

WHITE PAPER

ActivIdentity: Digital Proof of Identity for Evolving Ecosystems

Sponsored by: ActivIdentity

Sally Hudson
October 2006

IDC OPINION

We are on the verge of a historic event. As organizations globally move to establish an infrastructure that meets regulatory compliance before the looming deadlines, we note a shifting paradigm: Governments and enterprises are adopting technologies that enable them to transition from paper to digital records. This evolution, based on achieving irrefutable proof of individuals' identities, enables digital record-keeping, auditing, and greater efficiency in commerce and ultimately allows organizations to establish legally binding evidence. IDC believes that as organizations transition from paper-based infrastructures to secure digital systems to achieve regulatory compliance, the following will occur:

- Companies and consumers alike will be protected by regulatory legislation.
- Digital evidence will be accepted as proof in courts of law.
- Online contracts will emerge, and they will become legally acceptable.
- Individuals' identities will be simplified and consolidated as standards continue to mature.

Further, IDC believes that with digital infrastructures in place, organizations can take advantage of subsequent benefits:

- Individuals will use one identity to prove their authenticity for all transactions, physical access, and access to and protection of their personal records.
- Individuals, enterprises, and governments will interact quickly and safely via electronic transactions.
- Internal and external fraud will be curtailed, resulting in realizable cost savings.

METHODOLOGY

IDC wrote this paper in August 2006. It is based on historical and current research. To augment this research, IDC surveyed customers and vendors affected by the challenges of meeting compliance regulations and documented their use of identity and access management (IAM) products and services. IDC conducted in-depth interviews with executives familiar with different regulatory compliance issues as well as many firms from different industries focused on implementing solutions specifically designed for regulatory compliance.

IN THIS WHITE PAPER

In this white paper, IDC profiles ActivIdentity™, a company forged from the merger of ActivCard and Protocom Development Systems. ActivIdentity develops technologies that provide customers with absolute proof of digital identity. Together with established technology partners and managed service providers, ActivIdentity can provide organizations with digital identification solutions to address today's requirement to safely conduct business in dynamically evolving digital ecosystems.

SITUATION OVERVIEW

Digital Identity Assurance: Allowing People and Organizations to Interact Electronically with Confidence — Anytime, Anywhere

The ability to prove external users' identities, and manage their interaction with commercial infrastructures, has encouraged countless organizations to launch lucrative online initiatives. Simply note the emerging online storefronts offering banking, financial services, travel, retail purchases, supply chains, and other products and services. This shift to online business perpetuates increased systems integration and access via the Web to sensitive resources and applications and is surreptitiously aggravated by emerging new challenges. These challenges arise from vulnerabilities associated with the broadening scope of ways in which individuals can transact financial information electronically and include online fraud, identity theft, data theft, unauthorized access to data, as well as outright acts of cyberterrorism. This document explains the need for government to develop regulations that protect businesses and consumers by restricting and auditing who can access business and personally sensitive information. Initiatives such as Sarbanes-Oxley and HIPAA in the United States, the European Union Directive on Data Protection, and the Australian Federal Privacy Act are among the most recognized examples. Failure to comply with these regulations results in stiff penalties for organizations.

What Is Identity and Access Management?

IDC defines IAM as a comprehensive set of solutions used to identify users in a system (e.g., employees, customers, contractors) and control their access to resources within that system by associating user rights and restrictions with the established identity. This is accomplished via implementation of one or a combination of the following technologies within an organization: Web single sign-on (SSO), host SSO, user provisioning, advanced authentication (which includes PKI, traditional hardware tokens, USB devices, and smart cards), legacy authorization, and directory services. These technologies are all critical components of identity and access management.

IAM technology converges multiple digital credentials into a single, secure identity that includes physical, logical, application, and remote identities. Over recent years, this group of technological solutions has matured rapidly in scope, available form factors, and capabilities. One of the key enablers has been the ability to administer large groups of identities (users, accounts, credentials) from a central location, which allows greater business agility for corporations in creating and delivering both products and services. IDC believes that strong identity and access management is the foundation that allows enterprise IT to securely extend network perimeters.

