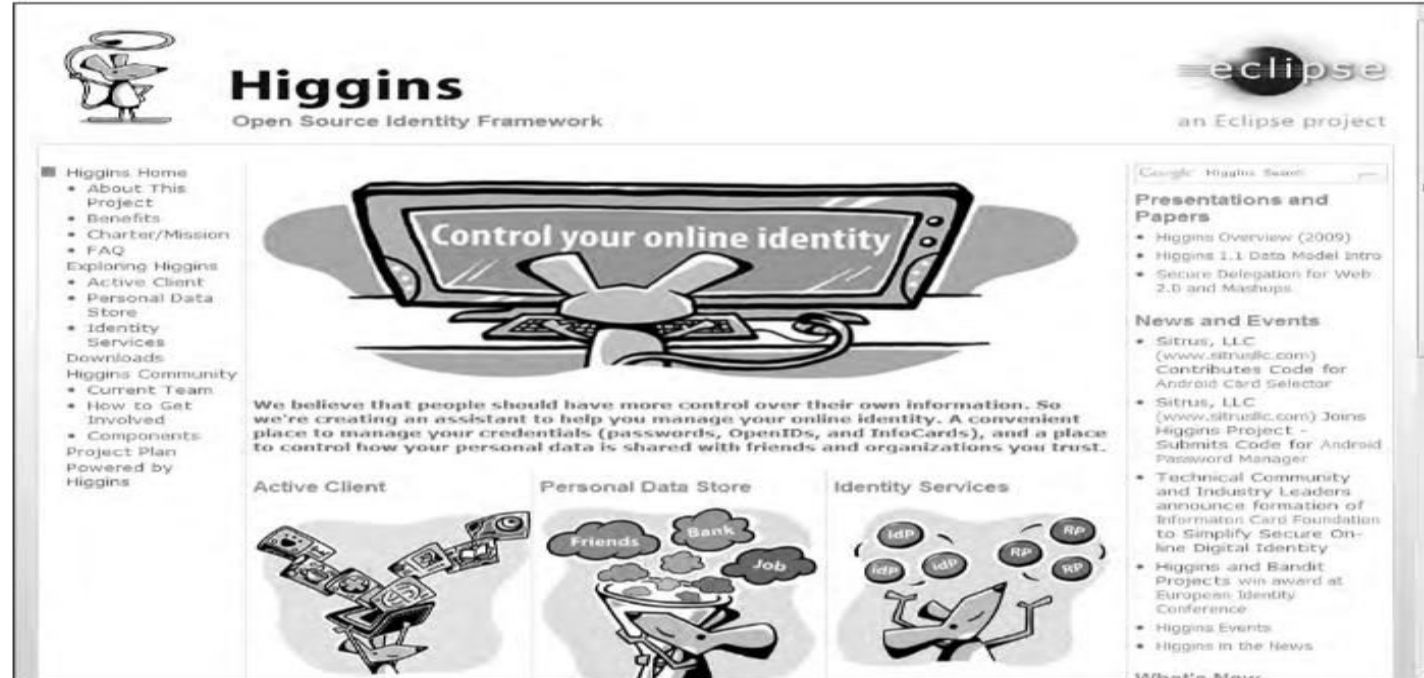
- CardSpace is a Microsoft software client that is part of the company's Identity Metasystem and built into the Web Services Protocol Stack.
- This stack is built on the OASIS standards (WS-Trust, WS-Security, WS-SecurityPolicy, and WS-MetadataExchange), so any application that conforms with the OASIS WS- standards can interoperate with CardSpace. CardSpace was introduced with .NET Frameworks 3.0 and can be installed on Windows XP, Server 2003, and later.
- It is installed by default on Windows Vista and Windows 7.
- CardSpace offers another way of authenticating users in the cloud. An Information Card may be requested with an HTML <OBJECT> tag, and the trusted Identity Provider then creates an encrypted and digitally signed token using the Security Token Service (STS) that is part of a WS-Trust request/ reply mechanism.
- CardSpace may be seen as an alternative mechanism to the use of OpenID and SAML and is used to sign into those services as well as Windows Live ID accounts.



