TriStrata

Open Group
26 January 1999

Don Adams

Agenda

- **Company Background**

- **System Overview**

- **System Demonstration**

- **Next Steps ?**

TriStrata's Purpose

Develop and deliver innovative solutions to protect and manage information assets, allowing enterprises to confidently use the full potential of the Internet

- **Expand global reach**
- **Reduce costs**
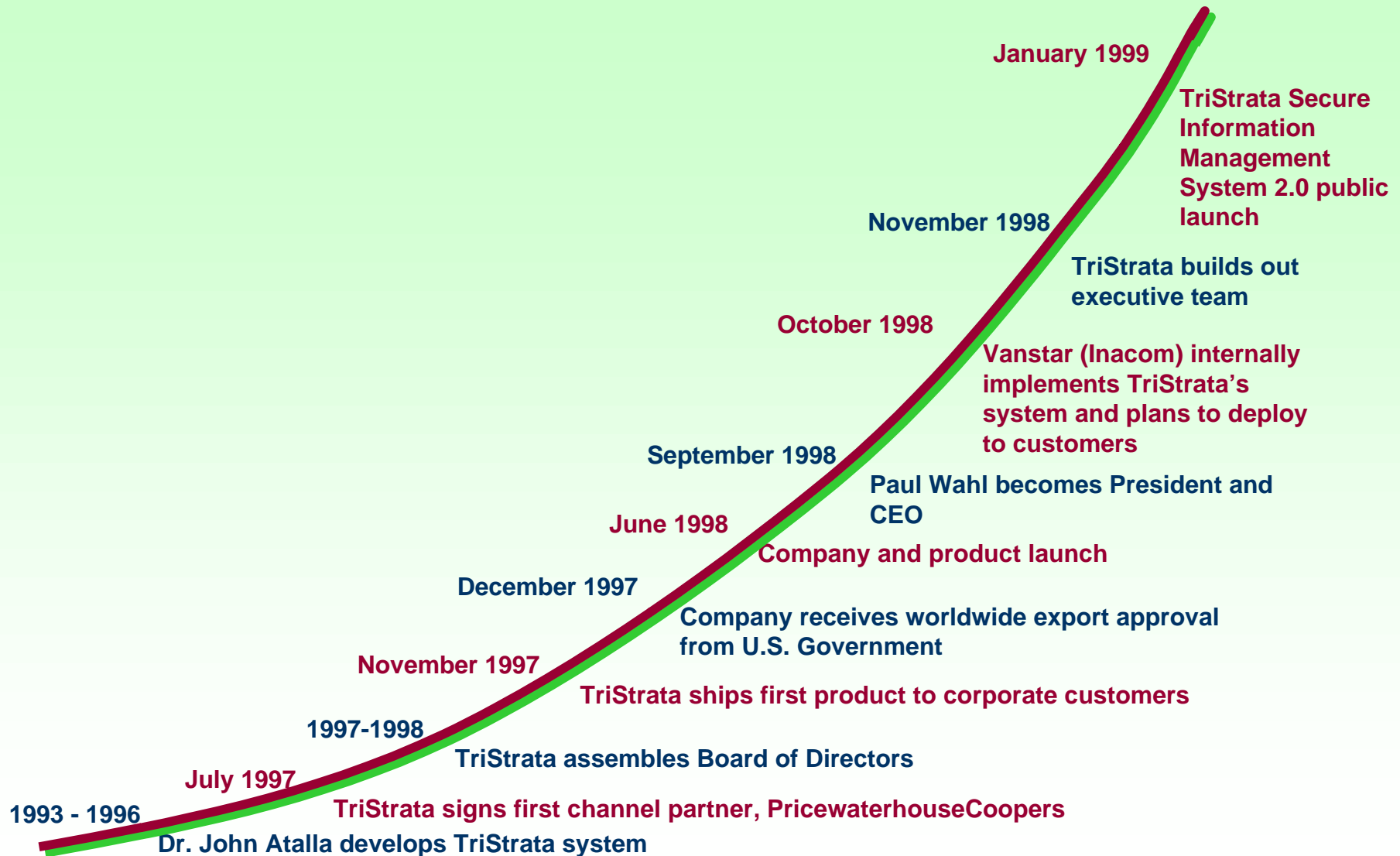- **Enable new business models**