Evolution of Digital Identification

Organizations today typically have established infrastructures that require employees to identify themselves electronically in one or more of four primary methods:

- ☒ **Physical Access** characteristically uses an ID badge for access to office buildings, hospitals, or restricted areas.
- ☒ **Remote Access** uses a variety of identity management (IDM) technologies, such as a smart card or one-time pass code token for access to the virtual private network.
- ☒ **Logical (or PC) Access** often uses a simple password or PIN, sometimes together with a smart card for access to corporate assets, bank accounts, Web sites, or consumer information held within a software program.
- ☒ **Digitally Signed Documents** use a smart card and/or digital certificates wherein a consumer or corporate entity is issued a secure digital signature that is accepted as valid, authentic, and legally binding.

These concepts are clearly illustrated in Figure 1.

FIGURE 1

All-in-One Physical/Logical ID Card



Source: ActivIdentity, 2006

The next generation of identity and access management technology focuses on providing individuals with a single form factor that consolidates their multiple authentication requirements into a unified identity. Commonly a smart card, this form factor captures and stores users' credentials and identifies them to their corporate back-end system, which had originally provisioned their credentials and rights across the enterprise. Many organizations are working toward this common goal not only to ensure secure, safe access anytime and anywhere but also to facilitate compliance regulations and ultimately streamline business processes.

Many of the trends driving this market already noted, such as compliance and the need to protect information, increase security, and improve efficiency, are further magnified by the business needs of individual sectors and government standards. This includes directives such as the FIPS-201 initiative in the U.S. federal government space, and others, which are standardizing universal digital identity assurance. These capabilities will ultimately be key success factors in crossing international boundaries and industry segments. Further, many of the standards established in government become benchmarks for other sectors.

For today's organizations, achieving efficiencies in regulatory compliance becomes increasingly important. Fortunately, over the past several years, advances in identity technologies have permitted industries and service providers to coalesce along vertical lines, creating communities of interactive ecosystems linked by business need and enabled by technology. Examples can be seen in healthcare, education, finance, banking, and manufacturing.

Defining Identity: It Begins at Birth

In much the same manner that government is involved with the emerging standards for digital identification, in previous decades, it also set the standards for proof of identity. A newborn child's identity starts with a name, which is used to create a birth certificate and social security number. This individual uses these documents to obtain a driver's license and a passport, open a bank account, trade stock, and establish credit. At all stages of life, the person must continually rely on standardized documents to authenticate and verify identity for goods, government services, travel, and financial transactions.

It is more urgent in today's technology-powered industries to use global standards as a vital baseline in establishing identity. As companies become more interdependent on one another for information necessary to conduct business, and employees and consumers become increasingly more mobile, the ability to positively identify and track a person at all points of contact within the enterprise, commercial, and government sectors is essential.

How Does Identity and Access Management Work?

IAM technologies determine who is granted access to enterprise systems and under what circumstances, and the fundamental starting point is at proof of identity. The ability to authenticate an identity has become fundamental to the success and longevity of any organization. Another critical layer to identity and access management is the ability to audit and report on these actions, which is critical to compliance.

Once identity is authenticated, access can be granted at appropriate points within a designated community. In healthcare, for example, identity verification might begin in the parking garage at the hospital and move on to grant access to administrative systems and patient medical records. It might then link to the pharmacy, enabling prescription drugs to be administered; laboratory test data to be created, distributed, and assessed; and billing information to be implemented. All this activity is based and dependent on the individual's access profile parameters.

