



OASIS Demonstrates SAML 2.0 Interoperability

In mid-January the OASIS SSTC approved the SAML 2.0 specifications as Committee Drafts and has submitted them to OASIS for balloting in pursuit of OASIS Standard status. This has released the industry to begin implementation of the draft standard. In February thirteen vendors teamed with the U.S. General Service Administration (GSA) E-Gov E-Authentication Initiative to demonstrate interoperability of the Security Assertion Markup Language (SAML) 2.0. SAML enables secure exchange of authentication, attribute, and authorization information between disparate security domains, making secure Internet e-business transactions possible.

"SAML 2.0 brings together SAML 1.x,

Liberty Alliance and Shibboleth functionality to provide a logical convergence point for new products and deployments in the coming months," said Dan Blum, Sr. VP and Research Director, Burton Group. "This OASIS InterOp demonstration offers an important proof-of-concept for the new specification."

"If you look at the backers of the Liberty Alliance, and the backers of SAML, they're one and the same now," said Rob Philpott, Co-Chair of the OASIS Security Services Technical Committee. "Identity is central in the digital ID world and we need ways to federate those identities. You also want to control who has access to that ID information. SAML 2.0 helps do that." ■

Applied Identity Completes \$8 Million VC Financing

Applied Identity (www.appliedidentity.com) today announced it has completed an \$8 million first round of institutional venture financing from Bay Partners and Sigma Partners. Applied Identity addresses the problems of enterprise network resource access control and identity management. The Applied Identity Identiforce™ policy enforcement gateway appliance works with a customer's existing authentication and directory services to cloak all network resources except those explicitly allowed to any user or group.

"Applied Identity has developed a breakthrough solution to a huge problem nearly every enterprise faces today – how to get highly granular access control and policy enforcement without adding significant cost and overhead to the corporate network," said Bob Williams of Bay Partners. "Applied Identity's implementation is simple to deploy, integrates with Microsoft's Active Directory or any LDAP-compliant solution, and requires no client-side interaction." "As a former CIO of a Fortune 100 company, I believe the market for a robust identity enforcement solution is enormous," said Pete Solvik of Sigma Partners. ■

Survey at HIMSS Says IdM Top HIPAA Priority

Identity and Access Management Solutions Provider BNX (www.bnx.com) conducted a survey of Health Care senior IT and security executives at the March Healthcare Information and Management Systems Society (HIMSS) show. The survey – developed to analyze Identity Management trends in the healthcare sector – revealed that despite the April deadline for compliance with the Security Rule of HIPAA, only 16% of those surveyed had a plan completed and implemented. 36% have a plan completed but not implemented, and 29% are still conducting analysis.

Even though only 33% of respondents

had Identity Management systems already in place, they ranked it as a top measure in strengthening security for 2005, a 100% increase from what they stated was important in 2004. Identity Management was considered the highest impact technology for compliance with HIPAA rules. When asked about the primary drivers for their IT security strategy, surprisingly, 35% of surveyed attendees found improving operational efficiency the highest priority. Other IT drivers, in order, were: strengthening security (33%), HIPAA compliance (19%), minimizing errors (7%) and reducing IT costs (6%). ■

XACML 2.0 Access Control Language Approved as OASIS Standard

The OASIS standards consortium members have approved the eXtensible Access Control Markup Language (XACML) version 2.0 as an OASIS Standard. XACML is used to represent and evaluate access control policies. “XACML is designed to standardize the use of declarative policy to control access to resources,” said Hal Lockhart, co-chair of the OASIS XACML Technical Committee. “XACML 2.0 can be of particular interest to those deploying SAML, looking for a practical way to implement RBAC or protecting hierarchical resources, such as portions of XML documents.”

XACML 2.0 incorporates new profiles for Role Based Access Control (RBAC), Privacy, and Lightweight Directory Access Protocol (LDAP). XACML 2.0 profiles also provide integration and hierarchical resources for the Security Assertion Markup Language (SAML) OASIS Standard. Dan Blum, Sr. VP and Research Director of Burton Group, noted, “Access control is a requirement of almost every application. XACML goes beyond simply denying or granting information access, it defines the mechanism for creating the rules and policy sets that enable meaningful authorization decisions.” ■

Logic Trends, Inc. Announces Acquisition of iconomics, LLC

Atlanta software consulting firm Logic Trends, Inc. has acquired iconomics, LLC, a Cleveland based software delivery and consulting firm specializing in the areas of identity and access management and infrastructure solutions. The acquisition of iconomics, LLC extends Logic Trends ability to offer its Enterprise Integration and Identity Management services in the Mid-West and Great Lakes regions. Additionally, this acquisition will strengthen and support customer relationships already established in the area and to provide services including Logic Trends Identity and Access

Management 5 (IAM5) program to iconomics clients.

