

WHITEPAPER

eB2Bcom Identity & Access Management Solutions

eB2Bcom today announced the immediate availability of eB2Bcom Identity Management Suite. Complete with a robust, comprehensive set of access control, identity administration, provisioning and directory services capabilities together with Professional Services, this release enables organisations to manage the end-to-end lifecycle of user identities across heterogeneous enterprise resources within and beyond their organisational boundaries, while helping to streamline sustainable compliance policies and controls.

eB2Bcom Identity Management suite integrates multiple key software solutions that eB2Bcom partners with, together with eB2Bcom organic development including Web access management, user provisioning, identity federation, virtual directory and Internet directory services, as well as directory security. Built on open-standards, eB2Bcom Identity Management suite is hot-pluggable application suite that interoperates with packaged applications including Microsoft Exchange, SunOne, Lotus Notes, Microsoft Active Directory, SAP, IBM DB2, Oracle E-Business Suite, Oracle's JD Edwards EnterpriseOne, PeopleSoft Enterprise and Siebel applications, Salesforce.com and many other applications. The new release also offers support for a range of different platforms such as Solaris 2.6 up to version 10, Windows 2000, 2003, Vista and two varieties of Linux platforms, demonstrating eB2Bcom's commitment to heterogeneity.

Each component of eB2Bcom Identity Management features a range of capability including full compliance to SOX, JSOX, HIPAA as well as standards such as ACP 133, ACP 145, LDAPv3, XMLeD, XLDAP and WS and a range internationalization and localization support for many languages including support for double byte.

Added to this integrated set of solutions, eB2Bcom Identity Management provides a comprehensive set of Professional and holistic Identity Solutions consultants to undertake Identity and Access Management projects for customers.

Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials.

The underlying problem is the absence of federated directories. Microsoft defines federation as "the technology and business arrangements necessary for the interconnecting of users, applications, and systems. This includes authentication, distributed processing and storage, data sharing, and more." Federated directories interact and trust each other, thus allowing secure information sharing between applications. Companies are currently running isolated, independent directories that neither interact with nor trust each other. This is a result of applications having their own proprietary identity stores. Each proprietary directory requires its own method of user administration, user provisioning, and user access control. This scenario, sometimes referred to as identity chaos, sparks growing problems in a company's technology infrastructure. The problem with proprietary identity stores is that users require a logon for every application, which in turn burdens users with having to remember numerous username and password combinations. The problem with proprietary administration is that every application will have its own set of tools, procedures, and policies to manage users.

Therefore, each new application adds a significant burden on the IT staff and unnecessarily complicates a company's identity management infrastructure. The problem with proprietary user provisioning is demonstrated in the amount of time necessary for a user to be given access to the resources needed to conduct business. The problem with proprietary user access control is that it leads to various methods of authentication within the company. Therefore, users are burdened with having to logon and authenticate multiple times and with various credentials. Due to the functional inability of these current processes, companies are finding it more difficult to manage user identities throughout the identity lifecycle.

The identity lifecycle consists of account provisioning, maintenance, and removal (deprovisioning).

- Account provisioning consists of giving users the appropriate level access to resources necessary to do their job. Account maintenance consists of keeping user identity information up-to-date and to appropriately adjust levels of access to resources needed to conduct business.
- Account de-provisioning consists of deactivating the user account when the user is no longer affiliated with the company. As companies rely more heavily on computerized systems to run the business, companies are experiencing increased difficulty in efficiently managing user identities at each of the three stages of identity lifecycle management.

The business risks associated with the current user identity management techniques are lower productivity, duplicate and conflicting user information, lack of information security, and difficulty in evaluating regulatory compliance. All of the above business risks result in increased costs. The loss of productivity is caused by the amount of time it takes to execute routine account management tasks such as password resets, changing identity information, and provisioning access to resources. For example, for companies with more than \$500 million in annual revenue, META group research shows that the average time to complete a user provisioning request is 6 to 29 hours. The lower productivity of the IT help desk also affects the user, who has to wait to gain access to resources.

Due to the number of identity stores, duplicate and conflicting user information threatens the quality of customer service and reduces productivity due to erroneous data. For companies with more than \$500 million in annual revenue, META group research shows that, on average, internal user information is stored in 22 different identity data stores and external user information is stored in 6 different identity data stores.

