



## Sun Integrates ID Management Portfolio

Sun announced the consolidation and integration of their Identity Management portfolio from eight products into three while making them more modular. The Java System Identity Manager combines user provisioning and meta-directory capabilities to securely manage both identity permissions and profiles, while also providing synchronization services for identities across the enterprise. The Java System Access Manager manages secure access to both internal and external web-based resources, and supports both Liberty Phase 2 and SAML 1.1 federation. The Java System Directory Server Enterprise Edition is a central repository for storing enterprise identity information and provides enterprise-level services such as built-in fail-over, load-balancing, security and enhanced integration with Microsoft Active Directory.

"Effective identity management is the single most important enabler of the networked economy and arguably one of the largest market opportunities," said Jonathan Schwartz, Sun President and COO. Sun also announced new partnerships with Deloitte & Touche and PricewaterhouseCoopers. Sun offers packaged integration with over 60 partner-supplied enterprise resources to provide end-to-end compatibility with third-party components and existing investments. Supported operating platforms include: Solaris, Linux, Windows, HP-UX, IBM AIX and IBM OS/390. Supported enterprise software environments include: BEA Systems, Entrust Technologies, IBM, Microsoft, Netegrity, Novell, Oblix, OpenNetwork, Oracle Corporation, PeopleSoft, RSA Security and SAP. The new identity management products will be generally available July 1, 2004. ■

## SourceID Releases WS-Federation Open Source Code

SourceID ([www.sourceid.org](http://www.sourceid.org)) has announced a new release of its open source WS-Federation code in conjunction with a WS-Federation demonstration at Microsoft's TechEd conference. SourceID is sponsored by Ping Identity which recently conducted a survey to gauge the interest in federated identity management that showed a growing interest in the WS-Federation protocol.

SourceID began as an open source project focused on federated identity using the Liberty Alliance specifications in January of 2002. Its Liberty code has been logo certified interoperable by the Liberty Alliance, and SourceID has expanded its efforts to add open source SAML and WS-Federation projects. SourceID has become widely recognized as the destination for individuals and enterprises wanting to implement the varied protocols and specifications associated with federated identity. With over 5,000 downloads to date, SourceID continues to build community around federated identity. ■

## Email Caller-ID and SPF Specs to Merge

A concern of those hoping identity comes to email to fight spam and spoofing is that competing standards will create confusion and delay adoption. Microsoft Corp., author of the Caller ID for E-mail proposal, and Meng Wong, co-founder and CTO of Pobox.com and author of the Sender Policy Framework (SPF), announced that they have agreed to converge the two proposals into one specification. Both protocols are designed to help eliminate domain spoofing and provide greater protection against phishing schemes. By providing a unified specification, Microsoft and Wong hope to simplify industry adoption of effective e-mail authentication technology, thereby helping to more swiftly provide greater spam protection to e mail users worldwide. A formal specification will be published in June and submitted to the Internet Engineering Task Force (IETF) standards body for evaluation and review, as part of its work to

define effective industry Internet e-mail standards to address the problem of spam.

Under the merged proposal, organizations will publish information about their outgoing e-mail servers, such as IP addresses, in the Domain Name System (DNS) using the industry-standard XML format. Backward compatibility will be provided for the many domains that have already published information in the SPF TXT format. The converged specification will enable receiving systems to test for spoofing at both the message transport (SMTP) level, or envelope, as originally proposed in SPF, as well as in the message body headers, as originally proposed in Caller ID. Testing for spoofing at the message transport level allows receiving systems to block some spam messages before they are sent. For cases in which a deeper examination of the message contents is required to detect spoofing and phishing attacks, the Caller ID-style header check can be employed. ■

## ActivCard Supports MasterCard's Chip Authentication Program

ActivCard Corp. announced it will support MasterCard International's Chip Authentication Program to offer its customers chip-based cardholder authentication solutions for non face-to-face transactions. As part of its global MasterCard SecureCode initiative, MasterCard created the Chip Authentication Program (CAP), which is designed to build on the ease of use and security of an EMV-compliant smart card for authentication through a user's PC. With CAP, a cardholder inserts a smart card into a card reader and enters a PIN. The card's chip then generates a value that the cardholder places into the issuer authentication window that appears during completion of online purchase. This solution is supported by both standalone and connected smart card readers.

