zapthink
zapnote

Doc. ID: ZTZN-0610-1D
Released: July 19, 2002

ZapThink ZapNote™

RSA Security
Application Security Tools Leader

Briefing Date: May 31, 2002

Analyst: Jason Bloomberg

Abstract

RSA Security has been in the encryption business since day one, and they have since successfully leveraged their early leadership to offer a range of security products and technologies in the application security space. RSA offers encryption components that form the basis of many of the evolving XML security efforts on the market today, such as XML Digital Signature, and their pioneering work with the Security Assertions Markup Language (SAML) has affirmed their position as a leader in the identity management product space.

Trailblazer for Application Security Tools

RSA Security helps its customers build secure, trusted foundations for eBusiness through its two-factor authentication (schemes that involve physical tokens like smart cards or biometrics), access management, encryption and digital signature solutions. RSA provides security software and hardware that enterprises use to protect and manage network access. Companies use RSA's SecurID product line (which includes smart cards, tokens, and software) to manage and monitor user access to enterprise applications and associated data. The company also offers digital certificate management applications, as well as software development tools for creating encryption components.

RSA's experience with encryption dates back to 1976, when MIT researchers Ronald Rivest, Adi Shamri, and Len Adelman (whose initials formed the RSA name) developed a breakthrough in encryption in a multi-user environment. Expanding on earlier work on public key encryption by cryptography pioneers Whitfield Diffie and Martin Hellman at Stanford, Rivest, Shamri and Adelman developed an encryption technique (now called the *RSA algorithm*) that did not require any active participation between the person encrypting the data and the person decrypting it at the other end. Such encrypted communications rely on each party having a public key and a secret, private key. By obtaining a person's public key, the two parties are able to independently agree upon a formula that lets them exchange encrypted information.

RSA has since built their company on the RSA algorithm, developing components and associated tools that software developers can use to build public key encryption technology into their products.

RSA's encryption components contribute to implementations of XML Digital Signatures and the XML Key Management Specification (XKMS), RSA's primary contribution to the XML and Web Services space, however, is its identity management strategy, which is based on the SAML specification (see the sidebar for more information about SAML). As part of its identity management strategy, RSA is providing solutions to help enterprises manage the full lifecycle of a digital identity in a secure fashion, including the creation of the digital identity, its maintenance, and finally its termination. RSA's identity management approach also enforces enterprise policies regarding access to electronic resources. In addition to storing and provisioning digital identities, RSA's trusted identity and access management solutions offer authentication, access management, issuance and management of credentials, and encryption capabilities as well.

SAML (the Security Assertion Markup Language) is a standard for exchanging authentication and authorization information between systems or domains, and is currently a version 1.0 specification of the Organization for the Advancement of Structured Information Standards (OASIS) standards body.

The SAML specification provides three types of assertions:

- Authentication assertions (facts about users and their identities)
- Attribute assertions (information about the user such as credit limits)
- Authorization decision assertions (whether the user is authorized for a particular activity, such as purchasing)

SAML concerns itself only with authentication and authorization. Its main goal is to provide a standard procedure for enabling single sign-on across organizational boundaries using Web Services. The SAML protocol describes how systems request and retrieve assertions. The SAML protocol then defines the request and response messages and the simple choreography for using them.

Focus on Application Security

RSA Security's products focus on the following four core areas:

- *Authentication* — RSA SecurID systems offer two-factor user authentication. They use physical tokens such as smart cards in addition to passwords to provide robust user authentication.

- *Web Access Management* — ClearTrust Web access management software is a single sign-on solution that enables secure access to Web-based resources within intranets, extranets, portals and exchange infrastructures.

- *Encryption* — BSAFE software provides implementations of a variety of security standards such as SSL and other PKI standards for vendors to integrate into their own products, in the form of software components and associated tools.

- *Digital Signatures* — The Keon product line is a family of interoperable software modules for managing digital certificates and creating an environment for authenticated, private and legally binding electronic communications and transactions.

The ZapThink Take

RSA was the creator of some of the key cryptographic protocols that gave birth to modern application level security, and they continue be thought leaders in the industry. Their primary contributions to XML and Web Services security include providing the development toolkits that enable other companies to build PKI-based solutions, including those built upon XKMS. In addition, RSA has provided great leadership with the SAML specification and the associated Liberty Alliance federated single sign-on specification.