The identity management infrastructure consists of many authoritative sources, a directory Infrastructure component, an administration component, a directory integration component, a provisioning component, an access control component, and a generalized application interfaces component. The authoritative sources are the point where identity data originates. For example, an authoritative source for user's contact information may be an existing human resources database. An authoritative source for a user's email address would be the company email application.

The main component of the identity management solution is the Internet LDAP or XML directory. The directory component stores identity and resource information, policies, and user credentials. It provides a logical architecture to define schemas and namespaces. It protects the confidentiality, integrity, and consistency of identity data as well as provides for monitoring and auditing of its data. LDAP, which is based on the ISO X.500 specification, is the emerging directory standard. Using the LDAP protocol, any application running on any platform can query and access data stored in the LDAP directory via TCP/IP. LDAP can be implemented over HTTP to leverage Internet communications. If sensitive communication needs to be secured, LDAP can be implemented over SSL or TLS. The administration component, directory integration component, provisioning component, and access control component interact directly with the directory.

The directory integration component has two main functions. First, it facilitates the bi-directional flow of information due to synchronization of changes between the directory and other identity stores. This is using meta-directory services, custom scripts, or import/export utilities. Alternatively it facilitates the virtualization of Identity across the enterprise by doing real time jobs rather than integration. Although user accounts may be stored in various sources scattered across a heterogeneous environment, the directory integration component can create a unified view of user account. Secondly, it processes the unidirectional flow of data coming from authoritative sources and transfers the data into the identity management system.

The provisioning component provides the tools to manage user and application access to resources. The three main functions of this component are to efficiently provision users, deprovision users, and manage provisioning policies. Users are provisioned with the appropriate amount of access based on company defined

application definitions. Application definitions define the appropriate amount of access required to perform a specific business process. Application definitions may specify access to multiple resources. Users may be assigned to any number and combination of application definitions. Users are de-provisioned rapidly because the component knows what the user has been provisioned. Users are effectively de-provisioned if their account is disabled or if their application definitions are removed. Provisioning policies can be centrally administered to ensure that policies are applied universally and uniformly.

The access control component generally called ESSO provides management of authentication and authorization methods. The access control component relies on policies and allows for Role Based Access Control. Role Based Access Control manages user access based on a grouping of functions, rules, or privileges. This component tracks user sessions to maintain state and conserve bandwidth.

The administration component provides the tools to manage and search directory entries. The administration component provides a framework to delegate administration to certain departments, business partners, or users themselves. This component allows users to reset their own passwords. Customized application interfaces can be tailored to each user, which helps to ensure that users are only given the least amount of privilege necessary.

The generalized application interfaces component allows developers to interact with the identity management system without having to interface directly with vendor-specific application interfaces. There is a directory integration interface, provisioning interface, access control interface, virtual directory access and an administration interface. The directory integration interface facilitates the one-way data flow and data conversion from the authoritative sources to the directory component of the identity management system. The provisioning interface transfers data from the directory component to the systems to which it provisions.

The access control interface passes user credentials to the access control component. The administration interface passes information between any components of the identity management system. There may not be an administration interface to allow communication between any two components. The identity management solution consists of various software packages.

Companies tend to select "best-of-breed" products that address five of the seven components of the identity management infrastructure: directory, administration, directory integration, provisioning, and access control. The generalized application interfaces component is not included in the solution because it is custom developed after the software packages are selected. The generalized application interfaces component is not provided by any vendor, but is instead created by each company to address the specific identity management solution that is implemented. Authoritative sources are not included in the identity management solution because they already exist in the company as the directories, databases, and applications that act as "systems of record" for the information they contain.

Provisioning in Identity Management is predicted by leading analysts to be a multi-billion dollar market by 2010 and is one of the fastest growing areas in the market today. Provisioning is a must: As directory proliferation leads to an increased state of enterprise complexity, with disparate data stores existing across diverse technical and organizational environments, it's becoming more challenging to manage, synch, create and migrate data across (and into) directories.

This is being driven by:

Reducing Cost: user administration and support is one of the largest cost elements within organizations today. Automated Provisioning reduces the help desk burden by providing users with self service provisioning and removing the manual overhead associated with provisioning users.

Simplifying Complexity: automated provisioning often involves an approval process which if managed manually gets extremely complex due to the high volume of related tasks. Automating this process ensures consistency and accuracy and removes complexity.

Increasing User Productivity: new users can take days if not weeks to become fully productive as they do not have access to the tools and applications required to do their job. Automated provisioning ensures users are provided with the tools and applications without undue delay.

