FACT SHEET - February 23, 2004

# IBM Plans First Identity Management Solution Using OATH

Concurrent with VeriSign's announcement of the Open Authentication Reference Architecture (OATH), IBM is announcing that it plans to make its Tivoli integrated identity management software interoperable with the VeriSign Intelligence and Control Services for Strong Authentication.

OATH is a standards-based approach to "strong authentication." This new way to bolster business security combines a user ID with a software or hardware 'token' in the form of a unique device that validates a user's identity, thereby granting access to a software application, network, or location. This can strengthen security and reduce the cost of implementing stepped up authentication for identity management, particularly for trusted networks between business partners. This new initiative is important because of its open, standards based approach -- giving customers more options, which won't lock them into a single form of strong authentication.

IBM plans to focus on simplifying and automating the process of integrating these new devices into existing identity management systems within a business. Identity management is already a huge benefit to businesses today, helping companies control who has access to business applications, operating systems and networks, as well as letting network administrators distribute, change or revoke "digital identities" for employees, partners and customers.

IBM Tivoli identity management software and VeriSign's new services can work together to provide second-level authentication through new VeriSign services based on this Open Authentication Reference Architecture. User information will stay in the enterprise, managed by IBM. Specifically:

-- IBM Tivoli Identity Manager will provision new user accounts that now include the needed strong authentication information
-- IBM Tivoli Access Manager will let security managers define who needs this stepped up level of authentication and communicate with VeriSign's new service
-- IBM Tivoli Directory Server will be the authoritative enterprise directory that Tivoli Access Manager uses for the first level of authentication

Here are a few examples of how our integration could work:

Scenario 1 (end-to-end identity management): HR teams often enter new employee information into their internal employee management systems. When corporate security policy dictates that a second form of authentication (beyond a password) be presented for access to Web applications from outside of the company network for certain critical applications such as early quarterly financial data, IBM Tivoli Identity Manager will automatically provision identities and access rights to the appropriate applications, operating systems and network infrastructure, and the user will automatically be enrolled for VeriSign strong credentials. When the employee tries to access critical applications within the employee portal, IBM Tivoli Access Manager will enforce strong authentication policy consistently, requiring users to present their USB token, their smart

card, etc., where appropriate. When the employee or contractor leaves the company, IBM Tivoli Identity Manager will automatically de-provision their identity and security credentials will be de-provisioned, thereby preventing unauthorized access to enterprise resources.

Scenario 2 (single sign-on): The strong authentication solution for enterprise access combines simplicity with security and mobility. For example, a user will be able to use a USB token or smart card then use single sign-on technology from IBM to gain access to applications. By integrating IBM Tivoli Access Manager with VeriSign validation services, user credentials from these devices will instantly become available to all enterprise systems that use IBM Tivoli Access Manager. Because this approach does not require any change to the application, the traditional integration cost for deploying strong authentication solutions can decrease. For example, an end user will be able to login into the enterprise portal using a one-time password generated by a VeriSign token. IBM Tivoli Access Manager will forward the validation request to VeriSign validation services. After the two-factor authentication process is complete and successful, IBM Tivoli Access Manager will grant the user access to the portal. Using single sign-on technology, IBM Tivoli Access Manager will then carry the strong authentication event across many other applications without burdening the user to remember or present a new credential.

Media interested in more information about this new interoperability, contact:

Cas Purdy
IBM Media Relations
512-286-3208
cpurdy@us.ibm.com