



# Entrust Authority™ Security Manager Comprehensive

## Course Overview ...

The Entrust Authority Security Manager Comprehensive is an in-depth, five-day, hands-on course of the Entrust Authority Security Manager. The course begins with a discussion about the encryption and digital signature processes, trust models, and digital certificates. What produces a digital certificate, what are its contents, and why do we trust it? This segues into a discussion about the functions of the Certification Authority and the other components that comprise the PKI architecture. There are lessons devoted to each of these four main components: Security Manager (CA), Security Manager Administration (RA), the Directory, and Entrust Entelligence Security Provider (client). Students install and configure each of these applications, save the Directory. Students learn how to manage certificates and user accounts, customize groups, policy, roles, and user templates, and add new database fields, certificate extensions, and certificate types to the Security Manager. Lastly, students learn how to implement a roaming user solution, cross-certify with other CAs in a network or hierarchy environment, and recover the Security Manager's data after a disaster (DR). For all of these topics there are hands-on lab exercises led by a certified instructor.

## Course Objectives...

Upon completion of this course, participants will be able to:

- Describe some of the standards that relate to PKI, a high-level understanding of cryptographic processes, and the basic architecture of an Entrust infrastructure, including the functions of the various applications and processes.
- Perform both the day-to-day and the more advanced tasks related to management of the Security Manager and Entrust users.
- Customize groups, policy, roles, user templates, and add database fields and certificate types to the Security Manager.

## **Prerequisites...**

- Experience using Windows
- Prior knowledge of PKI concepts is helpful but not mandatory

## **Who should attend...?**

This comprehensive hands-on five-day course is intended for technology professionals who will be planning, implementing and managing the Entrust Authority Security Manager.

## Course Topics...

1. Security Concepts
2. Digital Certificates
3. Entrust Certification Authority
4. Entrust PKI
5. The Directory
6. Install Entrust Authority Security Manager
7. Entrust Authority Security Manager Control Command Shell
8. Create administrative users
9. Entrust Entelligence Security Provider
10. User lifecycle management

11. User operations from Entrust Authority Administration Services
12. Key management
13. Revocation lists
14. Audit logs and user reporting
15. Groups and searchbases
16. General security policy
17. Client policy
18. Certificate definition policies
19. Roles and permissions
20. Customization
21. Bulk operations
22. Entrust Authority Roaming Server

23. Cross-certification
  24. Regrouping exercise
  25. Hierarchical cross-certification
  26. Disaster recovery
- Appendix A. ePassport Public Key Infrastructure
- Appendix B. Entrust Authority Security Manager Proxy
- Appendix C. Build an Entrust Entelligence Security Provider installation package

© 2011, Entrust. All rights reserved.

Entrust is a trademark or a registered trademark of Entrust, Inc. in certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances may warrant.

Export restrictions apply to all cryptographic products and export/import licenses may be required.

The information contained in this document may not be duplicated in whole or in part without the prior written approval of Entrust.