This is a private CardSpace Identification Card. Managed Identification Cards that store similar information are stored on a network service and can be shared to the cloud.



The Higgins Open Source Identity Framework uses an i-Card metaphor and interoperable identity service APIs to create a vendor-neutral cloud-based authentication service.



The screenshot shows the Higgins Open Source Identity Framework website. The header features the Higgins logo (a stylized bird) and the text "Higgins Open Source Identity Framework". To the right is the Eclipse logo with the text "an Eclipse project".

The main content area is titled "Control your online identity" and features a large illustration of a computer monitor displaying a stylized 'X' shape. Below the monitor, a paragraph states: "We believe that people should have more control over their own information. So we're creating an assistant to help you manage your online identity. A convenient place to manage your credentials (passwords, OpenIDs, and InfoCards), and a place to control how your personal data is shared with friends and organizations you trust."

The website is divided into three main sections:

- Active Client:** Illustrates a user's active client with a stack of i-cards.
- Personal Data Store:** Illustrates a user's personal data store with a cloud containing "Friends", "Bank", and "Job".
- Identity Services:** Illustrates a user's identity services with a cloud containing "IdP", "Rp", and "WP".

The left sidebar contains a navigation menu:

- Higgins Home
 - About This Project
 - Benefits
 - Charter/Mission
 - FAQ
- Exploring Higgins
 - Active Client
 - Personal Data Store
 - Identity Services
- Downloads
- Higgins Community
 - Current Team
 - How to Get Involved
 - Components
- Project Plan
- Powered by Higgins

The right sidebar contains a search bar and two sections:

- Presentations and Papers:**
 - Higgins Overview (2009)
 - Higgins 1.1 Data Model Intro
 - Secure Delegation for Web 2.0 and Mashups
- News and Events:**
 - Sitrus, LLC (www.sitrusllc.com) Contributes Code for Android Card Selector
 - Sitrus, LLC (www.sitrusllc.com) Joins Higgins Project - Submits Code for Android Password Manager
 - Technical Community and Industry Leaders announce formation of Information Card Foundation to Simplify Secure Online Digital Identity
 - Higgins and Bandit Projects win award at European Identity Conference
 - Higgins Events
 - Higgins in the News

At the bottom of the right sidebar is a section titled "What's New".



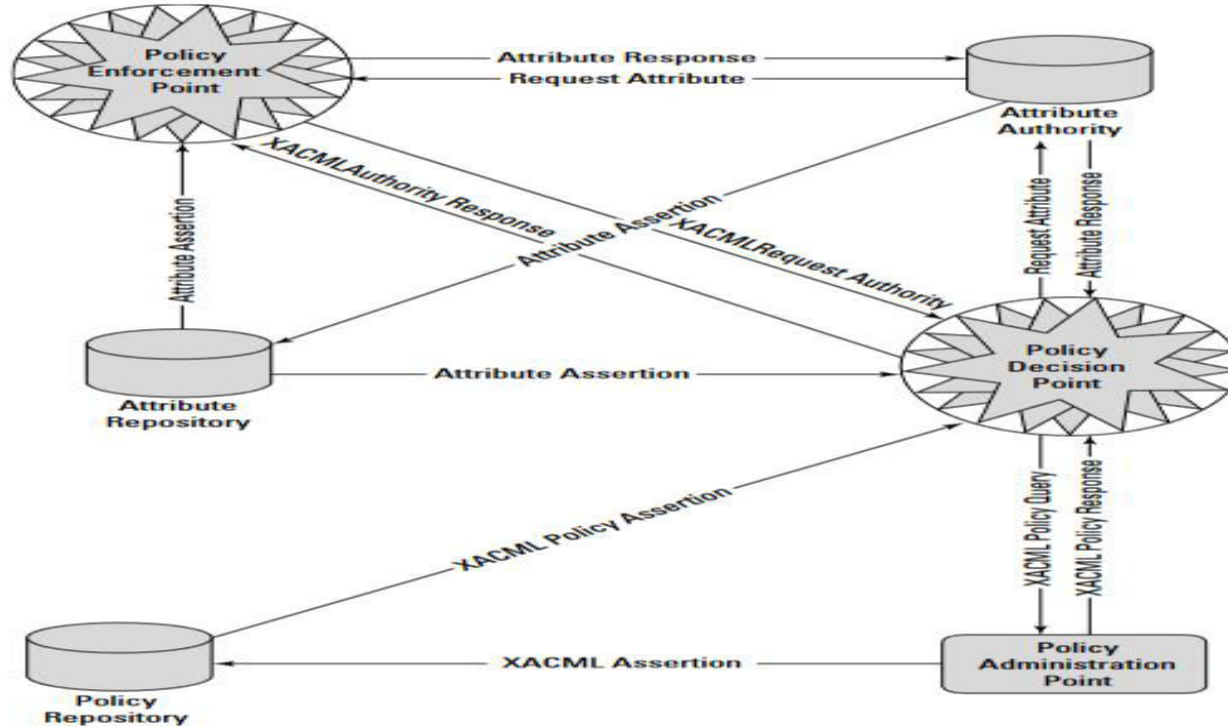
Authorization Markup Languages *Go, change the world®*