A similar scenario can be drawn in the banking and financial sectors, where an individual's point of access also begins with physical access to buildings. This same identification mechanism can be used to grant access to a bank's computer network as well. For remote or highly mobile employees, the same ID form factor would be utilized to ensure authentication and grant access to appropriately authorized accounts. In a brokerage situation, the identification mechanism could be extended to be universally recognized globally by all participating and approved trading partners under a specific industry regulation or standard or a set of specific industry regulations or standards. Similarly, in the mortgage broker/application/approval process, a single identification factor could seamlessly and securely allow an approved entity to move through various credit agencies and other pertinent third-party systems to streamline the multiple steps required in a mortgage approval process.

ActivIdentity: The Digital Identity Assurance Value Proposition

Company History and Direction

ActivIdentity is the combination of ActivCard and Protocom.

ActivIdentity, a public company founded as ActivCard in 1988, maintains its international headquarters in Fremont, California. The company has almost 15 million users and 5,000 customers worldwide.

For businesses, governments, and consumers, ActivIdentity provides digital identification solutions to address today's requirement to safely conduct business in the electronic world. The ActivIdentity solutions enable individuals to establish and use a trusted digital identity to securely access systems, networks, applications, information and services; protect data; access facilities; communicate; and digitally sign documents and transactions.

Unlike many closed, proprietary point solutions, ActivIdentity's digital identity assurance platform delivers the industry's most complete set of integrated and open standards-based applications. It allows customers to implement and use the digital identification capabilities they need now while preserving their investment in the future. Open standards-based technologies allow customers to seamlessly add more applications and services as needed, without having to rip and replace technology installed to meet critical security needs today.

ActivIdentity has many notable large customers in the government, healthcare, financial, and technology sectors, including U.S. Department of Defense (DoD), U.S. Department of the Interior, U.S. Department of Veterans Affairs, Singapore Defence, World Bank, U.S. Federal Reserve Bank, British Telecom, Emory Healthcare, the Spanish Ministry of Works, ABN AMRO, Citigroup, Monsanto, and ING Direct.

The U.S. Department of Defense: A Case Study

ActivIdentity technology supports open standards-based APIs. This open approach allows both government and commercial organizations to preserve their existing investments in IT infrastructure and applications while adding the critical layers of identity and authentication required. It also created an especially appealing offering to the federal government, which was particularly concerned with the cost of replacing years of legacy technology. In 2001, the U.S. Department of Defense deployed a Common Access Card (CAC) program using ActivIdentity smart card technology. The deployed solution exploited existing management systems, directories, and user databases to provide secure access and authentication for 3.5 million service members, civilian employees, and contractors. To date, some 10 million smart cards have been issued, at a rate of approximately 10,000 cards per day across 1,500 issuing stations around the world. This ability to securely connect to DoD resources via the CAC method allows these individuals to access healthcare benefits, information, and other services vital to their well-being.

Converging Identity Management

The ActivIdentity Smart Employee ID Card

Today, ActivIdentity is a leader in providing end-to-end smart card life-cycle management systems that cover:

- Receipt and processing of participant data from enrollment system
- Secure data management for card issuance
- Card life-cycle management (additions, deletions, updates, and additional functionality)
- Post-card-issuance data and applet updates

ActivIdentity offers a variety of authentication products that provide customers with a multitude of options to solve their user identification needs. These options include smart card systems, biometric hardware, server software, client software, and authentication hardware. The company provides key enabling tools and technology for accessing enterprise and government assets securely and also enables secure remote communications. It also can provide authentication solutions utilizing all of the hardware authentication form factors (smart cards, tokens, and USB tokens) married to a complete identity assurance software system.

Single Sign-On

ActivIdentity has deployed SecureLogin Single Sign-On in many of the world's largest enterprise single sign-on (eSSO) production environments. The software provides integration with components for advanced authentication, self-service password reset, and auditing capability. ActivIdentity SecureLogin version 6.0, released early in 2006, integrates eSSO with smart cards and delivers on ActivIdentity's mission of identity convergence for lower total cost of ownership and significantly improved enterprise security.

