



Entrust Presentation

**RSA Conference
January 1997**

Ian Curry
Entrust Product Manager
icurry@entrust.com

<http://www.entrust.com>



Copyright Entrust Technologies Limited, 1997



Agenda

- Introduction
- Key lifecycle management
- Entrust product family
- Summary



Introduction

- Entrust Technologies
 - subsidiary of Northern Telecom
 - formerly “Nortel Secure Networks”
 - introduced Entrust product family in 1994
 - active participant in security standards bodies
- Focused on public-key infrastructure products and technologies
 - an unbiased vendor in the software industry





Goals

- Provide a comprehensive security infrastructure
 - provide scalable security
 - enable business process re-engineering
 - minimize administrative costs & risk
 - allow application developers to quickly add best-in-class security to their applications
- Allow organizations to establish and maintain trust in networking transactions ... without burdening end users
 - transparency for end users is critical

Entrust
TECHNOLOGIES



What is Entrust?

- Family of software-based security products
- Works across applications and platforms
- Based on open standards
- Provides scalable, automatic, and transparent key lifecycle management

Orchestrating Enterprise Security

Entrust
TECHNOLOGIES

Copyright Entrust Technologies Limited, 1997



What is Key Management?

- “... the most difficult security problem.”

BSAFE Programmer's Guide, p. 60

- Issues

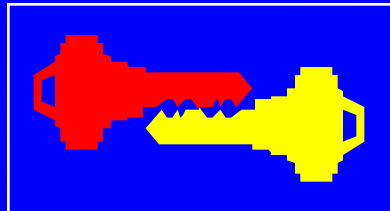
- generating keys
- keeping backup keys
- dealing with compromised keys
- changing keys
- destroying old keys
- ...