ActivCard smart card software and hardware products leverage the full capability of chip technology for validating a cardholder's identity – with the ideal combination of convenience for the cardholder, reliability for banks, and liability protection for merchants. While enhancing the security of MasterCard payment transactions, ActivCard products make it possible for financial institutions to offer their customers enhanced online services, via the Internet. "ActivCard solutions leverage the familiar ATM experience of entering a PIN to receive access to banking services," said Mehdi Bery, ActivCard Solution Marketing Manager, "while ensuring the complexity of trusted transactions are transparent and simple for the cardholder." ■

## Liberty Alliance Looks to Federate Digital TV

Digital television, the Internet and the convergence of communication technologies have created an overabundance of programs and personalization options from which the average consumer can choose. The use of DVRs – devices that record, store and playback live television – has skyrocketed as a means to manage and automate viewing preferences. The Liberty Alliance Project and TV-Anytime Forum, have announced a joint initiative to address the requirements for digital identity in the Digital Video Recorder (DVR) market, including issues of privacy, security and interoperability in TV-Anytime's upcoming Phase 2 specifications. "Privacy and security are two of the biggest issues around delivering any type of personalized service," said Michael Barrett, president of Liberty Alliance. "This is why our work has been so applicable to a cross-section of industries – from wireless to financial services to government.

Working with an established organization like TV-Anytime will help ensure the television industry and consumers can easily reap the fruits of recent advances in digital identity management."

The TV-Anytime Forum was created in 1999 to develop a universal standard for DVRs. Now working with the Liberty Alliance, it will expand on existing work to address new content types, emerging technologies, and ongoing issues such as privacy and security of viewer preferences. "Since its inception, TV-Anytime has been serious about the rights management issues that will play a role in the DVR market and on-demand broadcasting," said Simon Parnall, Chair of TV-Anytime Forum and Director of Advanced Technologies in the TV Platforms Division at NDS. "This is where we see synergy with the Liberty Alliance and we look forward to seeing fruit in the liaison relationship between our two organizations." ■

## Netegrity Releases IdentityMinder eProvision 4.0

Netegrity announced the release of its Netegrity Identity Minder eProvision 4.0 provisioning solution, completing the integration of their acquisition of Business Layers. "This release marks an important milestone for Netegrity as it illustrates the successful integration and execution of our provisioning acquisition," said Bill Bartow, vice president of engineering at Netegrity. "With this release we are leveraging Netegrity's longstanding expertise in enterprise class manageability and platform neutrality, and adding that to eProvision's existing leading functionality and scalability."

The new version has full J2EE architecture and features enhanced workflow and simplified graphical administration,

an enhanced policy builder, and optimized task generation and scheduling. IdentityMinder eProvision is a component of the Netegrity identity and access management product line which enables companies to manage external and internal users and their access to both enterprise and Web applications. "Implementing provisioning is a two-edged sword for many companies. They need to demonstrate success high and early, yet select a solution that is capable of meeting the more complex and shifting challenges of today's business environments," said Kevin Kampman, practice manager and senior consultant at Burton Group. "Netegrity has improved eProvision with features that address these immediate and long-term deployment objectives." ■



## Precisia Produces RFID tag with Printed Antenna

Precisia, LLC, a separate business unit of Flint Ink Corporation, announced that it is the first company in the world to produce fully functional radio frequency identification (RFID) tags with high-speed printed antennas in one location. RFID tags consist of two essential components - a chip and an antenna. Precisia's innovative manufacturing processes utilize conductive inks to produce printed antennas at high speeds in place of copper, aluminum or screen-printed antennas. Its tag production system assembles the unique components of an RFID device in one location, the first

step toward complete high-speed antenna printing and chip attachment in a single production process.