Michael Hrobat, Managing Partner of iconomics, stated, “After having worked closely with Logic Trends for a number of years, we are excited that we will be able to further capitalize on the strengths of both organizations. Given the recent successes of our joint sales initiatives, this acquisition allows us to provide extended identity and access management programs and comprehensive solutions to our customers.” Logic Trends was recently named 53rd on the Inc. 500 List of Fastest Growing Private Companies in the United States. ■

RFID Car Keys & Gas Pump Pay Tags Carry Security Risks

A popular RFID system that is used to deter car thefts and as a convenience device for the purchase of gasoline can be defeated with low-cost technology, computer scientists from The Johns Hopkins University and RSA Laboratories have determined. Their findings, described in a new research paper, indicate that the encryption in RFID microchips in some newer car keys and wireless payment tags may not keep thieves at bay. Using a relatively inexpensive electronic device, criminals could wirelessly probe a car key tag or payment tag in close proximity, and then use the information obtained from the probe to crack the secret

cryptographic key on the tag, the scientists said.

“We’ve found that the security measures built into these devices are inadequate,” said Avi Rubin, technical director of the Johns Hopkins Information Security Institute and an author of the study. “Millions of tags that are currently in use by consumers have an encryption function that can be cracked without requiring direct contact.” The paper does conclude that “Our attack on the DST cipher by no means implies wholesale dismantling of the security of the SpeedPass network, nor easy theft of automobiles.” The research paper has been posted online at: <http://rfid-analysis.org/> ■



Liquid Machines Announces Document Control 5.0 for RMS

Enterprise Rights Management solutions provider Liquid Machines, Inc. announced the Beta release of Document Control 5.0 for Microsoft Windows Rights Management Services (RMS) for Windows Server 2003. Liquid Machines Document Control v5.0 extends RMS policy enforcement to desktop and enterprise applications including Adobe Acrobat and Microsoft Visio. Additionally, Document Control 5.0 will allow customers to use Microsoft Office 2000 and Office XP to view and modify RMS-protected documents created in Office 2003. Document Control 5.0 for RMS provides users with persistent protection of electronic information throughout the collaborative business process – from the moment of creation through distribution, editing, storage, and

subsequent destruction and disposal.

“Concerns over intellectual property leakage, regulatory compliance, and data privacy are making it necessary for organizations to invest in an area we refer to as Content Security,” said Dan Keldsen, Senior Analyst and Chief Technology Officer at Delphi Group. “As enterprises evaluate Content Security solutions, they must ask two important questions: Can the security scheme consistently be applied across platforms, applications, and content types and does the system enable collaboration and innovation as well as ‘locking down content?’ Delphi Group sees enterprise rights management (ERM) and solutions such as those from Liquid Machines and their partner Microsoft, as key components in a modern Content Security architecture.” ■

RFID Anywhere Simplifies RFID Network Deployment

Anywhere Solutions, Inc., a subsidiary of Sybase, Inc., announced RFID Anywhere, a middleware platform that helps enterprises plan, develop, deploy and manage RFID network solutions. With an advanced service-oriented architecture, RFID Anywhere speeds the deployment of RFID solutions through easy integration with existing applications and processes – even those that are highly distributed. In addition, the software directly manages RFID and other data collection and control devices, such as barcode readers and printers, so that developers and integrators are insulated from low-level interfaces and can focus on business logic.

“Challenges faced by customers implementing RFID solutions are similar to those found in mobile and remote applications, such as the need for always available access to information, integration of a variety of data sources and managing data and devices remotely,” said Steve Robb, senior director of marketing, iAnywhere. “With more than a decade of experience in solving these issues, iAnywhere is well positioned to help customers solve their RFID challenges.” Operating as a network service, RFID Anywhere provides extensibility so that a physical network of readers can be leveraged in additional, future, RFID use cases allowing multiple business scenarios to be addressed with a single solution. ■

BNX Releases Authenticated Sign-on for Healthcare

BNX Systems has announced the release of BNX Authenticated Sign-On 5.4. In addition to integrating strong authentication and enterprise single sign-on (E-SSO), BNX Authenticated Sign-On now offers healthcare users context management, supporting the Clinical Context Object Workgroup (CCOW) standard. Context management allows patient information in separate applications to be unified so that each individual application is referring to the same patient or encounter. Context management speeds access to patient records, increases productivity for clini-

cians and reduces medical or informational errors.