Entrust
TECHNOLOGIES

Copyright Entrust Technologies Limited, 1997



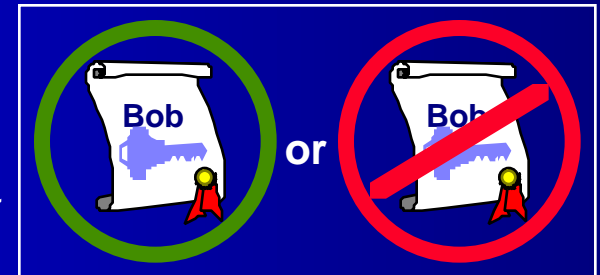
Key Lifecycle Management



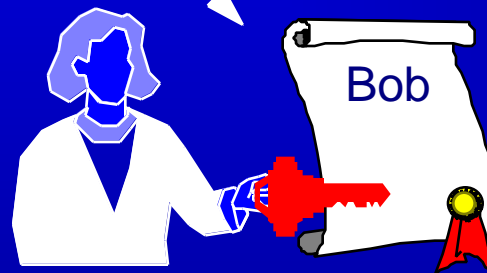
Key Generation



Certificate Issuance



Certificate Validation



Key Usage

Alice

Bob

Key Expiry



Key Update

Entrust
TECHNOLOGIES

Copyright Entrust Technologies Limited, 1997



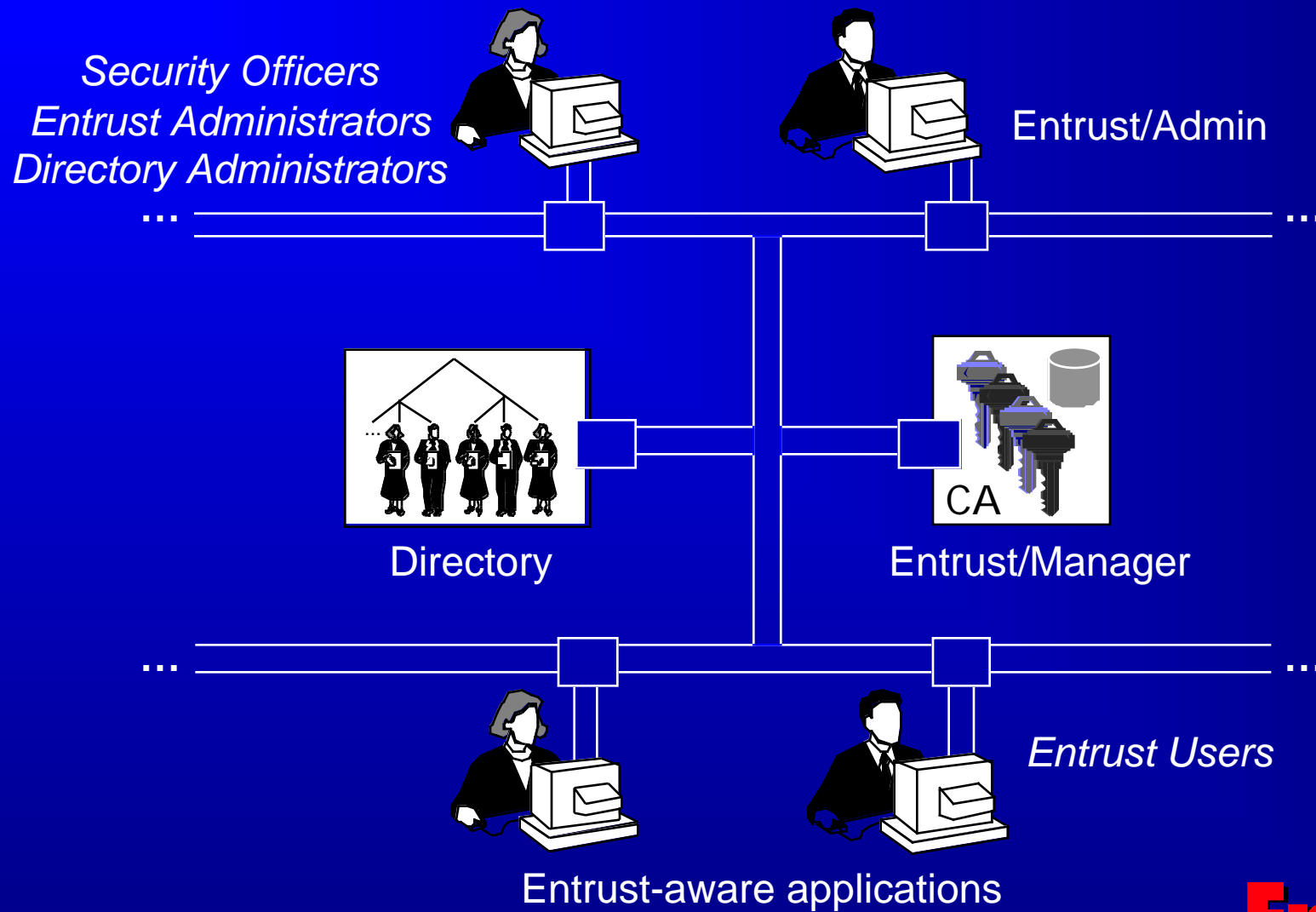
Entrust Product Family

- Entrust
 - scalable public-key infrastructure
- Entrust/Lite
 - for workgroups
- Entrust/Toolkit
 - family of standards-based application programming interfaces
- Entrust/WebCA
 - Certification Authority for Web applications
- Entrust/ICE
 - Windows 95 and NT desktop security





Entrust Architecture



Entrust
TECHNOLOGIES

Copyright Entrust Technologies Limited, 1997



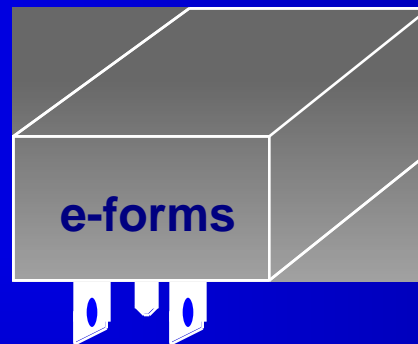
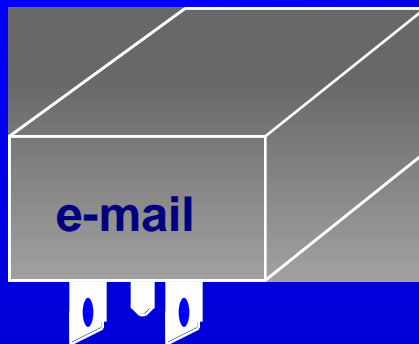
Entrust/Toolkit

- Family of security application programming interfaces
- Store-and-forward interfaces
 - EntrustFile Toolkit
 - EntrustIDUP Toolkit for S/MIME
 - ◆ implements IDUP-GSS-API with S/MIME
- Real-time interfaces
 - EntrustSession Toolkit
 - ◆ implements GSS-API with SPKM
- Certificate management services
 - EntrustCMS Toolkit