- Information requests and replies in cloud computing are nearly always in the form of XML replies or requests. XML files are text files and are self-describing.
- That is, XML files contain a schema that describes the data it contains or contains a point to another text file with its schema.
- A variety of specialized XML files are in the identity framework, the ones of note being XACML and SAML, shown in Figure.
- The eXtensible Access Control Markup Language (XACML) is an OASIS standard (see <http://xml.coverpages.org/xacml.html>) for a set of policy statements written in XML that support an authentication process.
- A policy in XACML describes a subject element that requests an action from a resource. These three elements operate within an environment that also can be described in terms of an Action element.
- Subject and Action elements (which are terms of art in XACML) are elements that can have one or more attributes. Resources (which are services, system components, or data) have a single attribute, which is usually its URL.



Authorization Markup Languages *Go, change the world®*

SAML integrates with XACML to implement a policy engine in a Service Oriented Architecture to support identity services authorization.

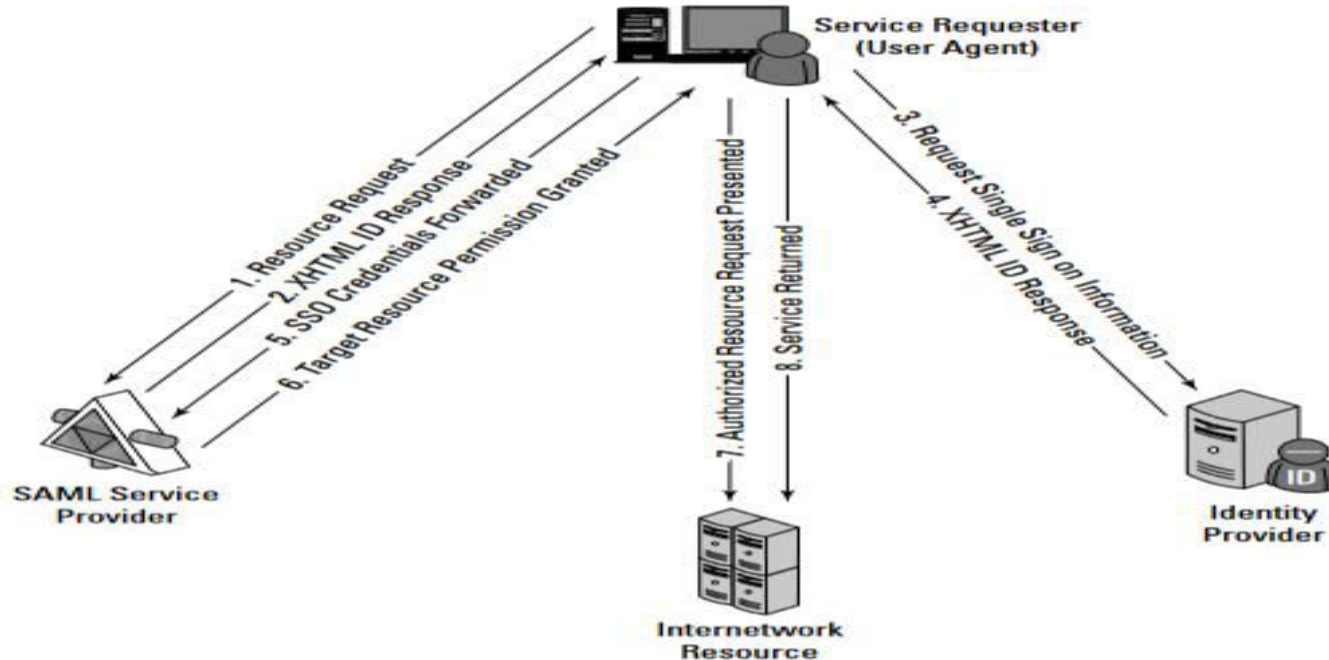




Authorization Markup Languages *Go, change the world®*

SAML provides a mechanism by which a service requester can use a Single Sign On logon to access Web services securely.

SAML Single Sign On Request/Response Mechanism





Authorization Markup Languages *Go, change the world®*

- A SAML assertion is a security statement in the SAML file that makes a claim regarding authentication, attributes, or authorization.

The statement is of this form:

- Assertion X created at Time T by User U about Subject S is true when Conditions Care TRUE.
- It is up to the identity provider to parse this statement and determine its validity. The SAML protocol request is often referred to as a query; the three different supported query types are an authentication query, an attribute query, and an authorization decision query.