Improving Security: in a manual provisioning process the complexity and pressures can lead to human error. Automated provisioning removes human error and ensures users are provisioned and de-provisioned in a timely, consistent and accurate way eliminating the opportunity for security breaches.

Generating Return On Investment: In addition to the above drivers automated provisioning delivers a rapid Return on Investment making it extremely attractive to organizations today.

Key solutions include:

* **eB2Bcom Identity Manager** (provided by partner MaXware Identity Centre) - automates the process of provisioning IT resources in real time across heterogeneous business processes and managed platforms; is now integrated into the eB2Bcom Identity Management framework; features a new module for audit and compliance with expanded data capture, an SOX and JSOX framework, improved reporting and comprehensive platform support as well full support for Role Based Access control; As companies face the challenge of managing identity information, they must implement a technology solution that will help them strengthen business relationships, meet regulatory requirements and create efficiencies that sustain financial viability. MaXware Identity Center is a suite of products that helps organizations handle the complex requirements of identity management by offering provisioning, workflow, password management, reconciliation and Meta directory functionality in a single, vendor-neutral software solution. MaXware's modular approach allows an organization to deploy the entire identity management stack all at once or deploy the components in phases to meet the organization's need for process management and cost control. Building on the features supplied with the MaXware Identity Center, managers can provide value and return on investment and achieve buy-in from senior executives. MaXware Identity Center reduces the cost of managing your applications and enables you to deploy new applications in a timely manner. The architecture of MaXware Identity Center is designed to provide maximum flexibility, scalability and security in a single software solution. This allows identity management across multiple applications and databases both within the organization and in an extranet environment. The MaXware Identity Center offers a complete range of identity management functions: • Workflow • Rules- and roles-based provisioning • Meta directory • Password management and very comprehensive Audit and monitoring. The MaXware Identity Center is used to provide control of all identities within the organization, not only for employees, but also for contractors, customers, partners and other identities that need to access the organization's applications. Using MaXware Identity Center will improve the overall quality of the identity information within the organization. The solution proves who has been granted access, and who approved the access. It can be configured to connect to any number of different applications, and to ensure that the identity information is correctly updated in each of these applications. In addition, the web-based workflow can be used to define an approval process before access is granted or other operations are performed. As well providing full support for eB2Bcom Internet Directory services, MaXware Identity Centre is certified for, **Encentuate TCI**, **Computer Associates** Identity and Security Solutions and **RSA**.

* **eB2Bcom Access Manager** (provided by partner Encentuate TCI) - provides full Enterprise Single sign on (ESSO) including Windows single sign on, Legacy Single Sign on and Web single sign-on, identity administration and comprehensive reporting and auditing; This includes advanced password management capabilities, performance enhancements, shared-secret enhancements to improve security between software components, additional authentication triggers and new third party platform certifications; ESSO tools provide the ability for users to authenticate once to the tool and be subsequently and automatically authenticated to other target systems when they are accessed — almost always without modification to the target systems. ESSO tools provide this functionality for systems that use Windows, network, Web and terminal client interfaces. ESSO tools also handle password change requests from target systems. Encentuate was founded in 2001, and it is currently an ESSO pure-play vendor. Encentuate's TCI product implements a middle tier for administration and policy and credential storage. The initial identity profile and attribute data can be brought in from a variety of directories including eB2Bcom Internet Directory service, and connectors are provided for this as part of the base product. Full support for eB2Bcom Identity Manager is provided In addition to SSO support for Web, desktop and legacy applications, Encentuate Web Workplace also provides SSO to any published Web applications for workstations and PDA-based browsers, without requiring the SSO agent to be installed on the client. The administration component is Web-based and provides very good granularity regarding security policy settings by users and groups. Canned but good reporting capability is built in. TCI's has very good ease of integration with target systems. Sign-on automation is wizard-based and XML-parameter-driven. TCI also has good features for providing post sign-on automation. A variety of strong authentication devices are supported and OTP tokens, biometrics and smart cards are supported for secondary authentication to high-risk applications. Encentuate also sells a "smart label," called iTag, which is a passive proximity/radio frequency ID tag that can be affixed to any device the user carries and can be used as one form of authentication to TCI. Encentuate also supports the use of a cell phone with an OTP code as the authentication token.