"This milestone gives us the potential to break time and cost constraints that have limited the production capacity of mass quantities of RFID tags," says Jim Rohrkemper, president of Precisia. "Today, we can formulate and manufacture conductive materials, print hundreds of thousands of antennas per hour, and attach RFID chips or straps at a rate of a few thousand per hour. We are working to attach straps at high speeds by the end of the year." ■

## Unisys Completes Acquisition of ePresence

Unisys Corporation announced that it has completed the acquisition of the assets of ePresence's security services and identity and access management solutions business. Unisys adds approximately 90 skilled staff and a suite of next-generation identity and access management to extend and enhance an already broad portfolio of Unisys security services. In addition, ePresence customers will now have access to the full range of Unisys solutions.

The management of user identities and

access to organizational resources is one of the top security challenges facing enterprises and governments today. It is a critical requirement for Web-based e-business and e-government initiatives. Identity and access management involves controlling the process that enables people or systems to have secure, consistent access to business resources, including networks, business applications and organizational information through the use of digital identities, such as passwords, smart cards, digital certificates and biometric identifiers. ■

## Microsoft Modifies NGSCB to Simplify Use

Microsoft announced that it is modifying its NGSCB trusted computing architecture to make it easier for application programmers to integrate. The original NGSCB architecture isolated a project from the Windows development process and also required modifications to applications using NGSCB features. The revised NGSCB will make its capabilities far more accessible to applications without extensive modifications. Microsoft Product Manager Mario Juarez said, "Last year, we presented a very preliminary vision. Since then, we have refined the vision and we're making changes to provide broader value to customers and partners."

There was a brief "media flap" when the announcement was misinterpreted as saying Microsoft had killed NGSCB. "[Microsoft is] broadening the capabilities of the technology," said Juarez, "and evolving the project. It's the exact opposite of us shelving or killing off the project. It's about giving it broader value. We're still targeting Longhorn. We're looking to make sure that the work we're doing is appropriately integrated into Longhorn, but the architecture will naturally evolve as we receive feedback from customers and partners." ■

## Fellowes Standardizes on M-Tech's IDM Suite

Fellowes, a global supplier of office products for businesses and homes has selected the M-Tech Identity Management Suite to administer their corporate identity management requirements for users' accounts and passwords, as well as provide self-service employee access to network resources. Fellowes was facing several key user provisioning and password management challenges, including managing user IDs and passwords for their employees across heterogeneous environments, and multiple servers.

"M-Tech's IDM Suite was the clear choice to meet our identity management requirements. It will provide us with a comprehensive and secure solution that has already proven to deploy rapidly and require minimum customization," said Brad Hillebrand, manager of enterprise technology for Fellowes. "In addition, our initial implementation of M-Tech's password management component was transparent to the user community and created no disruptions in workflow." ■

## Novell Announces Roadmap for Next-Gen Identity Services

Novell has announced a strategy to help customers significantly reduce the time and cost required to design and configure sophisticated identity management systems through next-generation tools. These tools will be based on the open source Eclipse framework and will allow administrators to visually architect and build a sophisticated identity foundation. Novell will combine its Nsure and exteNd technologies to provide advanced identity management applications for enhanced user provisioning with workflow to dramatically simplify the deployment of identity-based services. Novell will also provide pre-built identity applications. For example, ready-to-use portals will enable the dynamic generation of complex corporate directories and organizational charts that display multiple levels of hierarchy with multiple view criteria. When individuals change roles or take on new responsibilities, managers can easily re-provision the employee by dragging and dropping the employee's profile within the organization chart.

