

A New Model for Deploying Identity-enabled Solutions

A White Paper

May 2009



NetStar-1 Identity Services

A New Model for Deploying Identity-enabled Solutions

Introduction	3
The Need for a New Model.....	3
NetStar-1's Co-sourced Managed Identity Services™.....	4
Is It in the “Cloud”?.....	5
A Business-Centric Approach.....	5
The Role of Identity Assurance.....	6
Identity and Compliance Automation	8
The Advent of the Identity-enabled Solutions Era	9
Who Should Care?.....	10
Why now?	11
Conclusion.....	11
About the Author.....	12

A New Model for Deploying Identity-enabled Solutions

Organizations need to implement means to increase the assurance levels of the identities of those individuals with whom they interact, whether they are online consumers, citizens, patients, partners, employees or contractors.

INTRODUCTION

As more high value services migrate towards online and electronic channels, organizations are faced with the challenge of securing and managing access to sensitive information at a very granular level in real time; and in doing so, strike the right balance of security and convenience that can effectively foster adoption of personalized services, in a way that complies with industry regulations, adheres to best practices, scales both administratively and operationally, and above all, delivers a positive return on investment (ROI).

The combination of technologies, policies, operations and legal frameworks employed to implement a solution that satisfies these needs, including the identification of individual to whom digital identities are issued and the protection of such identities is what is known as Identity Management (IdM).

Implementing an efficient and scalable IdM solution is no trivial task, and is critical if the organization is to realize value from it. It is today among the top 5 priorities in CIO's initiatives.

NetStar-1 has introduced a novel model for deploying IdM solutions based on co-sourced approach, a model that differs from the traditional deployment models used to date. A co-sourced model is one where a trusted provider is involved in the design, implementation and ultimate operation of the service infrastructure, which is then governed by established parameters and service standards, and whether it is hosted in premise, collocated or outsourced (in the "cloud"), in the end, the client sees immediate value for the services they purchase.

This white paper introduces NetStar-1's novel approach to delivering identity-enabled solutions, and contrasts it against traditional models followed to date when implementing IdM infrastructure.

THE NEED FOR A NEW MODEL

Let's start with a show of hands:

1. Raise your hand if you have been involved in or responsible for the deployment of an identity management solution;
2. Now, raise your hand if this deployment has succeeded in meeting the business objectives and stayed within the timelines and budget it was estimated for;
3. Now, raise your hand if your organization has gone through more than one attempt at implementing an identity management solution, including replacing technology vendors or system integrators;

The fundamental issue with traditional models is that the organization's best interest is not well aligned with that of the partners it relies on to undertake the deployment. The organization is at the center of the storm, looking at mediating and balancing the interests of the vendors, system integrators, and its own staff.

4. Lastly, raise your hand if your organization is able to measure the ROI on this initiative, and whether or not it is positive.

After over 12 years of experience deploying identity management solutions, large and small, I have seen a very small number of people in a crowd that can actually keep their hand up throughout all of these questions. Even though the number has increased over the years, it is still not as high as most would want it.

One would wonder: “why is it so?” and explanations will abound. Many will cite issues with the technology choices underpinning the solution; others will point at lack of alignment and sponsorship between technology and business stakeholders; some will say that there were no clear business objectives and expectations were not properly managed, a few will venture that identity management solutions are complex and difficult to implement, and underestimating their size or complexity was a recipe for disaster.

All valid reasons, no question; but does this mean that there is low probability of a success in deploying identity management? Is there no way but to suffer and struggle through this undertaking?

Under the established deployment approaches commonly used to date, the answer will not be very encouraging. To date, most if not all identity management deployments follow a traditional enterprise deployment model: faced with requirements from its organization's business stakeholders, IT selects a technology vendor, allocates the environment in which it will run (hardware, software, network and data center), in most cases, engages a system integrator to help design the architecture, map the business requirements and processes, and implement the solution, and once it is deployed, it is tasked to hire, retain or grow the qualified personnel it needs to operate the infrastructure; this is why most projects run longer and cost more than expected, in many cases they do not meet the business requirements that they were meant to address, and the organization is left with a capital expenditure that needs to be recovered over time. Therefore, it embarks on programs looking to integrate more applications, absorb more environments (M&A, intranet, extranet, etc.), and the success rate increases marginally; in many cases, attrition of the internal personnel complicates the ongoing success of the deployment.

