Identity Relationship and Access Management for the Extended Enterprise

Benefits in External Identity Management

GLOBALSIGN WHITE PAPER

www.globalsign.com

CONTENTS

INTRODUCTION

Once again the way companies are doing business is transforming. The Internet brought along lots of changes, and now we are seeing that even the most traditional industries such as manufacturing, energy production, utilities, construction, and processing are embracing the web at large. The trend is clear - companies need to gain competitive advantages and diversify their offering. Producing electricity is no longer enough as smart homes, smart metering and more demanding customers emerge.

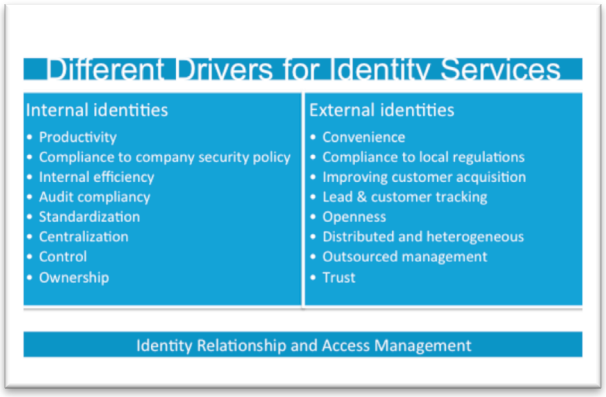
Businesses in general are adding more and more online services to their portfolio, no matter what the industry or vertical they are operating. Company boundaries are blurring as businesses interact closely and utilize online services in growing numbers.

This growing business ecosystem includes a lot of different stakeholders from customers, partners, and subcontractors to owners and investors. Companies need to engage each stakeholder category in different ways. One service for all will not cut it. Each stakeholder has their own motivation to do business with a provider. They have their own business processes, infrastructure, and identities. When the number of external stakeholders grow, so does the need to better manage these identities. It is not enough to know *who* is accessing your online services, but also *in which role / capacity* they enter, or who they *represent*.

Traditional Identity Management solutions, which concentrate on provisioning employee identities from the HR -system to the Active Directory, and providing Single Sign-On to internal applications are ill-suited for this situation. New ways of thinking is required to improve convenience and loyalty towards customers, to deploy secure online services, to minimize the cost in customer acquisition and external identity management.

INTERNAL VS EXTERNAL IDENTITIES

When an investment decision is reached to deploy an Identity Management or Identity Relationship Management product there are always business driven factors behind it. It might be about regulatory demands, desire to cut cost, improve security etc. These driving factors are different when we look at internal vs external identities. This translates to different demands to the solutions companies need to select in order to satisfy the business objectives.



Let's take a closer look at these different factors, and explain them.

Productivity vs Convenience

The technology behind is Single Sign-On, but the driver might be different. Internally the wish is to increase productivity by enabling employees to login into company applications without repeated password entry. For external identities SSO brings convenience for the business customer as they can login from their corporate network to the online services with their own business IDs.

Compliance

There's a different emphasis for compliancy in internal and external identities. The driver internally is to comply to the security policy, which might take into account local regulations. Compliance to local regulations typically means that sometimes it might be necessary to enforce stronger authentication to grant access to sensitive information, and maybe use a credential which has a security level described by the local legislation / regulation (e.g. NIST or STORK).

Efficiency vs Customer Acquisition

Workflows such as inviting people to use a service or requesting access privileges with the tools the IAM provides can improve internal efficiency. But for external identities it's a tool to facilitate customer acquisition process by enabling e.g. sales people to invite leads and customers to use the services directly from the CRM.

Audit vs Lead and Customer Tracking

Improving the quality of the data (what happened, who used and what resource, i.e. logs) has different drivers internally vs externally. Internally it is important to have good audit trails available, but for external identities the same audit trail can provide data which can be used to

better target existing customers with upsell opportunities and converting leads into paying customers faster.

Standardization vs Openness

Identity Provider can be used internally to standardize access policies and methods, and connect to separate internal identity silos whereas the same Identity Provider should enable the business to integrate various kinds of technologies and standards that the external resources use. An internal corporate network gravitates towards standardization whereas the external networks that a B2B service provider wants to connect will remain heterogeneous and diverse.

Centralized vs Distributed and Heterogeneous

Again the underlying technology would be the Identity Provider (IdP) and much the same way as in standardization companies wish to centralize the access policies and decision points. Externally the IdP should support also decision making points within the customer organization (who can access) and let the customers manage their own privileges. This means that even though internally the company might select a single standard or process to follow, for external connected identities and networks they need to embrace diverse options.

Internal Control vs Outsourced & Tiered Management

Employees and their access credentials as well as authorization should be controlled internally. Externally it makes much more sense to let the customer organization attach (authorize) access privileges to their employees. This would save a lot of effort for the company offering the online service to external companies i.e. customers.

