TriStrata Integrates PKI Authentication

By Dorothy E. Denning
Georgetown University
December 13, 2000

TriStrata has extended its Management System for Information Security to support multi-vendor, open X.509v3 public key certificates for user enrollment, authentication and digital signature applications. This new capability allows companies to leverage their investment in PKI while gaining the advantages inherent in TriStrata's security backbone for protecting information, controlling access to encrypted data, managing roles and authorizations, plus real-time auditing.

Enterprises and their employees using public key certificates will now be able to enroll in a TriStrata system simply by presenting their valid certificates and selecting their unique Personal Pass Phrase (PPP). Information in the certificate will be used to establish and confirm the user's identity, thereby expediting the overall TriStrata enrollment process. Once all enrollment procedures are satisfactorily completed, customers can then use either their private key associated with their certificate or their PPP to authenticate into the TriStrata universe of secured applications. In addition, certificate users will be able to use their private key to add their digital signature to documents and encrypted email messages. Document protection, integrity, assurance and accountability via audit are still handled with existing TriStrata methods.

TriStrata has effectively "opened" its system enrollment process to accept public key certificates from a number of leading PKI vendors.

THE TRISTRATA AND PKI BENEFITS

The use of public key certificates in an "open authentication" enrollment process to access TriStrata's security protection suite is not a new concept, but one that may now be successfully exploited by those enterprises undertaking various PKI initiatives. This development enables the strengths of both security approaches to be successfully realized.

It is generally accepted that while PKI solutions do in fact provide for strong authentication and digital signatures, PKI deployments in and of themselves generally do not offer a complete solution for the managed control and access to a business's most important intellectual assets. Many still consider PKI ill equipped to the task of providing all the necessary confidentiality and non-repudiation elements required in secure business-to-business transactions and collaborative communications. Very real problems with scalability, usability, user revocation and data recovery continue to thwart PKI-based business implementations, areas in which the TriStrata solution has been proven highly effective.

By combining the strengths and simplicity of TriStrata's centrally-managed data protection solution with the strongest attributes of public key certificates - namely PKI's capabilities for user authentication and digital signatures - users may now integrate the two and realize the benefits of TriStrata's comprehensive security solution in virtually all phases of their business.

HOW CERTIFICATE-BASED AUTHENTICATION WORKS

All enrolled clients of a TriStrata network must use a 256 KB private Access Signature in order to communicate with the TriStrata Extended Enterprise Security Server (TESS). This TriStrata Access Signature is used in the Private Access Line (PAL) protocol and serves to authenticate the client to the TESS. It is stored on the client machine, Triple-DES encrypted, under a hash of the user's Personal Pass Phrase. TriStrata has traditionally handled user authentication through this PPP, which then provides access to the TriStrata Access Signature.

To support certificate-based authentication, the TriStrata system encrypts the hash of the Pass Phrase with a randomly generated, cryptographically strong symmetric key. It then encrypts this key with the public key in the user's certificate. These values are stored in the PKI Authentication Token (PKIAT) for the user. When the user requests authentication with TESS via the certificate, the user's private key is used to decrypt the symmetric key, which in turn is used to decrypt the hash. Finally, the hash is used to decrypt the Access Signature.

During enrollment, the TriStrata Mass-Enrollment System checks that the certificate has not expired or been revoked. Certificate revocation information is obtained from an LDAP directory or an OCSP service as appropriate. The system assumes that a separate process keeps the revocation information up-to-date.

Although the user does not need to supply the TriStrata PPP during certificate-based authentication, the user will have to provide a PIN or password to gain access to the private keys used with the public key certificate. Thus, authentication still requires knowledge of a personal secret, albeit one that may offer slightly less security as a TriStrata PPP,

which must be at least 14 characters in length. However, if the user's private key is stored on an external device such as a smart card or even floppy disk that is protected, this helps compensate for a low security PIN. Ideally an external smart card reader with its own 'pin-pad' would be used in conjunction with the smart card and PKIAT, ensuring that the PIN is never exposed. Spyrus and Wave Systems provide readers that fit this model.

TriStrata's open PKI authentication works across Windows 95, 98, NT, and 2000 platforms. Certificate validation and cryptographic operations are handled through the Microsoft Cryptographic API (CAPI) using the Enhanced Cryptographic Service Provider modules. An Enhanced Provider CSP is needed to generate the cryptographically strong symmetric keys.

The two-level encryption of the hash in the PKIAT serves to accommodate deficiencies in pre-Windows 2000 versions of CAPI, which do not support direct decryption of a hash value with the user's private key. The PKIAT also includes a cryptographic checksum to defend against tampering attacks. This checksum is validated before the hash of the PPP is decrypted.

The TriStrata system can handle any X.509v3 certificate from a trusted Certificate Authority, including certificates from Verisign, Entrust, Xcert, and others. The initial release supports certificates that are stored on floppy disk, hard disk, or in an LDAP directory. It handles both IE 4 and Netscape 4 and above certificate stores. A future release update will support several smart cards, including Schlumberger Cryptoflex, Spyrus Rosetta, Spyrus Lynks and RSA SecureID 3100.

CONCLUSION

TriStrata has effectively "opened" its system enrollment process to accept public key certificates from a number of leading PKI vendors. This new adaptation allows for rapid user enrollment and authentication into a TriStrata security system, in addition to providing the digital signature capabilities inherent in the PKI architecture.

Enterprise PKI users can immediately benefit from TriStrata's total security system capabilities, including controlled access to information and communication methods as approved by senior management. With TriStrata in place, an organization can now establish desired access policies across diverse organizations, departments, and groups. Beyond open authentication, one-to-many secure messaging, dynamic group encrypted file sharing and immediate user revocation are just some of the many advantages TriStrata brings to bear on the problem of creating and maintaining a secure business environment.

DR. DOROTHY E. DENNING

Dorothy E. Denning is professor of Computer Science at Georgetown University. She is also professor and member of the advisory board of the Communication, Culture and Technology program and a faculty mentor in the Science and Technology in International Affairs program. Her current work encompasses the areas of information warfare and assurance, encryption policy and technology, and the impact of technology on law enforcement and society.

Before coming to Georgetown in 1991, Dr. Denning was a member of the research staff at Digital Equipment Corporation, a senior staff scientist at SRI International, and an associate professor at Purdue University. She has served as president of the International Association for Cryptologic Research, chair of the International Cryptography Institute, chair of the National Research Council Forum on Rights and Responsibilities of Participants in Networked Communities, co-chair of the ACM Conference on Computer and Communications Security, member of the National Institute of Standards and Technology Review Panel on Information Technology, member of the ACM cryptography policy study group, and member of the board of directors of the Computing Research Association. She is presently a member of the President's Export Council Subcommittee on Encryption Policy and co-chair of Georgetown's Technology Oversight Committee.

Dr. Denning is author of Information Warfare and Security (Addison Wesley, 1999), Cryptography and Data Security (Addison Wesley, 1982) and over 100 articles. She is co-editor of Internet Besieged: Countering Cyberspace Scofflaws (Addison Wesley, 1998). She has testified before the U.S. Senate and House of Representatives, is a frequent lecturer at conferences and symposia, and has appeared on TV and radio programs throughout the world. She is an ACM Fellow and has received the National Computer Systems Security Award and the Distinguished Lecturer in Computer Security Award.

In April 2000, she was named the TechnoSecurity Professional of the Year. Denning received the B.A. and M.A. degrees in mathematics from the University of Michigan and the Ph.D. degree in computer science from Purdue University.