The fundamental issue with this approach is that the organization's best interest is not well aligned with that of the partners it relies on to undertake the deployment. The organization is at the center of the storm, looking at mediating and balancing the interests of vendors, looking to maximize their product or maintenance revenue, system integrators, whose main interest is extending the duration and scope of their engagements, and its own staff, who is typically not qualified or unaware of the complexities of deploying and running an identity management infrastructure.

And this is why a new approach is needed, one that aligns more closely with the interests of the organization.

A novel, co-sourced delivery model that disrupts established conceptions around identity management deployments. Rather than having the organization striking a balance among the interests of vendors, system integrators, and its own staff; in this model, NetStar-1 acts as a trusted provider, entering a long-term relationship that is gauged by discrete phases and tangible results.

NETSTAR-1'S CO-SOURCED MANAGED IDENTITY SERVICES™

In response to this need, NetStar-1 is proposing a new model – a novel, co-sourced delivery model that disrupts established conceptions around identity management deployments. Rather than having the organization striking a balance among the interests of vendors, system integrators, and its own staff; in this model, NetStar-1 acts as a trusted provider, entering a long-term relationship that is gauged by discrete phases with nominal scope and measurable results.

A fundamental metric to gauge the success of the deployment is total cost of ownership (TCO). However, a big challenge for most organizations is to really quantify the TCO

of an identity management infrastructure. Since it is an infrastructure of complex nature, which integrates with several IT systems (such as email, HR, ERP, portals, directories, etc.), it is easy for costs to get diluted. Under a co-sourced model, NetStar-1, as a trusted provider, is involved in the design, implementation and ultimate operation of the infrastructure, which is then governed by established parameters and service standards, and whether it is hosted in-premise, collocated or outsourced (in the "cloud"), in the end, the organization sees immediate value for the services they purchase, in a predictable and simpler manner.

Under this model, NetStar-1 as the provider, and organization as the client, are both motivated in achieving successful results rapidly and engaging in a long-term relationship bound to operating an environment successfully with a tight control of scope and complexity, where the organization sees value on an ongoing basis.

Evidence exists, particularly in extranet environments, that "cloud" identity services are gaining popularity. However, they are not yet as mature or sophisticated to suit the needs of every organization, particularly those focused on internally facing environments.

Is It in the "Cloud"?

A lot of hype is building around "cloud" services and "cloud computing", and we concur that these models will thrive. Evidence exists, particularly in extranet environments, that "cloud" identity services are gaining popularity. However, they are not yet as mature or sophisticated to suit the needs of every organization, particularly those focused on internally facing environments.

Likewise, models of pure out-sourcing and "off shoring" have proven to end up costing more and yielding greater dissatisfaction, even though their per-item cost is significantly lower on paper.

A co-sourced identity management deployment model offers a balanced combination of internal resources with externally provided ones that allows organizations to easily measure and realize value from the services provided. The service is typically priced via periodic fees – monthly or quarterly, so that it is easier and more predictable to put in a budget plan.

The co-sourced, managed services model will allow the organization to more seamlessly measure their TCO, given that most of the cost comes as a periodic charge that can be easily added to a budget or a financial plan.

A Business-Centric Approach

For it to be viable, the premise for the co-sourced identity service model is that it aligns more closely with the business objectives of the organization. This means not only an alignment of interests and motivation between the organization and its provider, but it also means giving the organization visibility and predictability to effectively quantify and measure the success of their identity management solution. The co-sourced, managed services model will lend itself to this business-centric focus.

For starters, the model will allow the organization to more seamlessly measure their TCO, given that most of the cost comes as a periodic charge that can be easily added to a budget or a financial plan. The predictability of this model will allow the organization to simplify its cost structure computation and through this, enable it to make better decisions on what initiatives to undertake and which ones not to. At the same time, it will also allow it to forecast the long-term benefits of greater adoption and growth, which should lead to economies of scale – the per-item cost should improve as the number of items increases.