"Identity management can be a complex problem, particularly if you want to go beyond basic issues to fully leverage the power of identity across your organization," said Chris Stone, Novell vice chairman - Office of the CEO. "Novell is continually innovating to make it easier for organizations to manage users and their identities and to leverage them through identity-based applications that have a real business impact. Novell is a recognized market leader in identity management technology, and our roadmap puts us further ahead." ■

# OASIS Finalizes WS-Security 1.0 Specification

The OASIS international standards consortium members approved the Web Services Security (WSS) version 1.0 as an OASIS Standard in April - their highest level of ratification. WSS offers a trusted means for applying security to Web services by providing the necessary technical foundation for higher-level services. WS-Security handles complex confidentiality and integrity for SOAP (Simple Object Access Protocol) messages, providing a general-purpose mechanism for associating security tokens with message content. Designed to be extensible, WSS supports multiple security token formats.

WS-Security was originally crafted by

Microsoft, IBM and VeriSign to secure and manage the identity and integrity of Web services messages, and contributed to OASIS in 2002. The specification has evolved during the standards process, and final approval creates a standard version of WS-Security for the first time. WSS builds upon existing security technologies such as XML Digital Signature, XML Encryption and X.509 Certificates to deliver an industry standard way of securing Web Services message exchanges. Providing a framework within which authentication and authorization take place, WSS lets users apply security technology and infrastructure in a Web Services environment. ■

---

## Microsoft Hosts WS-Federation Interop

This May at TechEd, Microsoft Corp., together with six of the industry's leading identity management vendors, previewed interoperable federated identity management solutions based on the Web services architecture (WS-\*). Software companies IBM Corp., Netegrity Inc., Oblix Inc., OpenNetwork Technologies, Ping Identity Corp., RSA Security Inc. and Microsoft successfully demonstrated how their identity management technologies interoperate using the Web Services Federation (WS-Federation) specification, part of the WS Security set of specifications.

"Connecting companies offers significant business benefits by streamlining processes and enabling new business opportunities. However, customers have said that connecting with their partners is too complicated and often not cost-effective," said Andrew Lees, Microsoft Corp. VP for Server and Tools Marketing. The demonstration showed how federated identity management based on WS-Federation and the WS-\* architecture can simplify the work of IT professionals as they seek to cut the cost and complexity of passing identity credentials across security and organization boundaries in a Web services environment. ■

## Survey Shows Ease of Getting Passwords

An impromptu man-on-the-street survey conducted in April (as part of the Infosecurity Europe conference) showed that people will voluntarily give up their passwords surprisingly easily. Nearly three-fourths (71%) of the office workers approached at the Liverpool Street Station for the survey were willing to give up their password in return for a chocolate bar! The survey also found that a majority of those workers would take confidential information with them when they change jobs.

Over one-third (37%) of those approached immediately gave up their password. For the rest, the interviewers used “social engineering,” such as suggesting that the password might be a pet’s name, etc. When pressed in this fashion, an additional 34% coughed up their computer passwords. The survey further indicated that 47% of the workers would likely give their password to a phone caller if asked, and 40% knew the passwords of their co-workers, and 55% would reveal their passwords to their boss if asked. ■

---

## Ping & Oblix Partner on Federated Business & Legal Solutions

Ping Identity Corporation today announced that Oblix has joined its Business and Legal Partner Program to help users of federated identity technologies address the risk, liability, quality and compliance issues of cross-company single sign-on and identity attribute sharing. Federated Identity provides companies with standards-based infrastructure for enabling cross-company single sign-on, dynamic user provisioning and identity attribute sharing. Through identity federation, companies are able to extend their security perimeter to trusted partners while providing more frictionless access to protected resources. New identity federation standards provide companies with the foundation for securing their outsourced business processes, hosted applications and web services while simultaneously addressing a host of other security, man-

agement and integration challenges.