Ownership vs Trust

Companies want to own their employee identities at least to some extent. The concept of Bring Your Own ID (BYOD) might change this to some degree, but still the ownership of access privileges (roles, authorizations) should remain in the control of the company for internal identities. For external identities trust is much more important as an online service provider should be able to trust the identities coming from the customer domain, and trust that their access privileges are properly maintained within the customer organization.

Most of the underlying technologies for managing internal and external identities are similar. However, when you can standardize a lot of the infrastructure, software platforms, processes, and authentication methods within your internal environment, you must be able to support a wide range of diverse and heterogeneous customer settings if you wish to offer the extended enterprise experience for your corporate customers.

In essence the internal and external identity management practices are polarizing. Internal identity and access management products which concentrate on streamlining the employee life-cycle management from start to finish have been around for years, and they have gravitated towards certain models best suited for internal corporate processes. External identity management needs to engage customers, enable service providers develop and launch new business models, embrace and support a diverse set of requirements, improve convenience for the end user, enable cost savings, shorten the sales cycle, and more. The fluid business ecosystems that can be nurtured and extended using properly deployed external identity management can make a big impact on the bottom line for any service provider, manufacturer, utility company, retailer, financial or healthcare institute, or even the government.

WHY INVEST IN IDENTITY RELATIONSHIP AND ACCESS MANAGEMENT

A lot of the arguments in favor for adopting identity relationship and access management solutions for both internal and external identity management are similar. There are however benefits which can be clearly assigned to external identity management.

Cost Management (Reduction)

Identity and access management is a tool to reduce cost related to identities, but also to improve effectiveness of the operations both internally and externally, and enable new online services that in turn can be used to automate and smoothen things bringing in new ways to manage cost of operations.

Here are some of the functions within your company where cost savings can be achieved:

- Help / Service desk calls: According to studies having self service functions for end users to reset passwords reduced help desk calls related to forgotten passwords by over 90%. This applies for both internal and external identities. However internally an employee might have to remember only a few passwords, but if he's using 5-10 external services, the password fatigue will play a major role and users

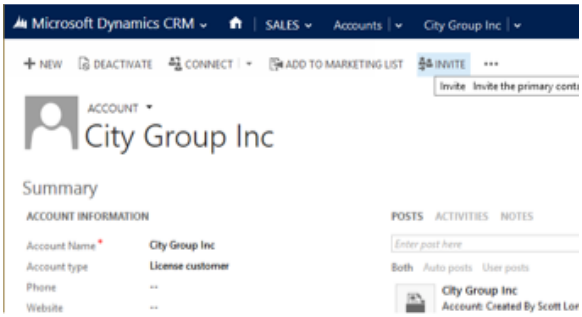
either forget the passwords quickly or start using poor / repeated passwords.

- No password management: If the IAM solution can provide Single Sign-On for the customers of the B2B service, password management related costs, such as reset costs, can be avoided completely.
- Account provisioning / registration: The B2B service provider has to provision their own internal accounts (employees), and internal IAM can help in that by automation and workflows. A greater effect can be seen in external identities if the B2B provider can simply rely on business identities coming from the customer network. There would be no need for separate account provisioning and life-cycle management for the B2B provider. External Identity Relationship management products such as GlobalSign CustomerID can link the customer to the B2B service and provide life-cycle management functions that the customer organization can utilize. This would minimize cost related to customer account or identity management for the B2B provider.

Business Performance

The simple metric for business performance is profit. If you are able to increase your profits you are performing better. Identity, authorization and access management solutions can help in ways that you might not have thought of. Here are some examples:

- Customer satisfaction: If you can provide for example SSO to your services, your customers will be happy. A satisfied customer will spread the word, and you will get an increase in the number of leads. If you can convert these leads into paying customers, you've managed to improve your performance.
- Conversion: The step that you need your leads to take can be an easy one, or a difficult one. Anything you can do to lower the threshold for your lead to turn into a paying customer increases your performance. External IAM can be used to improve tracking therefore giving better insight into leads and weed out the most promising ones quickly. Identity management solution such as GlobalSign CustomerID, which is linked to your CRM to enable instant invites directly from the CRM workspace will definitely improve your conversion rates.



Risk Management

One of the concerns for companies in moving towards online or cloud services is security. Moving your next generation Nobel prize winning solar panel blueprints into the connected service might be a risk that you're not willing to take. External IAM can help you manage risk, but naturally it boils down to your security policy and possibly to regulations if you can new online services. Here are some of the areas where you can mitigate risk:

- Adequate authentication: Not everything needs to be locked tight. Having different methods available for end user authentication helps you select the appropriate level of identity verification. Lobby services might use social identities, customer extranets would utilize SSO from the customer network, and some parts of your service might require strong two-factor authentication, if e.g. confirming purchase orders above a certain threshold.
- No user repositories to hack: Bring Your Own Identity is a way to help your customers use their existing identities. If they can do so, there's no need for you to create a large database with user names and passwords and other customer information that could be potentially accessed from the Internet or gaining access through social engineering and persistent threats. Blogs such as krebsonsecurity.com and others are filled with reports on big hacks on a weekly basis, and if you can avoid becoming the next blog article it will definitely be worth it.