Another important consideration, particularly from a business perspective, in judging the success of an identity management deployment is the balance of elements that often move in opposite directions and how this balance allows the organization to achieve its business goals. There are typically four elements:

- **Convenience** – which in itself is a determining factor in the success of any solution – it must be easy to use to be successful. For an online portal, having a user struggle to login after forgetting a password or follow a very lengthy

registration process may result in lost business, as the user may choose to do business with a more “convenient” provider. For the organization, convenience also equates to how much administrative cost is required to support the end user experience – resetting passwords, approving requests, monitoring exceptions, etc.

- **Privacy** – how much personal or sensitive information must be disclosed by the individual, and how well is this information protected and used by the organization that collects it. End users would be concerned if their SSN or credit card information was needed to open an online email account for instance. At the same time, an organization must be concerned about the liability it assumes if it misuses this sensitive information.
- **Security** – what mechanisms are in place to prevent the information from being intercepted or tampered with, both in real-time as the transaction occurs, and offline, once the data is stored, as well as to ensure that only the authorized user is allowed to transact. For the organization, this translates to how much investment is needed in security technology to achieve the appropriate level of risk mitigation.
- **Compliance** – compliance brings governmental legislation and regulatory oversight to gauge the governance and confidence in the way services are being provided. In today’s highly regulated world, organizations cannot ignore the role and relevance of achieving and staying compliant with the regulations that govern their specific line of business, such as NERC, PCI, FFIEC, SOX, HSPD-12, HIPAA, etc. Organizations need to approach compliance as a lifecycle process, which is bound to evolve and requires agility for the organization to stay current.

We believe that a managed, co-sourced approach to implementing an identity management solution, particularly when a trusted provider is tasked by the organization to deliver on tangible metrics, will enable the organization to benefit from the expertise and best practices that can be applied to its deployment, not only from inception, but throughout its lifecycle.

Organizations need to consider the assurance levels of the identities of those individuals with whom they interact, in accordance to the sensitivity of their transactions.

The Role of Identity Assurance

The co-sourced, managed service model hinges heavily on identity assurance as a business metric to help gauge complexity, sophistication and cost. Identity assurance is a very important concept, often disregarded in traditional identity management deployments, that can help organizations assess the level of sophistication and of course cost that their identity management infrastructure requires. This is particularly relevant when enabling collaboration with external business partners – suppliers, partners, business customers, etc.

Identity assurance is the ability for a party to determine, with some level of certainty, that an electronic credential representing an identity with which it interacts in a transaction can be trusted to actually belong to and being used by that person, and not someone else.

The level of certainty one can have about the identity credential is what is referred to as the "Assurance Level". Assurance Levels (ALs) are the levels of trust associated with a credential as measured by the associated technology, processes, and policy and practice statements. An assurance level describes the degree to which a relying party in an electronic exchange can be confident that the identity information being presented by a credential actually represents the identity referred to in it and that at present, it is this actual person behind the keyboard. Standards such as the Liberty Alliance Identity

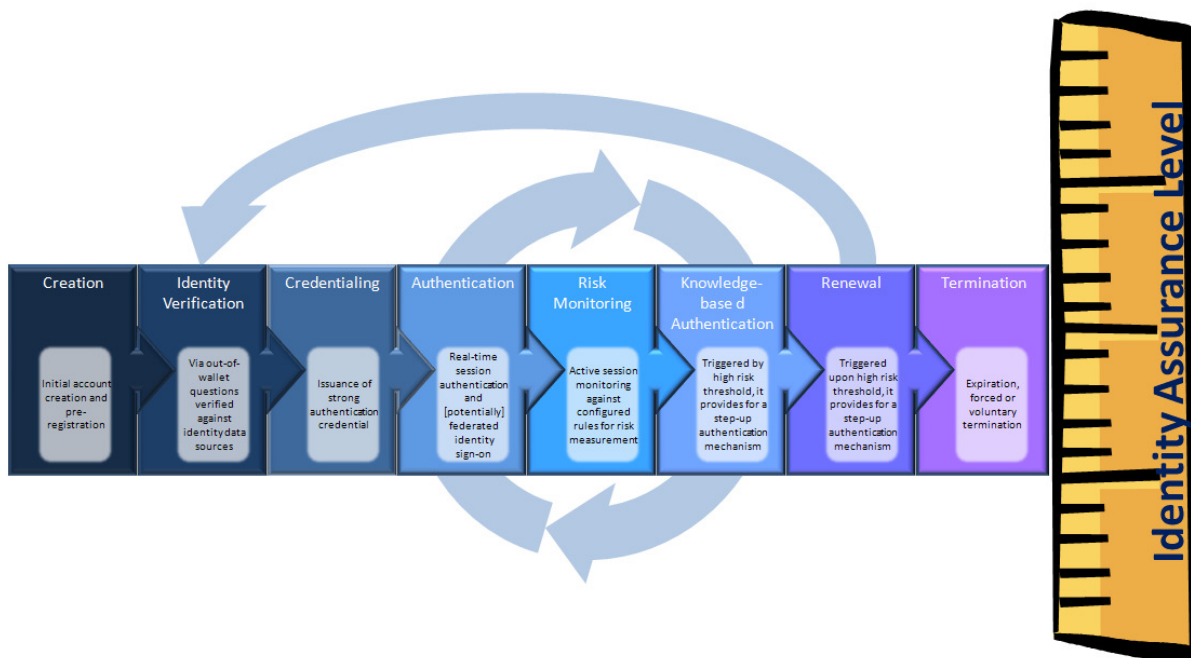
Assurance Framework (IAF)¹ and NIST Special Publication 800-63² provide guidance and definition for identity assurance, and are baselines that NetStar-1's co-sourced, managed model adheres to.