TriStrata Management

- **Chairman & Founder: Dr. John Atalla, inventor of the "Atalla Box" which secures 80%of the world's ATM machines**

- **President & CEO: Paul Wahl, former head of SAP Americas**

- **Board of Directors: John Young (Hewlett-Packard), Tom Perkins (Kleiner Perkins), Bill Zuendt (Wells Fargo), David Beirne (Benchmark Capital), Judith O'Brien (Wilson Sonsini)**

TriStrata Milestones

TriStrata

January 1999

TriStrata Secure Information Management System 2.0 public launch

November 1998

TriStrata builds out executive team

October 1998

Vanstar (Inacom) internally implements TriStrata's system and plans to deploy to customers

September 1998

Paul Wahl becomes President and CEO

June 1998

Company and product launch

December 1997

Company receives worldwide export approval from U.S. Government

November 1997

TriStrata ships first product to corporate customers

1997-1998

TriStrata assembles Board of Directors

July 1997

TriStrata signs first channel partner, PricewaterhouseCoopers

1993 - 1996

Dr. John Atalla develops TriStrata system

TriStrata Alliances

PricewaterhouseCoopers - worldwide team of over 200 providing consulting, deployment, and integration services

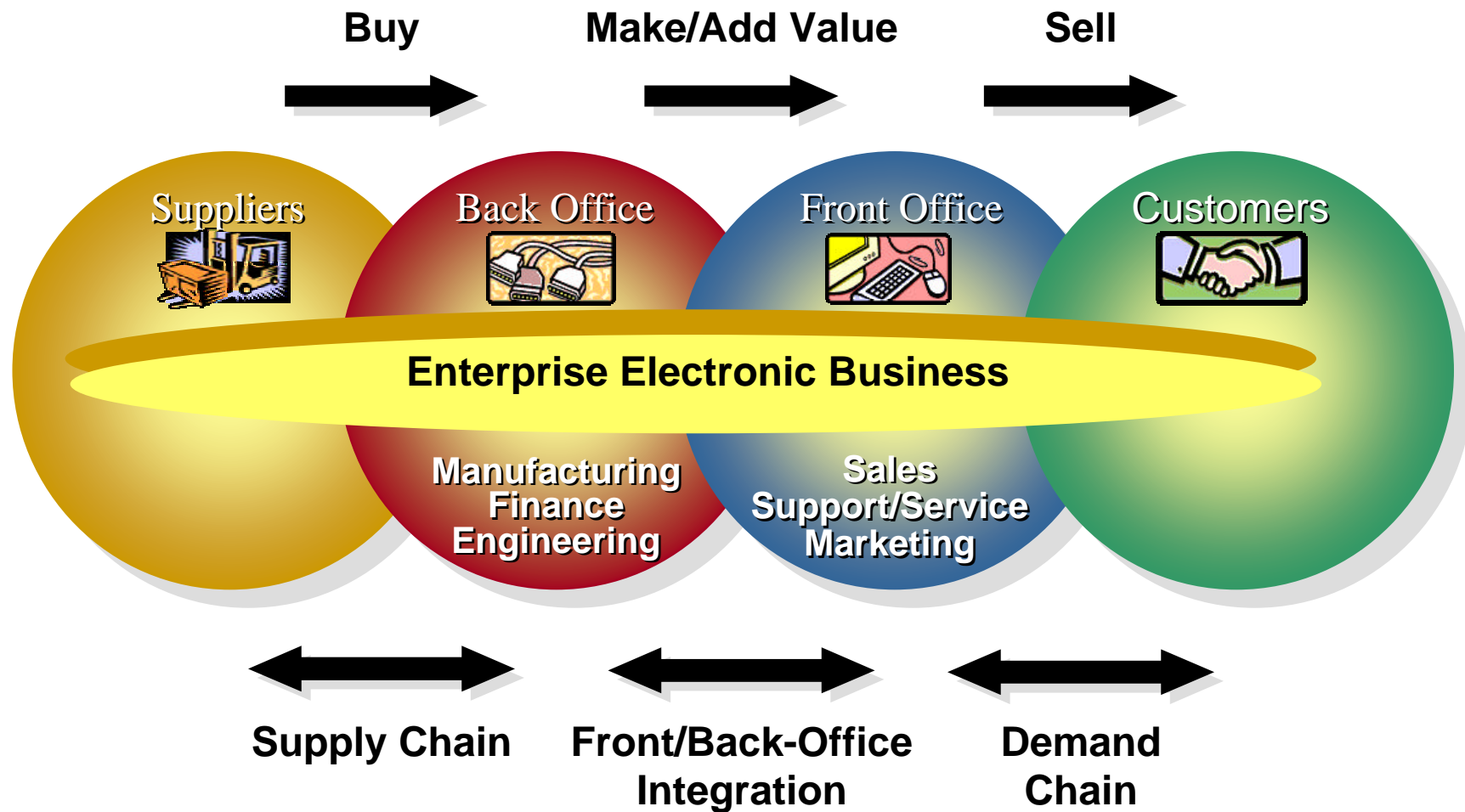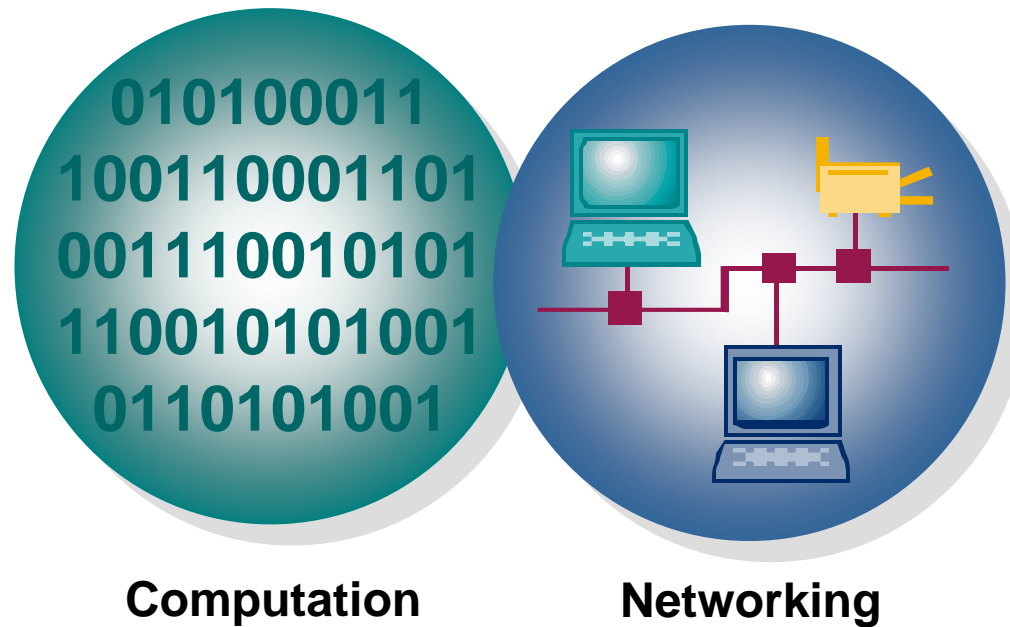**Vanstar (Inacom) - internal deployment for 7000 employees; authorized TriStrata systems integrator**