The components that form the identity assurance layer include:

- Strong authentication
- Credential management
- Authentication device management
- Smart card life-cycle management

These technologies are essential in building and maintaining an industry-compliant ecosystem and can be utilized to provide for the convergence of photo identification and physical access, logical (network) access, remote access, and digitally signed email and documents.

Common Risks in Identity Access Systems Today

- Weakness of passwords.** The inherent weakness in passwords as the single method of authentication is obvious: They fail to definitively identify the user. Anyone, anywhere can type in a password. Corporations are trending to using passwords with other trust-establishing devices, usually some method of two-factor authentication such as hardware tokens or smart cards. For physical access to locations, we are seeing an increased use of biometric technology.
- Lack of adequate management tools.** Management tools must address the range of identity information sources and ensure a one-to-one relationship between valid users and identity.
- Lack of integration with existing identity storage.** A system that provides trust has to be a good neighbor to the existing sources of user identity. Creating separate sources of identity stores works against the notion of using identity management to centralize the identity in the first place. There must be a method of centrally managing and synchronizing all facilities that manage user identities within an organization.

- ☒ **Weak authentication mechanisms.** Good policies can establish the proper security principles over the rightful users in the system. A policy links the identity to the rights. However, what occurs if the person using the identity is not actually the preauthorized person? This type of breach breaks down the identity ecosystem because there is no security or trust if one cannot identify digitally and with absolute certainty who the user actually is.
- ☒ **Exposed provisioning.** Provisioning extends the identity to the applications, and it can create delays or risk if there is no trust in establishing who will actually use the application. A system for trust needs to ensure that credentials stay safe even as they are pushed out to the application.

A fundamental issue here is what we call "access with trust." The identity of anyone accessing the system must be established beyond any reasonable doubt. Without absolute proof of identity, the foundation of any IAM ecosystem is structurally weak. Without proof of identity, a company cannot prove who was accessing what system for what reason and when. The process cannot be successfully audited, and therefore the company can be held in noncompliance.

With positive digital proof of identity becoming an increasing reality for organizations, the use of digital IDs and electronic contracts will become more commonplace in the coming years (it is already used in banking and finance), eventually leading to the acceptance of digital evidence in courts of law. Standards will play a pivotal role here as well, enabling federated communications among organizations, entities, and ecosystems with secure digital ID mechanisms in place.

To this end, ActivIdentity proposes the following five principles as keys to achieving digital identity assurance for the government and commercial sectors:

- ☒ Build and bind physical access authorities to the enterprise identity management system and a secure identity device that utilizes multifactor authentication
- ☒ Add logical access, the ability to securely identify oneself to the network
- ☒ Leverage the identity credential for single sign-on to securely bridge to legacy applications and at the same time increase security through the use of stronger authentication and access
- ☒ Integrate remote access to networks and applications with a single corporate identity, eliminating the need for costly tokens
- ☒ Utilize digitally signed email and documents that provide admissibility in legal transactions and reduce administrative costs

Achieving these goals will allow individuals to carry a single device as an identifier, which will ultimately be much more cost-effective and aid in simplifying systems management for enterprise IT.

Commercial entities are looking to achieve an advantage from newly implemented government ID programs. The ability to electronically cross-sign between government ID programs (such as those currently implemented in Belgium and some Nordic countries) and the commercial sector with a single digital identifier will be invaluable in streamlining systems management and closing current loopholes in identification access and authorization systems.

We are beginning to see this type of government/commercial sector universal ID today in the United States, as we move to embed smart card chips in passports. Within the U.S. Registered Traveler program, another example can be seen in the ability to cross-check biometric fingerprints with the FBI.

ActivIdentity Partners

ActivIdentity works with several categories of partners, including global alliance partners, systems integrators, solution and technology partners, and channel partners.

Global Alliance Partners

ActivIdentity global alliance partners work with ActivIdentity to develop and deploy ActivIdentity digital identification and authentication solutions combined with their industry-leading identity management and provisioning systems. These partners reach all major markets worldwide and address verticals, including government, healthcare, financial, and enterprise. ActivIdentity global alliance partners include IBM, Novell, and Sun Microsystems.