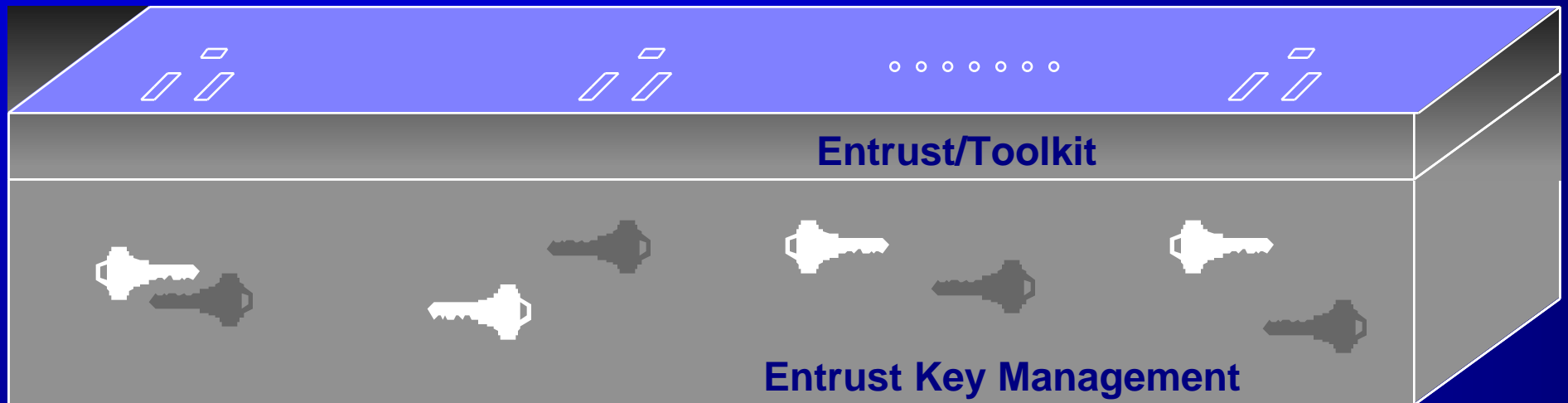
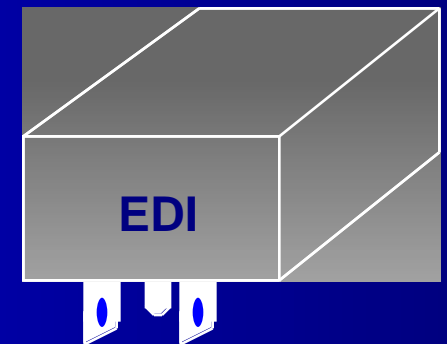
Entrust
TECHNOLOGIES



Security Across Applications



.....