The Extended Enterprise Today

Buy **Make/Add Value** **Sell**

Suppliers	Back Office	Front Office	Customers

Enterprise Electronic Business

Manufacturing Finance Engineering **Sales Support/Service Marketing**

Supply Chain **Front/Back-Office Integration** **Demand Chain**

Two Infrastructures Are in Place

Computation

Networking

Yet, There is a Problem

- **Attempts to define workable and secure E-business solutions have yet to gain market acceptance**
  - **Existing information security approaches are not integrated and are difficult to manage**
- **The promise of the Internet is unfulfilled**

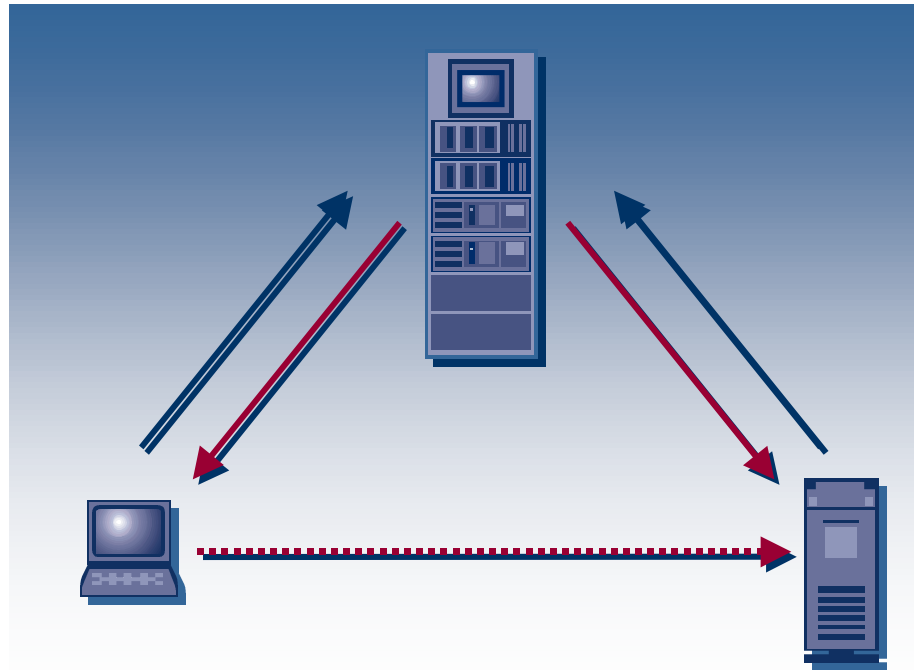# *What is Missing:*
A Protective Infrastructure

Secure Information Management

TriStrata System Overview

The TriStrata Information Security Philosophy

- **All information is secured whether in storage or in transit**

- **Access to information is enforced based on rules which can be dynamically changed**

- **All security operations are controlled by a network-centric management system that keeps a real-time audit of all processes**

Design Assumptions

- **Cost of memory will approach zero**

- **Cost of processing power will approach zero**

- **Networking will become ubiquitous and the cost will steadily decline**

The TriStrata Secure Information Management System

- **Adds a protective layer to an enterprise's existing computing and networking infrastructures**

- **The simple-to-install, easy-to-use system assures a trusted environment to conduct business anywhere on the Internet**

- **Enables new business opportunities, revenue streams, and operating efficiencies**