Identity assurance plays an important role in identity management deployments, as higher levels of assurance imply more thorough and secure processes for managing identities, which often equates to higher costs. Identity assurance is better understood as a risk equation – the higher the risk, the stronger risk mitigation mechanism required, hence, the higher the cost.

The idea is therefore to apply the right level of risk mitigation to enable a certain type of transaction to take place. For instance, difference levels of assurance will apply to sending an email via a personal email provider – say Google or Yahoo, versus authorizing an electronic fund transfer transaction from your online banking site. Organizations need to gauge what kind of identity management infrastructure, complexity and sophistication is necessary to facilitate these business transactions.

We believe that a managed, co-sourced approach will allow organizations to define the risk levels, and thus the assurance levels, that it needs to provide for a particular service, and hold its provider responsible for ensuring that the identity management infrastructure complies.

Identity assurance, like other facets of identity management, is a lifecycle process, a continuum. An identity lifecycle will include stages ranging from *registration* – initial creation, identity verification, credentialing; *contextual access control* – authentication, risk and activity monitoring, knowledge-based authentication; *renewal* and *termination*. The last two intended to refresh the assurance level of an existing identity.

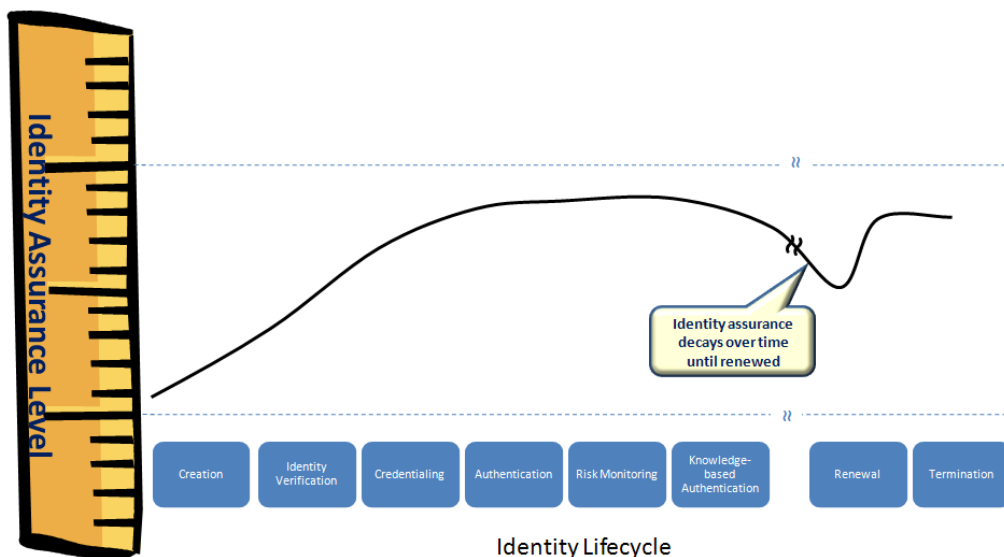


The identity management solution must account for the fact that identity assurance decays over time, and that renewal or termination steps are necessary to either preserve