“It’s only through an in-depth understanding of the protocols and their use-cases that partners engaged in identity federation can come to comprehend the full spectrum of legal and business issues surrounding cross-company single sign-on. Our solutions are designed to reduce the time, cost and effort associated with creating the appropriate agreements and structures,” said Linda Elliott – President of the PingID Network, Committee Chair of the Electronic Authentication Partnership and former Visa International Senior Executive. Ping Identity’s business and legal solutions range from templates around bi-lateral agreements to the PingID Network, the first identity network and membership association designed to provide a shared legal and business framework for quality assured identity federation. ■

## MaXware Integrates with Microsoft MIIS

MaXware AS announced that its Provisioning solution, MaXware Identity Center, will integrate with Microsoft Identity Integration Server 2003, Enterprise Edition (MIIS), the company’s identity lifecycle management offering. As a result of this integration, users will be able to benefit from a scalable and flexible identity management solution that integrates advanced synchronization capabilities with sophisticated provisioning and workflow functionality. By combining the two offerings, organizations are able to dramatically reduce security risks while decreasing administrative costs associated with keeping identity data current.

Together, MIIS 2003 and Identity Center enable end users to be more productive by allowing them to access needed systems faster, while enhancing corporate security through terminating employee access once the employee leaves a company. In addition, administrators are able to benefit from automated synchronization of identity information across a wide variety of applications, which improves their effectiveness. “MaXware provides additional features, such as robust workflow and provisioning capabilities, to enhance an MIIS deployment,” said Elizabeth Mann of Mycroft Inc. “It makes perfect sense for MaXware to port this added functionality to MIIS -- enabling enterprises to take advantage of the combined years of identity management experience shared by the two companies.” ■

# ClearOrbit Offers “Layer-In” RFID for Any ERP

**R**eal-time supply chain execution (SCE) software solution provider ClearOrbit has announced a product suite that allows companies to “layer-in” complete RFID capability on top of existing ERP systems, without requiring custom code or the “tear out” of old bar code or ERP software. The ClearOrbit solution—which includes ClearOrbit’s Compliance Label Manager, RFID Tracker, and Collaborative Print Manager—leverages the same configurability and scalability used to power bar code, print label compliance, and RF/mobile connectivity at thousands of manufacturing and distribution facilities across North America, Europe, and Asia.

“ClearOrbit is a company with a history of integrating bar code devices, printers, scales, and other real-time sources of supply chain information. They have grown up getting their hands dirty solving these kinds of problems,” said Steve Banker, Service Director, Supply Chain Management, ARC Advisory Group. “RFID is just another form of real-time data. As a result of its history, the ClearOrbit architecture is well suited to supporting RFID.” By driving RFID and bar code label production from a customer’s ERP, suppliers can easily comply with RFID requirements. All that is required is an RFID printer and an Internet connection at the supplier’s site. ■

---

## BMC Enhances Identity Management with Auditing

**B**MC Software, Inc. announced that they have expanded their Identity Management suite, CONTROL-SA, into the rapidly growing audit and regulatory management arenas. The new offering, InSight for CONTROL-SA by Consul, developed by Consul risk management, Inc. and based on their InSight Security Manager solution, delivers administrative and auditing capabilities to help customers further ensure their security event and policy management services while saving them valuable time and reducing consulting and auditing costs.

InSight for CONTROL-SA by Consul helps customers ease the pains of regulatory mandates such as Sarbanes-Oxley and Basel II by providing detailed audit

and exception reports and event-based alerts. Customers looking to address these challenges will also benefit from the CONTROL-SA Identity Management suite’s ability to simplify the user provisioning process through an intuitive interface. By adding the Consul functionality, InSight for CONTROL-SA by Consul offers customers a powerful identity management solution that streamlines and ensures the provisioning process, policy-based event management, and actionable audit. “Audit is an integral part of identity management – it ensures that the security policies that a company puts in place are effective and being complied with,” said Somesh Singh, VP and GM, Security Business Unit, BMC Software. ■