- SAML requests use a SOAP binding; that is, the SAML request or response is embedded in a SOAP wrapper within an HTTP message.
- SAML is used to provide a mechanism for a Web Browser Single Sign On (SSO). In this instance, a Web browser is the user agent, which requests access to a resource that is authorized by a SAML service provider.



Authorization Markup Languages *Go, change the world®*

- The service provider takes a request from a user for access to the resource and sends an authentication request to the SAML identity provider directly from the initiating user agent (Web browser). Figure shows the SAML Single Sign On Request/Response mechanism.
- The Service Provisioning Markup Language (SPML) is another of the OASIS open standards developed to provide for service provisioning. Provisioning is the process by which a resource is prepared for use, reserved, accessed, used, and then released when the transaction is completed. A classic example of provisioning a resource is the reservation and use of a phone line or a Virtual Private Network.
- A provisioning system has three types of components: A Requesting Authority (RA) is the client, the Provisioning Service Point (PSP) is the cloud component that receives the request and returns a response to the RA, and a Provisioning Service Targets (PST) is the software application upon which the provisioning action is performed.
- The SPML provisioning system (which can be thought of as an architectural layer) means that identity information need only be entered into these three components once. SPML is used to prepare Web services and applications for use, signal that the resource is available for use and waiting for instructions, and signal when the use or transaction has been completed.
- With SPML, a system can provide automated user and system access, enforce access rights, and make cloud computing services available across network systems. Without a provisioning system, a cloud computing system can be very inefficient and potentially unreliable.