¹ <http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf>

² http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1-0_2.pdf

the identity assurance level or eliminate the risk of a compromised identity. These lifecycle steps are all equally important in achieving and maintaining a consistent level of



assurance, which will ultimately allow end users and organizations to gain trust in online channels to conduct sensitive transactions. Though this very item may seem obvious, traditional identity management deployments do not incorporate identity assurance as a guideline, and thus rely on a static notion of the identity, with well-defined, discrete lifecycle steps – creation, authentication, updates and eventually termination; the notion of a continuum is fundamental in NetStar-1’s co-sourced, managed services model. The figure below provides a conceptual illustration of how identity assurance is managed through each stage in the lifecycle.

Identity and Compliance Automation

Given the heterogeneous nature and complexity involved in implementing identity automation, a specialized service provider can deliver a superior solution based on final deliverables, rather than technology products. Organizations will benefit from the best-in-class nature of the service and focus on the actual information being delivered and the actions it triggers, rather than the complexity in integrating and operating sophisticated identity and compliance automation technologies.

Automation is essential in achieving scalability and cost efficiencies in any IT infrastructure, and identity management is no exception. In the context of an effective, managed service model, identity automation plays a crucial role. It includes event-driven workflows, which ensure that identity data propagates from source systems to target systems according to the right business rules and approvals, as well as adhering to a consistent identity data schema.

But in addition, next generation identity management solutions need to provide active automation. This encompasses processes such as identity activity monitoring, correlating audit and system logs to detect anomalies in patterns and measure risk, trigger in-session mechanisms, such as step-up, out-of-wallet or out-of-band authentication to preserve the assurance of a transaction, as well as reconciling dormant, unauthorized, expired, about-to-expire, and manually-added accounts, which may constitute threads to the integrity and security of the infrastructure as a whole.

Audit and compliance, which are typically approached as reactive, forensic processes, focused on harvesting and correlating logs, should evolve into active proactive risk mitigation mechanisms, through which not only the organization can satisfy their regulatory requirements – reporting and auditing, but can streamline tedious, labor-intensive and costly processes that tend to be treated as annuities from a cost perspective. Compliance automation is critical in the ongoing sustainability of the identity management infrastructure, particularly given the dynamic and complex nature of the compliance and regulatory landscape.

For instance, recurring audit and certification processes, required to remain compliant with SOX, NERC, ISO27001, PCI, and the next regulation “du jour”, should be incorporated as design and implementation requirements that the identity management solution should help facilitate. A managed services approach to identity management will provide the added benefit that the service provider will need to ensure that its own services and practices satisfy the regulatory requirements of the industries in which it provides its service, which translates to a pragmatic way for the organization to remain compliant.

Additional level of sophistications are possible by correlating behavioral patterns and transactional history in the active evaluation of in-session risks, a concept known as contextual access control, by leveraging richer data sets in making authorization decisions. For example, the authorization system could combine a variety of factors in a single policy, such as originating IP address, time of day, parameters qualifying the operation or resource, the type and version of the user’s browser, the user’s role and specific profile attributes in the context of the application. These factors are evaluated in a specific order to determine whether access is to be granted or denied before the transaction actually takes place, thus proactively avoiding downstream, costly damage control measures.

Forensic analysis of historical audit and activity data is and will continue to be necessary to reduce fraud and demonstrate compliance by running more sophisticated pattern analysis and activity correlation algorithms that can produce comprehensive reports tailored for target audiences, such as security officers, internal auditors, external audits, and line of business risk management teams.

NetStar-1’s co-sourced, managed services model will prove an effective way for organizations to achieve the appropriate level of automation it needs. Given the heterogeneous nature and complexity involved in effectively implementing identity and compliance automation, a specialized, trusted service provider can deliver a superior solution based on final deliverables, rather than technology products. Organizations will benefit from the best-in-class nature of the service and focus on the actual information being delivered and the actions it triggers at a business and operational level, rather than the complexity in integrating and operating sophisticated identity and compliance automation technologies.

