RFP CHECKLIST: ID MANAGEMENT

THE GENERAL SERVICES ADMINISTRATION has listed identity management systems as a core component of an HSPD-I2-compliant PIV II architecture. Although IDMS solutions have yet to undergo compliance testing for use in PIV II systems, agencies are expected to have several approved solutions to choose from. Here are some questions you should ask.

- ❏ What **server operating systems** does the identity management system support? What database and/or e-mail servers are supported?
- ❏ What operating systems do the **management consoles** require? Can they be Web-based?
- ❏ Does the solution integrate with the Lightweight Directory Access Protocol, Microsoft Active Directory, Novell eDirectory or other **common directory** protocols?
- ❏ Does the IDMS allow you to set policies for password difficulty and expiration? Can you specify minimum character ranges for passwords?
- ❏ Will it support **central caching of keys**? Can it require different authentication criteria based on different trust levels?
- ❏ Can the solution be expanded to include **new forms of identity verification** and assertion, should they arise?
- ❏ ... sion and storage? What forms of encryption does the software support?
- ❏ Is there a **self-provisioning** module? Does it allow for automated retrieval of lost passwords?
- ❏ Does the IDMS provide different degrees of **vetting for ID authentication**, based on security clearance? Does it easily integrate with tokens, smart cards or other types of physical or biometric authentication?
- ❏ Will it support **central caching of keys**? Can it require different authentication criteria based on different trust levels?
- ❏ Does the system **log failed log-ins** and allow you to lock out users after a specified number of failures?
- ❏ Does the solution support **password encryption**? Are passwords encrypted during both transmis-
- ❏ Will the solution **require users to periodically recertify** their identities? Will it automatically propagate authorized changes across all system resources?
- ❏ Can it **automatically locate and retire orphan accounts** that are no longer in active use?
- ❏ How granular is the **provisioning module**? How many roles does it allow you to create? How customizable are the rules for each role?
- ❏ Does the suite provide **pre-built interfaces into core enterprise applications**? Does it provide tools for customizing pre-built interfaces or building new ones from scratch? Can the vendor provide such services?
- ❏ What kind of **audit trail and report-**
- **ing capabilities** does the solution provide? Are the audit trails stored in a separate encrypted database?
- ❏ Can users create **custom audit reports**? Does the software support third-party audit tools?
- ❏ Does the solution allow for **secure, offsite backup and restoration** of identity data stores?
- ❏ Does the vendor have a **federated solution**? If so, is it compatible with the Liberty Alliance, WS-*, or SAML standards?
- ❏ What kind of **service level agreements** does the vendor provide? Does it offer 24/7 support or guaranteed minimum response times if its products fail?

—Dan Tynan

IDENTITY MANAGEMENT SYSTEMS

VENDOR	PRODUCT(S)	NOTES
CA Inc. Islandia, N.Y. (800) 225-5224 www.ca.com	eTrust Identity and Access Management Suite	This suite of five products offers soup-to-nuts protection across several flavors of Unix, Linux and Windows.
Courion Corp. Framingham, Mass. (866) 268-7466 www.courion.com	Enterprise Provisioning Suite	IDM specialists offer a full suite of password, provisioning and access modules; works with any directory, e-mail server or SQL relational database but may require a fair amount of programming expertise.
Hewlett-Packard Co. Palo Alto, Calif. (650) 857-I50I www.hp.com	HP OpenView Identity Management	HP offers sophisticated IDM tools as part of its OpenView management platform, adding to its suite of federation products with the acquisition of Trustgenix last November.
IBM Corp. Armonk, N.Y. (800) 426-4968 www.ibm.com	Tivoli Identity Manager, Tivoli Access Manager	Full suite of identity, directory, access and federation products works with directories based on Microsoft Active Directory, Sun ONE and its own LDAP-based Tivoli Directory Server.
MaXware AS Trondheim, Norway (732) 409-5000 www.maxware.com	MaXware Identity Center	This vendor boasts 280 clients in 30 countries, with strong ties to military and governmental agencies.
Microsoft Corp. Redmond, Wash. (425) 882-8080 www.microsoft.com	Microsoft Identity Integration Server 2003, Enterprise Edition	MIIS 2003 works with a number of non-Microsoft directories (including LDAP, Novell eDirectory, IBM and Sun/iPlanet) and e-mail servers, provided they run on a Windows platform.
Novell Inc. Waltham, Mass. (800) 529-3400 www.novell.com	Novell Identity Manager 2	Built around its widely used eDirectory structure, Novell's suite supports a wide range of operating systems and offers some good (though optional) tools for designing identity management schemes and running what-if scenarios.
Oracle Corp. Redwood Shores, Calif. (650) 506-7000 www.oracle.com	Oracle Identity Management	Recent acquisitions of top-tier IDM vendor Thor Technologies and OctetString strengthen Oracle's offerings, which include a full range of application-centric middleware products.
Sun Microsystems Inc. Santa Clara, Calif. (800) 232-467I www.sun.com	Java System Identity Manager	One of the oldest players in IDM software offers a full suite of access, auditing and federation products across diverse operating systems (AIX, HP OpenVMS, Solaris, Windows) using a Web-based management console.
Symark Software Inc. Agoura Hills, Calif. (800) 234-9072 www.symark.com	PowerBroker, PowerPassword User Management Edition, PowerKeeper	Longtime Unix/Linux enterprise software vendor added support for Windows last year with its PowerKeeper identity management appliance.