IBM

ActivIdentity offers a range of products for IBM, including SecureLogin Single Sign-On, ActivIdentity Card Management System, and 4TRESS Authentication Server, all of which are IBM Tivoli Certified. Together, these products enable IBM Tivoli customers to leverage their investments in Tivoli to issue and manage digital identities and use them to securely access facilities and information systems as well as digitally sign documents and transactions.

Novell

ActivIdentity continues to extend its range of joint solutions for Novell to include Novell SecureLogin and Novell Clinical Workstation, both of which utilize ActivIdentity single sign-on technology; Novell Identity Assurance for government and enterprise, which utilize components of ActivIdentity All-In-One ID; as well as two-factor authentication solutions for Novell NMAS, BorderManager, iChain/Access Manager, Security Manager, SUSE Linux, and Novell Client.

Sun Microsystems

Sun, as the creator of the JavaCard platform, has been a long-standing partner of ActivIdentity. The first and most notable joint project shared by Sun and ActivIdentity is the largest and most widely known smart card deployment in the United States: The DoD Common Access Card program, which is based on ActivIdentity technology, has deployed some 10 million smart cards to date. In addition, Sun has chosen ActivIdentity systems to deploy a smart card-based ID card to all of its employees for physical and logical access. Sun offers the ActivIdentity All-In-One ID and SecureLogin Single Sign-On products in conjunction with its Identity Management Suite to its customers worldwide.

Systems Integrators

ActivIdentity partners with the world's most respected systems integrators to deploy its digital identification solutions to government agencies and large enterprises. These systems integrators have built practices that include consulting, deployment, and operation of identity management and digital identification and authentication systems. ActivIdentity systems integrator partners include Bearing Point, CSC, Deloitte, EDS, General Dynamics, IBM Global Services, Lockheed Martin, MAXIMUS, Northrop Grumman, and Unisys.

Solution and Technology Partners

ActivIdentity must interoperate and integrate with a wide range of solution and technology partners to address the business and technical requirements of its customers to use their trusted digital identities to access information systems and facilities, communicate securely, digitally sign documents and transactions, and protect data. ActivIdentity partners with industry leaders to provide:

- ☒ **Information access.** Partners include Check Point, Cisco, Citrix, Juniper, and Microsoft.
- ☒ **Physical access controls systems.** Partners include AMAG, GE Security, Hirsch Electronics, Honeywell, Lenel, and Softwarehouse.
- ☒ **PKI certificate authorities.** Partners include Cybertrust, Entrust, Microsoft, and VeriSign.
- ☒ **Secure documents.** ActivIdentity partners with Adobe Systems to digitally sign and secure documents, forms, and workflows.
- ☒ **Data security.** ActivIdentity partners with PGP, Pointsec, SafeBoot, SafeNet, Utimaco, and WinMagic to encrypt and secure data.

FUTURE OUTLOOK

IDC forecasts that the market for IAM products will grow to more than \$5 billion by 2010, fueled by the following existing and emerging market demands. (These criteria will apply across a wide variety of industries and applications and will expand on a worldwide basis as business and technology continue to globalize.):

- ☒ Compliance with regulatory mandates (e.g., Sarbanes-Oxley, GLBA, HIPAA, HSPD-12, European Union Directive on Data Protection) as well as growing adherence to COBIT and ISO17789 best practices
- ☒ Consolidation of digital identities into a single, secure identity on one form factor
- ☒ Increasing and widely publicized incidents of identity fraud and compromised identity
- ☒ Increasing adoption of wireless and remote technologies
- ☒ Maturation of biometric technology
- ☒ Continued maturation of standards for identity federation and Web services security

Meeting Compliance

In the future, IDC believes that companies that build their IT infrastructures on a solid foundation of identity assurance will ease compliance requirements considerably because it makes all system access activities accountable. The ability for digital evidence to enable proof of actions and therefore facilitate workflow and ecommerce transactions is very important for the continued evolution of secure identity.