Identity as a Service (IDaaS)-Benefits *Go, change the world®*

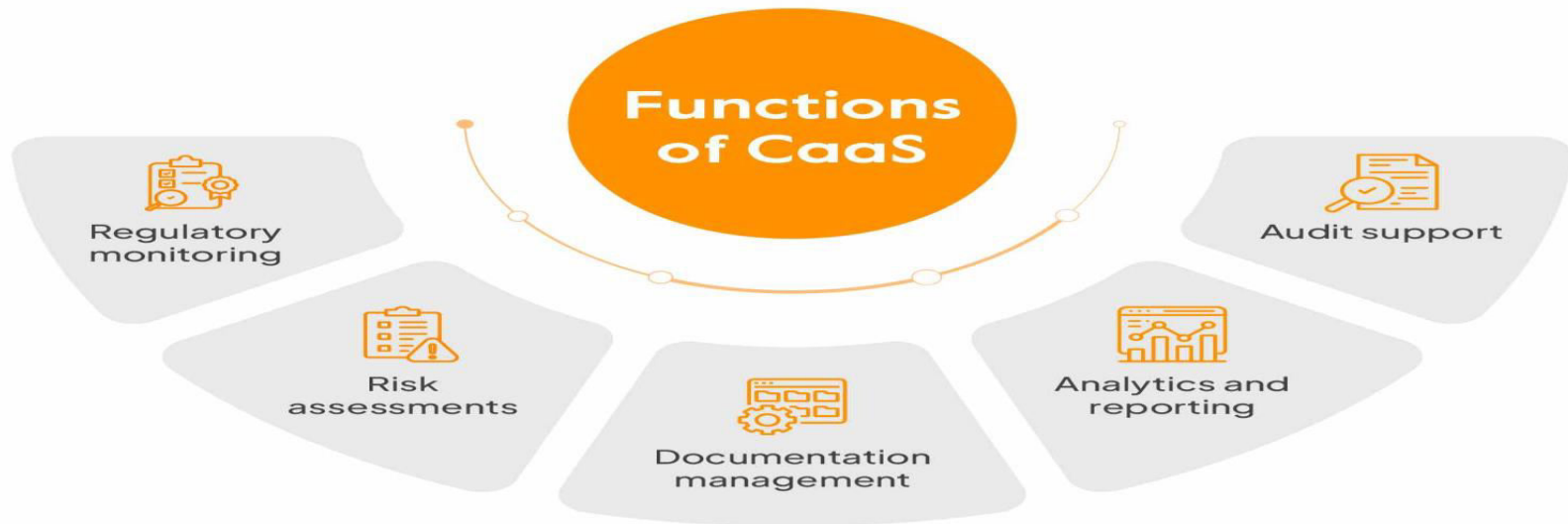
- Advantage of IDaaS is savings.
- Provisioning identity on site, with software such as Active Directory Domain Services, can be full of costs.
- Your team has to keep up servers; purchase, upgrade, and install software; back up data regularly; pay hosting fees; monitor the additional turf on premises for network security; set up VPNs; and much more.
- With IDaaS, costs drop to the subscription fee and the administration work.
- Besides savings, ROI for IDaaS includes improved cybersecurity and saved time with faster logins and fewer password resets.
- Whether a user is signing in from open WiFi at an airport or from a desk in the office, the process is seamless and secure.
- The improved security can keep companies from facing a hack or breach that might topple their business.



Compliance as a Service (CaaS)