BNX Authenticated Sign-On offers more than 80 pre-built adapters to enable E-SSO to popular healthcare applications from leading vendors such as Cerner, GE, McKesson, and IDX as well as other enterprise applications and operating systems such as Microsoft Windows, Microsoft Outlook, and Lotus Notes. Adapters for additional applications can be created within minutes using the BNX Adapter Wizard ^ a GUI that does not require programming, scripting, or other changes to the applications themselves. ■

Liberty Alliance Releases ID-WSF 2.0 Specification

Liberty Alliance, a global consortium for open federated identity standards and identity-based Web services, announced the public draft release of ID-WSF 2.0, a second-generation framework for identity-based Web services. The framework has been extended to include support for SAML 2.0, specifically defining how SAML 2.0 assertions can be used to communicate identity information among identity-based Web services.

“Successful identity management has become a critical factor in application development and the necessary foundation for deploying all Web services,” said George Goodman, president of Liberty Alliance’s management board and director of Intel’s Visualization and Trust Lab. “These specifications provide a blueprint for driving convergence between federated identity and Web services specifications, a necessary step to complete interoperability.”

The Web services specification, first introduced in April 2003, is already in use at many organizations across the globe. The first interoperability compliance testing on the specification was completed in October 2004, at which time several companies illustrated support and compliance, including Hewlett-Packard, Nokia, Novell, NTT, Sun Microsystems and Trustgenix. ■

Gemplus Launches Smart Identity Management Systems

Smart card solutions provider Gemplus International S.A. has announced the launch of SafesITe Enterprise and SafesITe Corporate, two new smart identity management systems tailored to meet the needs of large enterprises and growing corporations based in North America. The two systems are based on Gemplus’s global smart card-based identity management solution suite, SafesITe, and combine network and building access control on a single, smart badge for enablement of two-factor authentication and the consolidation of security infrastructures.

Corporations and large multi-national enterprises have distinct identity management and security requirements, which is why Gemplus has packaged

and integrated two specific systems to address each of their needs. SafesITe Corporate is a user-friendly and readily deployable system that helps growing corporations deploy and manage smart badges in Windows environments for building and network access. SafesITe Enterprise is a flexible system that addresses the complex and wide scale needs of large multi-national enterprises. SafesITe Enterprise and SafesITe Corporate include smart cards, desktop software, readers, a management system, as well as personalization, issuance, and professional services. All components of the system are pre-integrated and tested, ensuring ready deployment and interoperability throughout a company’s legacy environment. ■

Radicati: Two Thirds of Directory Costs Professional Services

In recent publications, technical market research firm The Radicati Group, Inc. estimates that for every \$1 spent on the acquisition cost of enterprise directories, an additional \$3 is spent on professional services. They do find that identity management is becoming easier to deploy, however, as directory vendors begin offering not only better integrated suites, but also more simplified suites, combining many solutions into 2-3 major offerings, with much richer capabilities.

Despite this difficulty in deployment, Radicati sees significant market growth in identity management. “Over the past two years, directories have moved into

the zenith of their success, providing the indispensable foundation for popular Identity Management suites. In 2004 vendors embraced more innovative technologies, such as virtual directories, which will continue to change the way corporate data is managed across all systems and applications, as well as help to deploy any application company-wide.” Radicati estimates that identity management will grow from a \$738 million market in 2004 to over \$10 billion by 2008. By comparison, they estimate that the North American market for Web services will grow in that same time to \$2.7 billion. ■



Federal Smart Card Standard Approved

The U.S. Commerce Secretary has approved FIPS 201, the Federal Information Processing Standard for Personal Identity Verification. FIPS 201 lays out the technical and operational requirements for the Personal Identity Verification (PIV) system and card. The system is a requirement of Homeland Security Presidential Directive (HSPD) 12, which was issued in August of 2004. HSPD 12 called for the National Institute of Standards and Technology (NIST) to produce a federal standard for secure and reliable forms of identification for federal workers in six months. The first efforts at FIPS 201 met with resistance,

but the standard has been modified and is now approved.

The first phase of compliance is due by Oct. 25 and includes common ID and security requirements for applications that will use the new cards. Second phase compliance, due a year later, will require agencies to begin issuing interoperable cards to employees and contractors. No deadline has been set for completing that issuing process. The cards will not apply to national security systems and facilities. GSA schedule contracts for smart cards will be modified to require compliance with FIPS 201, and GSA plans to encourage multi-agency buys to take advantage of volume card discounts. ■

Ping Identity Announces Risk-Free Trial, Pilot & Production Federation

Ping Identity has announced an innovative new pricing model for their Ping Federate commercial federation product. Under the "PingFederate Now" program, enterprises can trial, pilot, or build federations in both internal and external production scenarios. PingFederate can be installed on as many servers as desired, with no limit on the number of applications, connections or users. Use of the server and future upgrades are free for up to 100,000 transactions. A variety of licensing options are available after 100,000 federated transactions have been reached.