THE ADVENT OF THE IDENTITY-ENABLED SOLUTIONS ERA

So, does this represent a change, significant enough to be considered a new paradigm? We believe so.

We believe that only through a co-sourced, managed service approach can organizations readily and effectively benefit from these identity-enabled solutions, and moreover, position themselves to adopt business-oriented solutions that leverage identity to accelerate the transformation of manual, labor-intensive business processes.

This model will allow the transformation of processes, such as auditing and reporting, to move from being a cost-item, to potentially becoming differentiators and accelerators that can give the organization a competitive advantage. For example, by streamlining the process of achieving and maintaining compliance with industry regulations through identity automation, an organization can complete certifications and satisfy audits sooner than its competitors, thus having an opportunity for a faster go-to-market. Moreover, the managed service approach will allow the infrastructure to cater to multiple, ever-changing compliance requirements without significant incremental costs. Adherence to industry best practices, concepts such as identity assurance and guidance from industry standards and guidelines will prove effective in

Only through a co-sourced, managed service approach can organizations readily benefit from these identity-enabled solutions, and moreover, position themselves to adopt business-oriented solutions that leverage identity to accelerate the transformation of manual, labor-intensive business processes.

making this benefit tangible, and ultimately allowing the organization to compete in more markets or address broader market segments.

By integrating contextual access control and identity and compliance automation in its online channels, organizations can transform the perception, or perhaps reality, that security and compliance slow down the ability for business initiatives to be implemented in shorter timelines, towards a differentiator in gaining customer's confidence and effectively reducing fraud.

Introducing identity assurance, and embracing it as a construct in the implementation of identity management solutions, allows organization to treat and measure identity management as a risk mitigation mechanism, and thus equate levels of risk and corresponding assurance needed to allow certain transactions, of varied sensitivities, to take place in an electronic fashion. A very tangible example of the transformational relevance of identity assurance could be drawn from the ability to effect legally-binding transactions at higher levels of assurance. This literally means that a paper-based process, requiring a wet-ink signature, can be effectively migrated to an online process in which no manual, physical, or courier steps are involved. This could immediately translate to bigger margins on transactional-based businesses, increased transaction capacity, a better end-user experience and in many cases, all with increased security and compliance.

Another relevant example of the transformational nature of identity assurance is the migration from paper-based correspondence, for items such as statements, notices, confirmations, claims, etc. to electronically delivered information, which not only leverages online channels, but given the added assurance, can improve privacy and non-repudiation, and as such can mimic today's physical delivery processes by leveraging channels as ubiquitous as email, even personal, public email – thus fostering adoption.

Several organizations are embarking in these types of imitative and quickly realizing that identity assurance is in fact the cornerstone of transformation. Countries, such as Hong Kong and Brazil, are passing regulation requiring organizations, both in government and private sector, to correspond with their consumers via secure, electronic channels. At the same time, managed service approaches have proven effective in many cases, as a way for the organization to quickly adopt these next generation solutions, rather than having to build the infrastructure in-house from scratch.

Lastly, by providing organizations a simpler, cost-effective and more transparent option to deploying identity-enabled solutions, holding a trusted service provider accountable for service standards that deliver based on the parameters described herein, we believe that a new paradigm will start to take place, and adoption of the co-sourced, managed service model will quickly become the de facto approach for organizations to achieve the benefits of next generation identity-enabled solutions.

NetStar-1's long-term roadmap aims at the evolution from identity management solution to identity-enabled end-to-end services, which will drive real transformation and migration from manual, paper-based processes to secure, electronic-only environments.

Who Should Care?

This paradigm should be appealing to most organizations and stakeholders interested in fostering greater adoption of online and electronic channels to conduct business. Organizations that provide services to growing, fast-changing and diverse, external stakeholders, particularly those dealing with increasing numbers of consumers, will see immediate value and synergy with the concepts and managed service model described herein.

Organizations transacting with growing, fast-changing and diverse external stakeholders, particularly those dealing with increasing numbers of consumers, will see immediate value in the managed service model described herein.

The time is now for a paradigm shift in identity management to take place, and we are convinced that the co-sourced, managed identity services model is the next evolutionary step.

Why now?

Though it may sound existential, inaction is not an option today; it has not been for a few years.