The Liberty Alliance Project is an alliance of more than sixty technology and consumer organizations, including American Express, General Motors, United Airlines, Sun Microsystems, as well as RSA Security. The Liberty Alliance formed to develop and deploy federated identity specifications that support a wide range of network-aware devices. Liberty has largely based their specification upon SAML, and RSA is one of the first vendors to announce that they are building a product that supports the Liberty specification. RSA's prominent positions within the overlapping SAML and Liberty Alliance communities places them at the leading edge of the identity management market segment. As a result of RSA's continued leadership in the security space, coupled with their long history of leadership in the cryptography and broader application security markets, ZapThink believes that RSA Security will continue to drive the development of solutions to enterprise's security needs.

Profile: RSA Security (July 2002)

Date Founded: 1982
Funding: Nasdaq: RSAS
President, CEO, and Director: Arthur W. Coviello Jr.,
Employees: 1218 (in 2001)
Products:

- *RSA SecurID* software is a solution for two-factor authentication that helps to protect enterprise network resources by ensuring that only authorized users are granted access to email, Web servers, intranets, extranets, network operating systems and other resources.
- The *RSA ClearTrust* Web access management solution manages user access privileges to Web-based resources, including Web Services. RSA plans to incorporate SAML functionality into the ClearTrust software to enable Web single sign-on, as well as to allow multiple organizations and servers to share authentication and identity information.
- *RSA BSAFE* encryption software allows developers to implement a variety of security standards, including XML signing as well as encryption tools for the SOAP protocol.
- *RSA Keon* digital certificate management software creates an environment for authenticated electronic transactions and other communications.

Address:
174 Middlesex Turnpike,
Bedford, MA 01730
URL: http://www.rsasecurity.com

Main Phone: 800-SECURID
Contacts: sales@rsasecurity.com

Related Research

- *XML and Web Services Security* Report (ZTR-WS104)
- *Web Services Technologies and Trends* Report (ZT-WEBSRV)
- *Phaos Technology* ZapNote (ZTZN-0603)
- *Quadrasis* ZapNote (ZTZN-0304)
- *Vordel* ZapNote (ZTZN-0238)
- *Westbridge Technology* ZapNote (ZTZN-0612)

About ZapThink, LLC

ZapThink is an IT market intelligence firm that provides trusted advice and critical insight into XML, Web Services, and Service Orientation. We provide our target audience of IT vendors, service providers and end-users a clear roadmap for standards-based, loosely coupled distributed computing – a vision of IT meeting the needs of the agile business.

ZapThink's role is to help companies understand these IT products and services in the context of SOAs and the vision of Service Orientation. ZapThink provides market intelligence to IT vendors who offer XML and Web Services-based products to help them understand their competitive landscape and how to communicate their value proposition to their customers within the context of Service Orientation, and lay out their product roadmaps for the coming wave of Service Orientation. ZapThink also provides implementation intelligence to IT users who are seeking guidance and clarity into how to assemble the available products and services into a coherent roadmap to Service Orientation. Finally, ZapThink provides demand intelligence to IT vendors and service providers who must understand the needs of IT users as they follow the roadmap to Service Orientation.

ZapThink's senior analysts are widely regarded as the "go to analysts" for XML, Web Services, and SOAs by vendors, end-users, and the press. They are in great demand as speakers, and have presented at conferences and industry events around the world. They are among the most quoted industry analysts in the IT industry.

ZapThink was founded in October 2000 and is headquartered in Waltham, Massachusetts. Its customers include Global 1000 firms, public sector organizations around the world, and many emerging businesses. ZapThink Analysts have years of experience in IT as well as research and analysis. Its analysts have previously been with such firms as IDC and ChannelWave, and have sat on the working group committees for standards bodies such as RosettaNet, UDDI, CPExchange, ebXML, EIDX, and CompTIA.

Call, email, or visit the ZapThink Web site to learn more about how ZapThink can help you to better understand how XML and Web Services impact your business or organization.

ZAPTHINK CONTACT:
ZapThink, LLC
11 Willow Street
Suite 200
Waltham, MA 02453
Phone: +1 (781) 207 0203
Fax: +1 (786) 524 3186
info@zapthink.com