* **eB2Bcom View500 Internet Directory Services** - an LDAP v3 and native XML directory that leverages the scalability, high availability and security features of an XML Database; includes enhanced LDAP-based replication, integrated search engine with support for component matching, PKI matching rules, synonym and word matching, stem matching, acronym matching, sounds like matching and full support for open standards. It also offers password integration with Active Directory, and synchronization support for many applications; it also provides the ability to handle multiple schemas operating on the single platform as well as support for a variety of authentication methods including PKI. eB2Bcom View500 Internet Directory Services is scalable to tens of millions of entries in a single directory server and in consequent smaller footprint than others, with no restrictions on the number of entries, size or number of attributes, depth of the DIT, and numbers of schemas in operation or the number of connected users. It includes an optimized bulk loader for fast loading of entry sets of all sizes, with negligible degradation in load speed between the first and last entries loaded and which restarts rapidly after power failures regardless of the total number of entries. It also supports instantaneous moves and renames of non-leaf entries in the DIT and links are automatically maintained despite moves and renames e.g. "managed by", "manager of" relationships. It can also be configured to enforce various referential integrity constraints. eB2Bcom View500 Internet Directory Services comes with its own Web based User interface tool and has an open API for .Net with J2EE coming available by June 2007. Finally it offers increased manageability capabilities through integration with the eB2Bcom Identity Management Suite .Net administrative User Agent.

* **eB2Bcom High Availability Identity Services** – an LDAPv3 and XML Database with full DISP replication providing ' High availability Services is very often a concern for businesses especially in organizations where 24x7x365 operation is required such as Airlines, Defence etc. As more mission critical applications become directory enabled, high availability directory services become an absolute necessity for the enterprise. eB2Bcom High Availability Services is a dual fully synchronized LDAPv3 & XML Database platform providing full replication. With eB2Bcom High Availability services system administrators can change directory schema, add new entries, add attributes back up the servers all without taking the system off line. Administrators can also manage through the .NET ADUA (administrative User Agent) multiple high availability Directory servers from the one management workstation. add or delete directory servers and populate them without any interruption of service. An In-built multi-version concurrency control manager allows queries to proceed without being locked out by updates, even in the presence of a very large update operation like the total refresh of a replicated sub tree and routine maintenance activities, such as taking backups of the database and check-pointing update logs can proceed without interruption to service. Such activities can proceed even with a heavy update load.

***eB2Bcom Identity Access** (provided by partner Boldon James – MasterKey & MasterKey.Net)

MasterKeyPlus is a plug-in to Microsoft Outlook providing users with a sophisticated LDAP Address Book for searching or browsing a corporate directory. Its sophistication means it is well suited to directories that are either very large or have a deep hierarchical structure. MasterKeyPlus is an advanced e-mail address book designed to integrate seamlessly with Microsoft Outlook and provide many features over and above those in the standard product. Especially applicable in large organisations with multiple address books and directories MasterKeyPlus is designed to improve the accuracy of address book searches by providing more detail on recipients and thus avoiding any costly addressing mix-ups. MasterKey Plus is infinitely configurable and can be customised to match the organisation and structure of clients' directories and the data they hold. Whereas MasterKey.net allows organisations to extend the standard Outlook Web Access (OWA) address book to enable searches of LDAP and X.500 directory servers as well as Microsoft Exchange GAL and the contacts folder Microsoft's Outlook Web Access (OWA) client does not include support for searching LDAP directory servers. The only address books available with the OWA client, out of the box, are the Global Address List (GAL) and Contacts folders. This lack of functionality is a major limitation to users whose organisations have deployed an LDAP or X.500 Directory infrastructure within their messaging system to host corporate information. LDAP access is a standard feature within the Outlook desktop client and the fact that the thin OWA client does not include support for LDAP limits deployment options. Those users who require LDAP access will be limited to the desktop Outlook client only. This can be a significant issue as the latest incarnation of the OWA client is a key reason most organisations are selecting to upgrade to Exchange 2003. The product also works with the Check names feature included with the OWA 2003 client. If the user selects Check Names, then any LDAP address present will be searched as well as the standard GAL and Contacts. By enabling LDAP support from Outlook Web Access MasterKey.net provides a major feature enhancement to the thin client. More Organisations can now enjoy the increased productivity gains and lower TCO of Microsoft's OWA client.