Compliance

Some industries such as financial and healthcare have existing national or international regulations that can affect how you treat customer information and their electronic identities. In the payment industry you also have PCI-DSS standards, which you should follow. Identity, authorization and access management solutions in general have capabilities that you can use to meet the demands set forth in the law or regulations. Here are a few examples:

- Identifying the end user: SOX, HIPAA etc have provisions that state that you need to protect sensitive information. One way to do this is to withhold the information, but not necessarily the best one. The other option is to make sure you identify who has accessed, what they have accessed and when. Using logs from a centralized authentication platform can provide you with the necessary audit trails.
- Proper authentication: Granting access to a resource based on a Facebook identity most probably wouldn't be compliant with regulations that touch the issue of end user authentication. An IDaaS that can integrate to all STORK or NIST -level authentication credentials will guarantee that you have the proper identity assurance in place.
- Government issued / recognized identity attribute: Sometimes, especially when dealing with e-government services, the online service will expect to receive a unique attribute of the user as part of the authentication event. In Scandinavia the social security number is something that practically all e-government services will expect. As the IDaaS is connected to the national eID infrastructure, it can easily deliver this required attribute to the online service.

Convenience

Even though you can not put an exact price tag on end user convenience, it will help you against your competition and improves loyalty and makes it easier to upsell your products / solutions to your existing customers. Here are some ways to improve the convenience of your customers, partners and other stakeholders:

- Single Sign-On: Single Sign-On is a cost issue, reducing management cost for the service provider. It's a big advance in convenience for the end user if they can login into your systems from their own corporate domain.
- Verified Social Identities: Social identities such as Facebook or Google+ accounts by themselves are almost worthless in a B2B scenario. But if you enable your customers to register a Facebook account, and verify it with another, stronger method you end up with a verified social identity, which can be used to give your customers and other stakeholders convenient access to your services
- Bring Your Own Identity: On top of corporate Single Sign-On and verified social identities, you can ease the life of your customer by allowing them to access your services with credentials they already own. A good External IAM can link these credential to the relevant customer information.
- Adaptive Authentication: Strong authentication is not always needed. By using appropriate authentication related to the context, you can improve the customer experience.

DELIVERY MODELS

It matters how you acquire your Identity Relationship Management solution. Experience has shown us that it is best to start with a handful of applications and then extend the IRM solution to cover more services, include additional authentication methods, new workflows, and back-end integrations. The easiest way to acquire IRM would be to sign up with an IDentity as a Servier (IDaaS), available also from GlobalSign. With IDaaS you get the fixed set of functionalities, authentication methods and other features. If you need something out-of-scope of the IDaaS provider you can opt for a private cloud delivery model, or have the IRM solution installed on-premise.

For private cloud and on-premise installations GlobalSign can offer the quickest and risk-free delivery model with a pre-configured IRM solution. With 10 years of experience in delivering IRM software to various customers we've created a best practice deployment model which can be up and running in weeks instead of months. After the initial deployment, the delivered IRM solution is fully configurable, and can be extended and modified to accommodate new services, authentication and federation needs, REST integrations, customized workflows etc. With GlobalSign products, no coding is required, not even when integrating the online services to the IRM solution thanks to our extensive support for industry protocols and off-the-shelf integration components.

CONCLUSION

Traditional internal IAM is usually driven by the IT-department, and their need to improve security and reduce admin costs. External Identity Relationship Management is driven by the business. Internal IAM's goal is to streamline internal processes whereas with External IRM the goal is to grow existing business, and create new opportunities by forming business ecosystems with subcontractors, customers, partners and other stakeholders.

"GlobalSign CustomerID managed to cut down our corporate customer registration time from 2 days to 5 minutes generating us cost savings of over 1m$ / Year."

-Mobile Network Operator, GlobalSign SSO and CustomerID customer

INQUIRE ABOUT THE IDENTITY RELATIONSHIP AND ACCESS MANAGEMENT FOR THE EXTENDED ENTERPRISE

To inquire about IRM for the Extended Enterprise, please contact us at www.globalsign.com.
We would be happy to discuss your specific requirements.

For further information, data sheets, guides, white papers on GlobalSign products for Identity Relationship Management for the Extended Enterprise please go to:
http://www.ubisecure.com/

[Ubisecure, a Finland-based IRM vendor was acquired by GMO GlobalSign on September 30th, 2014]

ABOUT GLOBALSIGN

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As leader in public trust services, GlobalSign Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital ID Solutions, internal PKI & Microsoft Certificate Service root signing. Our trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, and member of the Online Trust Alliance, CAB Forum and Anti-Phishing Working Group, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

GlobalSign Americas Tel: 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	**GlobalSign EU** Tel: +32 16 891900 www.globalsign.eu sales@globalsign.com	**GlobalSign UK** Tel: +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel: +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	**GlobalSign DE** Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	**GlobalSign NL** Tel: +31 20 8908021 www.globalsign.nl verkoop@globalsign.com