The trend toward SSO integration with smart cards for credential consolidation is growing as commercial enterprise and government agencies alike are searching for integrated, seamless, and solid IAM solutions to increase security, meet compliance mandates, and eliminate ID theft and fraud. ActivIdentity is one of the first IAM vendors to deliver a solution with full integration of robust SSO and smart card integration out of the box.

Consolidation of Digital Identities

IDC believes the industry has begun converging physical and logical authentication. Technologies such as eSSO, enabling automated credential management, and strengthening of application passwords have become key components of an overall identity assurance platform, greatly enhancing end user convenience and security. Further, IDC sees an increase in the use of eSSO for integration of the trusted authentication to all applications on the desktop, including those located outside the sphere of influence for an identity management deployment.

Steps for a Successful Identity and Access Management Deployment

In general, IDC believes the components of a successful, secure IT infrastructure should meet the following criteria to achieve maximum security and reliability while maximizing ROI:

1. Increase IT productivity and efficiency
2. Improve IT operational performance, reliability, and security
3. Control costs and improve scalability
4. Enforce and enhance system and security administration
5. Provide common consoles and data repositories
6. Optimize performance and availability; manage common events
7. Consolidate functional toolsets; tools integration
8. Integrate enterprise management software and "frameworks"
9. Support changing business requirements: adaptive flexibility
10. Support regulatory compliance (e.g., Sarbanes-Oxley, HIPAA)

ActivIdentity fulfills these criteria as a provider of strong authentication and digital identity solutions joined with leading industry players to deliver total solution sets to customers worldwide.

Unlike many closed, proprietary point solutions, ActivIdentity's digital identity assurance platform can deliver a comprehensive and complete set of integrated and open standards-based applications. This platform allows businesses, governments, and consumers to safely conduct their affairs in today's digital world.

CHALLENGES/OPPORTUNITIES

The most immediate challenge for ActivIdentity is to reassure current customers that existing products and contracts will continue to be upgraded and serviced. As the company makes good on its existing customer commitments, ActivIdentity and its partners can continue to educate and evangelize organizations as to the value of digital proof of identity as a fundamental element in helping companies become proactive, as opposed to reactive, to compliance and other legislative change.

The opportunity for ActivIdentity is to put the digital proof of identity in place, allowing organizations to move forward in adopting end-to-end solutions for compliance. Eventually, this technology will evolve to provide a single, universally accepted digital identity that can be assigned to a person and follow that individual securely for the remainder of his or her life.

CONCLUSION

Today, companies looking to achieve compliance and reduce ID fraud via elements of IAM/IDM technology must remember that it is not necessary to make radical changes to existing systems deployments. First, an organization must outline and understand the issues at hand and then outline the goals to be achieved. Very often, to enhance existing systems functionality to meet compliance, an IT organization must determine how best to apply a layer of trust in digital identity within the existing infrastructure.

This layer of trust in digital identity is fundamental to the success of the system as a whole, and while it significantly reduces exposure to risk, when implemented properly, it can reduce operating costs as well.

The combination of strong authentication and credential management enables ActivIdentity to achieve its technology mission: "to enable a single and secure electronic identity that allows access to computer systems anywhere, anytime." The company's goal is to provide the industry with the leading identity assurance platform, delivering strong authentication, SSO, smart card life-cycle management, and credential consolidation.

As previously stated, government standards, such as the FIPS-201 initiative, are pushing the need for universal digital identity assurance. A universally accepted secure digital identity assurance framework will ultimately be the key to the success of this type of initiative as it crosses international boundaries and differing industry segments. This concept is moving beyond government and into the commercial sector. In addition, large-scale identity projects such as those recently announced in Germany, Australia, and Spain are reinforcing this trend.

ActivIdentity is well placed to capitalize on this opportunity.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.