Dan Blum, Sr. VP and Research

Director, Burton Group stated, „As the federation marketplace matures, one of the critical hurdles it must overcome is the problem of large enterprises needing to help their smaller partners realize the value of federating. Commenting on this innovative licensing model, Ping Identity CEO Andre Durand said, „You must fundamentally believe in the value of the federated approach to offer the market a solution under the terms of our PingFederate Now program. Companies are hungry for light-weight, standards-based solutions which can help them better integrate and secure their cross-domain applications, users and on-demand services. ■

MasterCard and mBlox Launch Cell Phone Fraud Detection

MasterCard and mobile messaging transmission and billing specialist mBlox, announced an agreement to integrate mBlox's mobile messaging service with Aristion, MasterCard's cutting edge fraud prevention tool. This new solution will become the first global fraud operation with twenty to thirty calls detection and alerting system, offering any bank a high quality, ready to use Short Message Service (SMS)-enabled solution. Existing Aristion users can install it in under an hour.

With this solution a customer first completes a simple registration process to enroll in the new service. Then, when a high risk transaction is identified, the customer will immediately receive an SMS text message on their cell phone to verify their transaction. If the consumer believes a fraudulent transaction has been committed, the bank can be notified to block further activity. This speed of response means cards can be blocked in a matter of minutes, reducing the number of fraudulent transactions and the impact for the bank.

MasterCard has launched this service globally and is concentrating initial efforts in Europe because of the highly saturated mobile services marketplace. Throughout 2005, MasterCard will be extending the service to Asia Pacific, SAMEA and later to North America. The product should start to impact consumers in the latter half of 2005. ■

Sun Announces Identity Auditor

Sun Microsystems, Inc. announced the Sun Java System Identity Auditor, a comprehensive identity audit solution to help improve audit and compliance performance. Identity Auditor enables customers to create a secure identity audit trail and present a unified view of an individual's identity and system access activities. The audit policy engine within Identity Auditor scans critical applications, flags audit policy violations and evaluates violation criteria, such as segregation of duties, unauthorized access changes, and erroneous access privileges.

To comply with regulations such as Sarbanes-Oxley and HIPAA, companies must be able to report on and manage who has access to critical information systems such as financial applications or medical records. Companies must provide data on historical access privileges as well as secure, auditable evidence that internal controls are in place. Identity Auditor helps automate the evaluation and enforcement of a company's internal identity and access controls so they can react quickly to any violations to minimize risk.

"Companies are spending substantial sums of money to hire and manage external consultants to perform auditing and compliance tasks for identity management activities," said Roberta J. Witty, Research VP, Gartner Inc. "To answer the question of 'Who has access to what?', and prove it, companies need a secure, automated analysis and reporting solution that is cost-effective and comprehensive in its capabilities." ■

IBM Acquires SRD

IBM has acquired privately held SRD, a provider of identity resolution software. SRD's operations will be integrated into IBM's Information Management software organization and SRD products will be immediately available from IBM. Financial details were not disclosed. The SRD technology helps organizations increase business insight by delivering an accurate view into individuals and relationships in real-time – associations that previously were nearly impossible to discover, enabling a wide range of solutions. Digital ID World profiled SRD in the March/April 2004 issue, delving into this one of a kind technology. IBM intends to integrate the SRD technology into its Business Intelligence (BI) platform.

"The seemingly simple questions of

'who is who?' and 'who knows whom?' cut across a wide variety of business problems today," said Janet Perna, general manager, IBM Information Management Software. "The SRD technology provides solutions to these age-old problems with unparalleled speed and accuracy." SRD software strengthens IBM's middleware portfolio via a multidimensional approach to analytics that dramatically extends the capabilities of identity-based applications. The combination provides value to business partners who deliver business intelligence and other applications that might require a single customer view, fraud detection, or customer relationship management across many industries, such as government, banking, insurance and healthcare. ■

CA Announces Roadmap for Netegrity Integration and SAML 2.0

Computer Associates International, Inc. has unveiled its strategic roadmap for a complete, integrated and open identity and access management (IAM) architecture. The roadmap features an aggressive timeline for continued innovation in identity and access management, including important advances in federation, compliance and policy management – as well as continued development of technology acquired through acquisition of Netegrity and integration of the Netegrity product line into CA's industry-leading eTrust IAM Suite.

"Deep integration between products in an identity and access management product suite simplifies administration, monitoring, and audit processes for large enter-

prises," said Phil Schacter, VP and service director of Burton Group. "CA is demonstrating that this level of integration is possible, and is setting a high standard in the market for similar capabilities in any identity and access management suite."

CA will continue its aggressive identity federation strategy with the delivery of support for SAML 2.0 in eTrust SiteMinder in the summer of 2005. Future releases of eTrust solutions will provide comprehensive auditing and provisioning capabilities for federated environments. These solutions will also enable eTrust users to give their customers control over how their private information is shared within federated business partnerships. ■