Go, change the world®

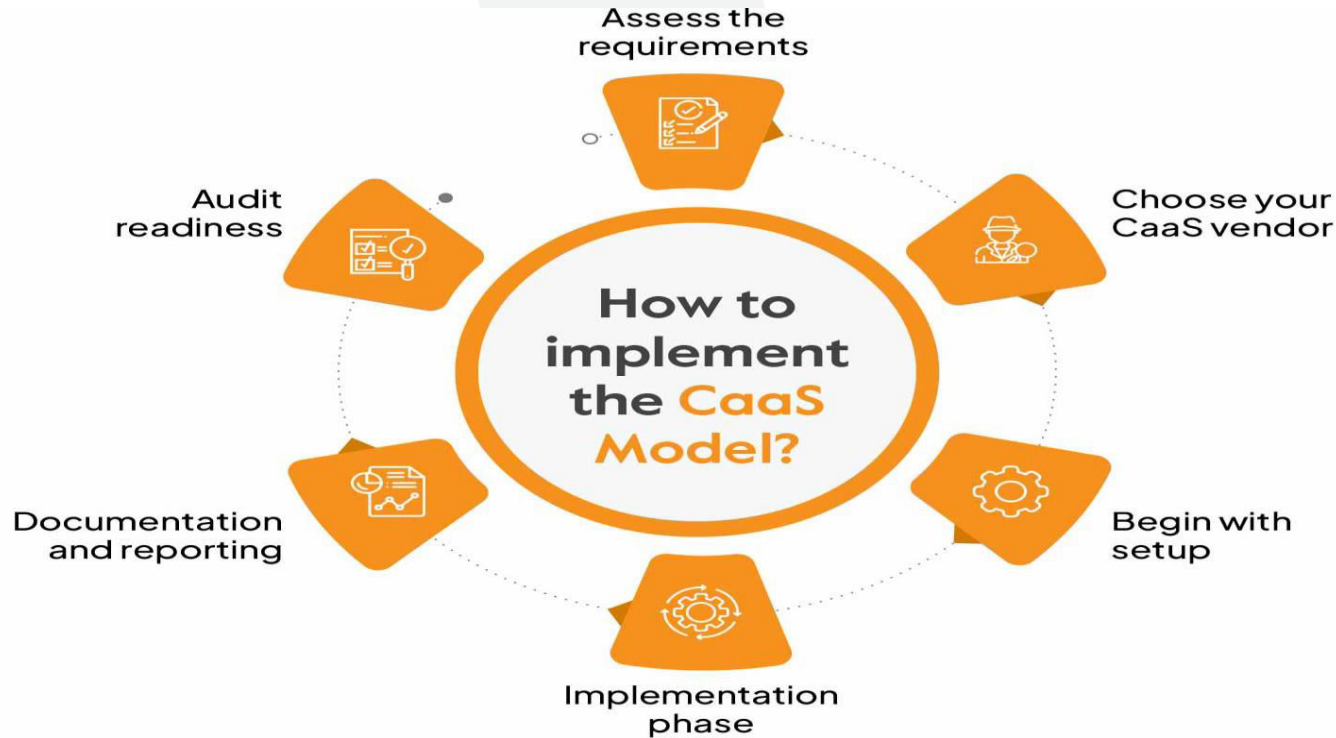
- Compliance as a Service (CaaS) is a cloud-based model that helps organizations meet regulatory compliance requirements by outsourcing compliance management to a third party.
- Compliance implementation, management and maintenance services to regulated companies in various industries, often such as healthcare, financial and government.





Compliance as a Service (CaaS)

Go, change the world®





Compliance as a Service (CaaS)

Go, change the world®

- Cloud computing by its very nature spans different jurisdictions. The laws of the country of a request's origin may not match the laws of the country where the request is processed, and it's possible that neither location's laws match the laws of the country where the service is provided.
- Compliance is much more than simply providing an anonymous service token to an identity so they can obtain access to a resource. Compliance is a complex issue that requires considerable expertise.
- While Compliance as a Service (CaaS) appears in discussions, few examples of this kind of service exist as a general product for a cloud computing architecture.
- A Compliance as a Service application would need to serve as a trusted third party, because this is a man-in-the-middle type of service. CaaS may need to be architected as its own layer of a SOA architecture in order to be trusted.
- A CaaS would need to be able to manage cloud relationships, understand security policies and procedures, know how to handle information and administer privacy, be aware of geography, provide an incidence response, archive, and allow for the system to be queried, all to a level that can be captured in a Service Level Agreement.
- CaaS has the potential to be a great value-added service



- In order to implement CaaS, some companies are organizing what might be referred to as “verticalclouds,” clouds that specialize in a vertical market.

Examples of vertical clouds that advertise CaaS capabilities include the following:

- **athenahealth** (<http://www.athenahealth.com/>) for the medical industry
- **bankserv** (<http://www.bankserv.com/>) for the banking industry
- **ClearPoint** PCI Compliance-as-a-Service for merchant transactions under the Payment Card Industry Data Security Standard
- **FedCloud** (<http://www.fedcloud.com/>) for government
- **Rackserve** PCI Compliant Cloud (<http://www.rackspace.com/>; another PCI CaaS service)
- CaaS system built inside a private cloud where the data is under the control of a single entity, thus ensuring that the data is under that entity’s secure control and that transactions can be audited. Indeed, most of the cloud computing compliance systems to date have been built using private clouds.
- CaaS could be an incredibly valuable service. A well-implemented CaaS service could measure the risks involved in servicing compliance and ensure or indemnify customers against that risk.
- CaaS could be brought to bear as a mechanism to guarantee that an e-mail conformed to certain standards, something that could be a new electronic service of a network of national postal system and something that could help bring an end to the threat of spam.