Difficult present economic conditions, ever increasing costs and complexity in the regulatory landscape industry wide, sophistication and proliferation of fraudsters and hackers, and the inevitable quest for higher productivity and cost containment, pushes organizations to look for effective ways to remain competitive and introduce greater value, differentiation and transformation to its critical business processes. Identity management must therefore evolve from a headache and cost element to a business transformation catalyst.

We believe that the time is now for this paradigm shift in identity management to take place, and are convinced that the co-sourced, managed identity services model is the next evolutionary step.

CONCLUSION

NetStar-1 is proposing an innovative and different approach to delivering identity-enabled solution which will provide tangible benefits and measurable returns to the organization, and which, in itself incarnate the start of a paradigm shift in the way identity management solutions are deployed.

We welcome the opportunity to discuss and demonstrate the elements and benefits of NetStar-1's co-sourced managed identity services™ delivery model.



ABOUT THE AUTHOR

Frank Villavicencio is a seasoned identity management expert with a successful track record of over 12 years spanning consulting, large implementations, business development, sales, product management and the invention of two awarded patents in the area of web access management, as well as published papers and public speaking engagement. Mr. Villavicencio leads NetStar-1's Identity Services practice.

Prior to NetStar-1, in 2007, Mr. Villavicencio joined Citigroup's Managed Identity Services product management team focusing on strategic partnerships, customer deployments, industry standards and business development at a global level. At Citigroup, Mr. Villavicencio led a business of high assurance digital identity credential issuance and lifecycle management compatible with the SAFE-BioPharma identity management standard, which cross certified with the US Federal Bridge CA.

Until March of 2009, Mr. Villavicencio was co-chair of the [Liberty Alliance Identity Assurance Expert Group](#), an industry forum for identifying and resolving the market acceptance and commercial obstacles to broad deployment and adoption of identity assurance services. This forum includes representatives from GSA's Office of Governmentwide Policy. Mr. Villavicencio led the work resulting in the publication of the [Identity Assurance Framework \(IAF\)](#) in 2008, which is a standardized approach that defines processes and procedures for credential service providers, relying parties, and operators of federated identity environments to trust each other's credentials at known levels of assurance across industries and Governments. IAF leverages the guidance provided by NIST SP 800-63 and OMB M 04-04 in defining four levels of assurance, and goes on to provide specifications for the strength and rigor of the identity proofing process, the credential's strength, and the management processes the service provider applies to it. The framework provides a pragmatic and thorough approach to standing up a service that provides a consistent level of assurance, not only during the identity proofing and registration stage, but throughout the lifecycle of an identity credential.

Prior to Citigroup, Mr. Villavicencio was at Oracle since March 2005 (after Oracle's acquisition of Oblix), leading a product team responsible for access management, single sign-on and identity federation products part of the Oracle's Identity Management suite. Mr. Villavicencio's in-depth knowledge in the contextual access control area is evidenced by [publications](#)³, and his direct involvement in [Oracle's acquisition of Bharosa in 2007](#), which led to the launch of Oracle's Adaptive Access Manager. Prior to Product Management, he led Oracle Consulting's identity management practice, overseeing successful deployments of identity management solutions globally.

Before Oracle, Mr. Villavicencio spent close to five years at Oblix, where he served as Practice Manager for the Professional Services group, involved in Oblix's client deployments worldwide.

Mr. Villavicencio holds a bachelor's degree in electronic engineering, cum laude, from Simon Bolivar University, Venezuela; and also holds a Master of Science in Information Networking degree from Carnegie Mellon University's Information Networking Institute.

³ "The advent of Access Management 2.0", SC Magazine, August 02, 2007 – Eric Leach and Frank Villavicencio. <http://www.scmagazineus.com/The-advent-of-Access-Management-20/article/35240/>



NetStar-1 Identity Services
A New Model for Deploying Identity-enabled Solutions
A White Paper
May 2009

Author: Frank Villavicencio

NetStar-1, Inc.
9713 Key West Avenue, Suite 400
Rockville, MD 20850
U.S.A.

Inquires
Phone: +1 240.425.4200
Email: frank.villavicencio@netstar-1.com
Web: <http://netstar-1.com/solutions/identity>

Copyright © 2009, NetStar-1. All rights reserved.
This document is provided for information purposes only and the contents hereof are subject to change without notice.
This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.