***eB2Bcom Data Synchronisation Services** (provided by partner MaXware - Data Synchronisation Engine) – provides an any to any data synchronisation and integration solution offering near real time and delta updates and many application templates. **The Data Synchronization Engine** synchronizes virtually any type of data to and from virtually any type of application. DSE's built in templates, customizable connectors and ability to auto-discover a repository's schema makes DSE a critical and flexible tool for an organization's Identity Management. DSE provides the mechanism for effortlessly reading, cleaning, joining, synchronizing, and writing identity data to and from disparate repositories. DSE's powerful Delta technology enables organizations to perform more efficient read/write operations and to deliver detailed audit trail reporting necessary for today's strict compliance. DSE's platform and technology independent architecture (both on Java or Windows) allows organizations to run DSE in the environment where it can be most effective. DSE adapts to an organization's process and procedures, fits within existing infrastructures and produces rapid return on investment. As well providing full support for eB2Bcom Internet Directory services, MaXware Data Synchronization Engine is certified for **Computer Associates** Identity and Security Solutions.

***eB2Bcom Virtual Directory** (provided by partner MaXware Virtual Directory) enables multiple LDAP directories or relational databases to look like a single, unified LDAP store; includes new audit and reporting features, and improved installation/configuration for use with a variety of Identity Management products, IBM Tivoli, and Microsoft Active Directory; Virtual Directory (MVD) acts as a single access point for various client applications. It provides real-time access to numerous disparate target systems without move data off those systems, offers fast, flexible and reliable service for authentication, authorization and provisioning and provides quick and non-intrusive configurations. MaXware virtual directory organizes any number of data sources into a directory tree effectively contains a directory tree without contents and directory nodes reference other data sources such as open databases, LDAP directories, proprietary data sources and value adding services. It also provides for data attribute filtering and conversions and schema/name space mapping. It can do Protocol Translation— Providing access to relational and other non-standardised data over standard LDAP and web services protocols without altering the data. It enables Web Service Enablement— responding to identity data requests made via DSML, SPML or any other service-orientated data format (standards-based or custom). It can offer Multi-Repository Search— Enabling a single search over standard protocols to return a single clean result-set containing identity data that resides in multiple repositories in multiple formats as well as providing Joined Identity View— Enabling a search that returns a view of single identities that are comprised of data from multiple repositories. Virtual Directory provides Permission-Based Results—Enable a customised view into a single data universe based on which application or which user is performing the search. As well as offering a Dynamic DIT— Building an on-the-fly directory information tree based on identity data attributes and full Authentication—Enable pass-through authentication from a single point of entry into multiple identity data stores. Finally it can provide Real-Time Data Access —Provide real-time access into back end systems. Because requests are passed to the originating data source, the search results can be as real time as required. As well providing full support for eB2Bcom Internet Directory services, MaXware Virtual Directory is certified for Computer Associates Identity and Security Solutions and RSA.

***eB2Bcom Identity Federation** (provided by partner MaXware – Federation Server) - a stand-alone, simple-to-deploy, fully functional federation server features enhanced support for SAML and WS-Federation but including the Virtual directory for auto provisioning... As more and more organizations depend on their users working across company boundaries, the need for federation of identities increases. Users expect to authenticate themselves only once, and expect to be able to run applications, without further authentications. The challenge for organizations is that the identity data often is stored in many different repositories in different formats. MaXware Federation Server (MFS) can join all this identity data into one common view which will simplify the task of defining federation between organizations. With failover and load- balancing features, the organization will have uninterrupted federation of identities with its business partners. MaXware Federation Server is the first federation product to integrate both virtual directory and federation technologies into a single core solution. The MaXware Federation Server opens up the world of dynamic, on-demand provisioning to partners by seamlessly automating the account creation process on the relying party side. This standards-based product enables companies to build interoperable services that ensure privacy and regulatory compliance. Combining identity data with Web Services is critical to the success of a Service Oriented Architecture (SOA). MaXware Federation Server allows enterprises to access their corporate identities through standards-based protocols like Security Assertion Mark-up Language (SAML) and Liberty Identity Web Services Framework (ID-WSF). The MaXware Federation Server builds on the technology of the well-proven MaXware Virtual Directory, with its advanced functionality for non-intrusive access to existing applications and repositories. This simplifies implementing a federation service, using the existing identity infrastructure, which may be stored in a multitude of disparate repositories. Leveraging Virtual Directory technology makes the federation server easier to integrate into existing environments by enabling a rich set of functionality like dynamic aggregation of attributes, account linking and on-demand provisioning. Using protocols like SAML for linking authentication and identities across multiple sites enriches end user experience by providing personalized user information. Companies can build interoperable services that are scalable to internet size while

at the same time ensure privacy and regulatory compliance. Federation is driven by real business needs for making collaboration between business partners easy and secure by enabling standards based interoperable Web Single Sign-On (Web SSO) and Web Services. Adding identity to Web Services is the key enabler of a successful Service Oriented Architecture (SOA).