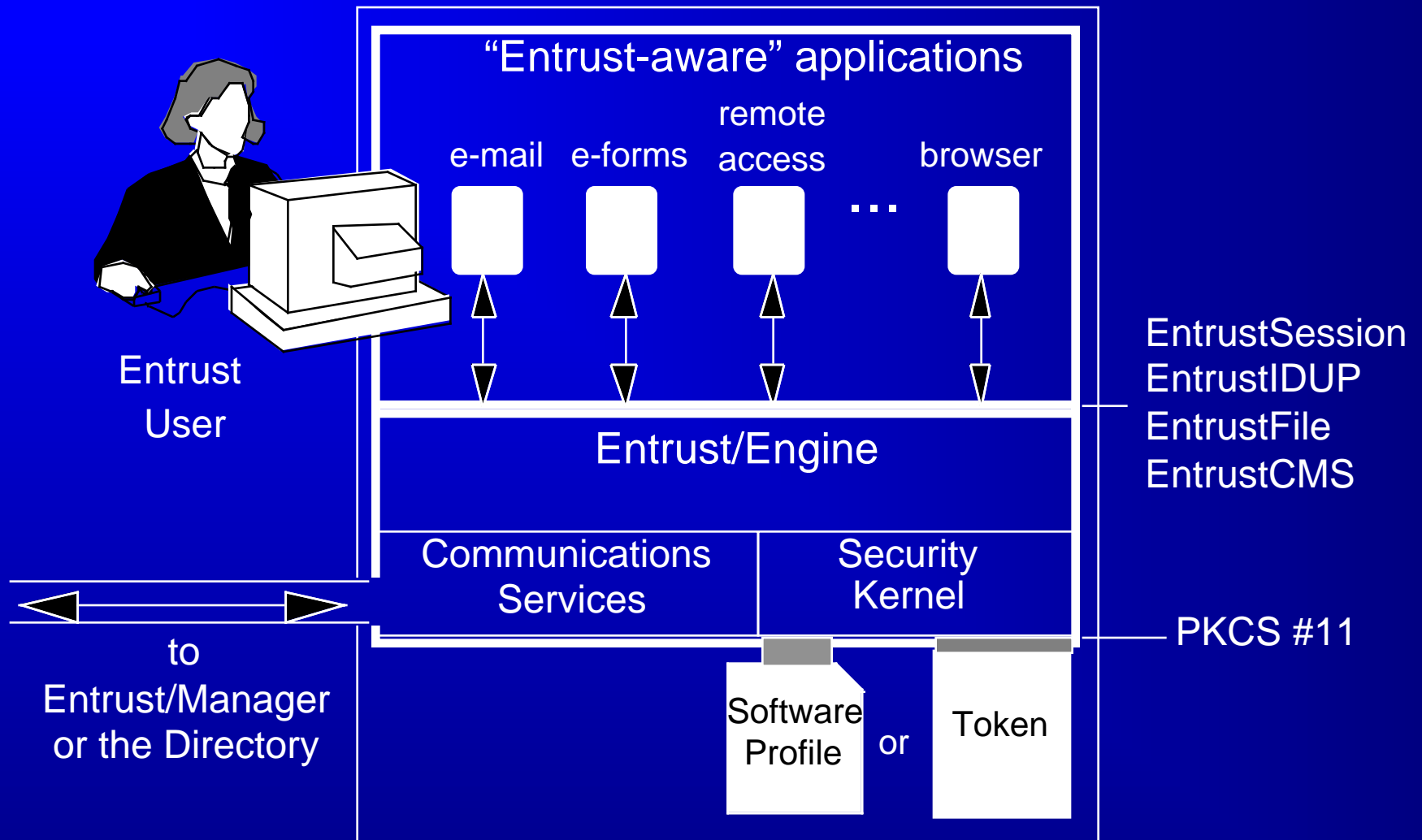


Entrust
TECHNOLOGIES

Copyright Entrust Technologies Limited, 1997



Client-side Architecture



Entrust
TECHNOLOGIES



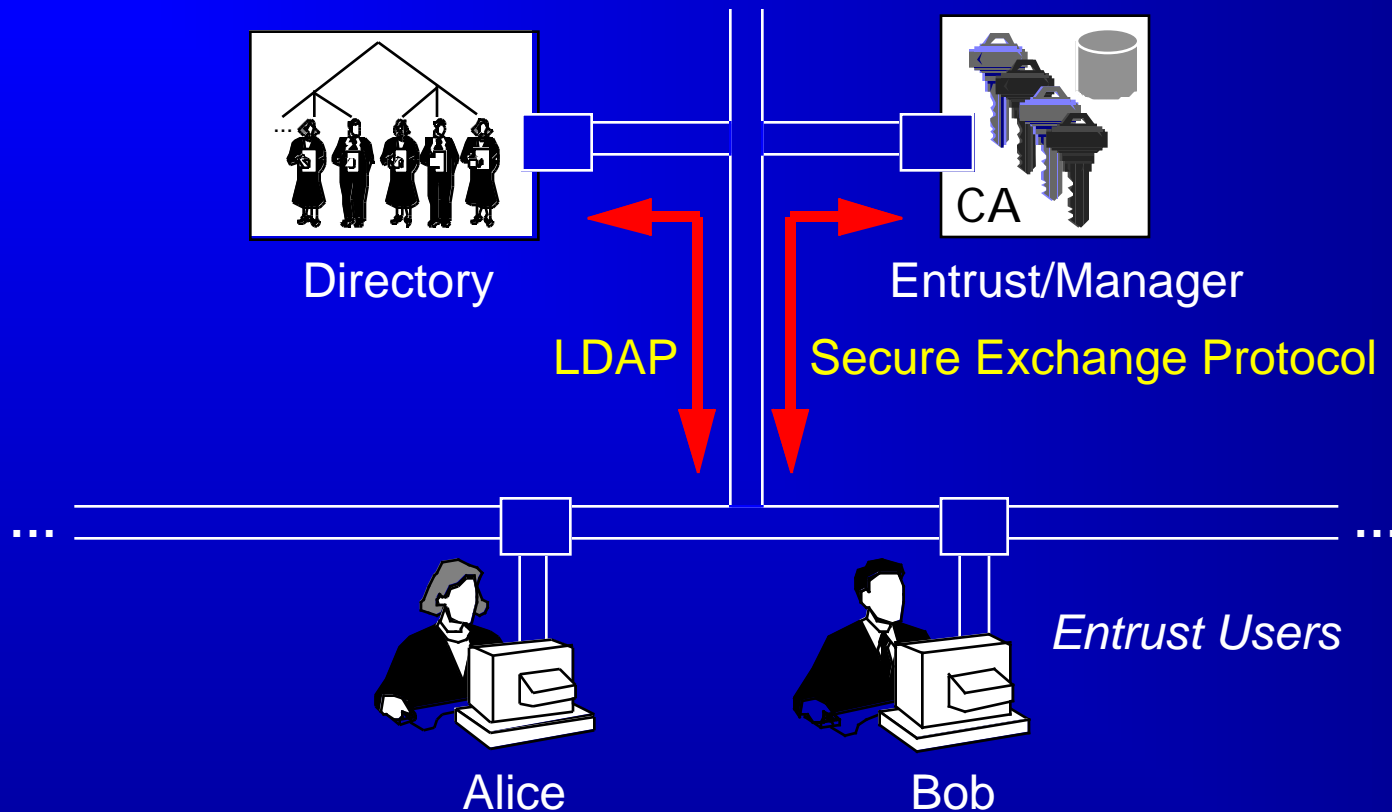
Entrust Security Kernel

- First software validated to FIPS 140-1
 - required for use in US and Canadian Federal Governments
- Algorithm independent
 - public-key: RSA, DSA, Diffie-Hellman
 - ◆ 1024-bit key pairs for encryption and digital signature
 - symmetric: CAST (128, 80, 64, 40), DES, Triple-DES (3-key), RC2 (128, 40)
 - ◆ CAST is now publicly available, royalty-free
 - hashing: SHA-1, MD5

Entrust
TECHNOLOGIES



Entrust in Action



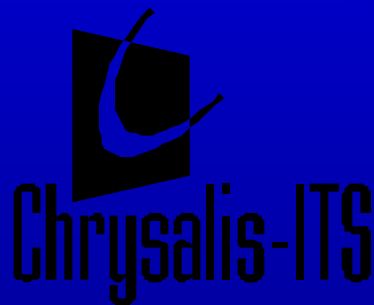
This is an animated slide

Entrust
TECHNOLOGIES

Copyright Entrust Technologies Limited, 1997



Entrust-aware Application Vendors



... and many more!





Entrust OEM and Channel Partners

- IBM
- Tandem
- Control Data Systems
- Hewlett-Packard
- Microsoft
- SAIC
- Choreo
- Bell SYGMA
- + others...

Entrust
TECHNOLOGIES



Entrust/WebCA

- Provides Certification Authority software for Web browsers and servers
- Uses browser-based administration
- Provides flexible administration models
- Includes an LDAP-compliant Directory

Entrust
TECHNOLOGIES

Copyright Entrust Technologies Limited, 1997



Entrust/ICE

- Integrated security for Windows NT and Windows 95
 - Entrust-aware application
 - fully-integrated into Windows Explorer
- Automatic encryption of files in folders
 - multiple modes of operation
 - flexibility to meet the needs of any user
- Secure deletion of files

Entrust
TECHNOLOGIES

Copyright Entrust Technologies Limited, 1997



Summary

- Entrust is a family of scalable, public-key infrastructure security products
 - provides key lifecycle management across applications and platforms
 - allows application developers to quickly add security to their applications
 - minimizes administrative costs & risk
- Allows organizations to establish and maintain trust in networking transactions ... without burdening end users

Entrust
TECHNOLOGIES



For More Information

Entrust Technologies
representatives are available to
answer your questions about
Entrust.

Visit the Entrust Web site at

<http://www.entrust.com>