***eB2Bcom Internet Directory Bastion** (provide by partner Clearswift – Directory Bastion). Directory Bastion is a specialised stand-alone product, which purpose is to allow Directory data to be synchronised between two Directory System Agents (DSAs) on two otherwise disjoint networks of different or the same classification, whilst maintaining an assured separation between the two networks it interconnects. The Directory Bastion ensures that the only communication that it allows to traverse between the two networks conforms to the Directory Information Shadowing Protocol (DISP, defined in ITU-T Rec. X.525) between explicitly identified DSAs. Because DISP is the standard protocol to synchronise directory data between DSAs, a Directory Bastion can be inserted between two DSAs without requiring anything other than normal shadowing agreement configuration on the DSAs. Apart from network level addressing, the Directory Bastion is entirely transparent to the DSAs. The Directory Bastion builds on the existing Bastion product, and the ITSEC E3/Common Criteria EAL4 evaluated component of Bastion is unchanged in Directory Bastion.

***eB2Bcom Identity Solutions Professional Services.** eB2Bcom has an unsurpassed track record at undertaking Identity Management projects within the Asia Pacific region. We have completed projects in Singapore, Malaysia, Hong Kong, China, Australia, New Zealand & Fiji. eB2Bcom Identity Solutions Professional Services consists of a team of very experienced solutions consultants based in Singapore, Melbourne, Canberra and Sydney. We undertake Business requirements specification, building business cases for identity management projects including return on investment strategies, business process workflow mapping and business process re-engineering, technical requirements analysis, Identity infrastructure and directory design, Access control policy development and Password Management policies as well as all Implementation and delivery services associated with our comprehensive product suite. The eB2Bcom Consulting team includes two authors of the IETF LDAPv3 standard and the co-author of the new IETF XLDAP and XMLeD standards. The eB2Bcom Identity Solutions Professional Services team also includes staff cleared to Defence Secret and expertise in undertaking work on classified projects for the Defence, Intelligence, and Police & Homeland Security markets. The eB2Bcom Identity Solutions Professional Services team also works very closely with the eB2Bcom IT Data security consulting team which undertake holistic reviews and projects for customers in a variety of sectors including Government, Defence, and Health & Education. eB2Bcom has a number of CISSP certified staff and an Australian Department of Defence certified I-RAP assessor on staff.

"...Now more than ever, customers are looking for a comprehensive identity management software platform and services that can be implemented via a single sale and supported by a single vendor," said Andrew Ferguson, Director, Identity & Access Management Solutions at eB2Bcom (Asia Pacific) Pte Ltd. "eB2Bcom Identity Management suite provides customers with an identity platform, that increases business agility and helps to reduce costs and to achieve regulatory compliance so that enterprises can get the most from existing and future IT investments. Also unlike other vendors eB2Bcom offers a simple easy to understand pricing model and real experience and track record at implementing comprehensive Identity Management solutions. With 12 years experience of Identity and Access Management projects, over many major Identity Management projects completed throughout the Asia Pacific region and unsurpassed knowledge and capability including two of the authors of the LDAP standards, eB2Bcom Identity Solutions delivers real Return on Investment for our customers and delivers a holistic approach to IT Security and Identity Management.."

About eB2Bcom

eB2Bcom is an innovative independent company specialising in the development, distribution, implementation, reselling and support of best-of-breed products for Identity Management, Directories Messaging, secure information sharing and security solutions for the Defence, Homeland Security, Health and Government sectors. The company was founded in 2004 and has a close working relationship with its sister organisation eB2Bcom of Australia which was established in 1996.

For more information, visit the eB2Bcom web site at www.eb2bcom.sg

- end -

For product or media enquiries please contact:

eB2Bcom

Lisa Vuu
Marketing Co-ordinator
Tel: +61-3-9896-7800
Email: lisa.vuu@eb2bcom.com
Web: www.eb2bcom.com