TriStrata Core Benefits

- ■ **Comprehensive Information Management**
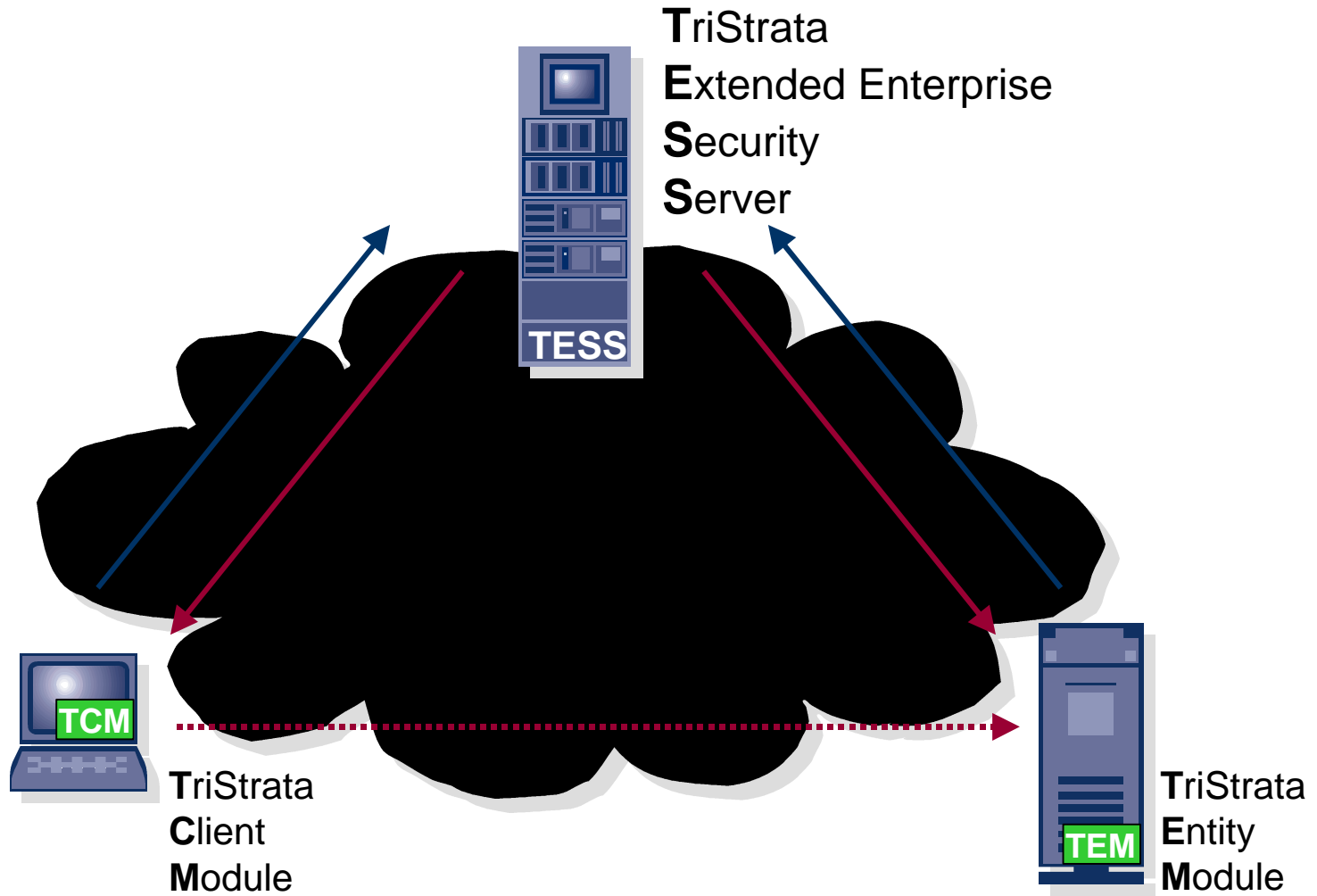 - • **Provides centralized control and tracking of enterprise information**

- ■ **High Performance and Scalability**
  - • **Delivers information protection transparently and without compromises**

- ■ **End-to-end Security Solution**
  - • **Delivers an open, integrated system which significantly lowers cost of ownership**

System Overview

TriStrata
Extended Enterprise
Security
Server

TESS

TCM

TriStrata
Client
Module

TEM

TriStrata
Entity
Module

Fundamental Components

PAL

- **Private Access Line between TESS and client/entity**
- **Extremely low overhead**
- **Authenticated and encrypted**
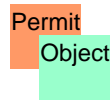- **Used to authorize all security operations**

Random KeyStream^{TM}

- **High performance encryption using simple XOR logic**

Fundamental Components

Permit

"**Permission**" **to encrypt or decrypt data**

Seal

Can only be opened by TESS

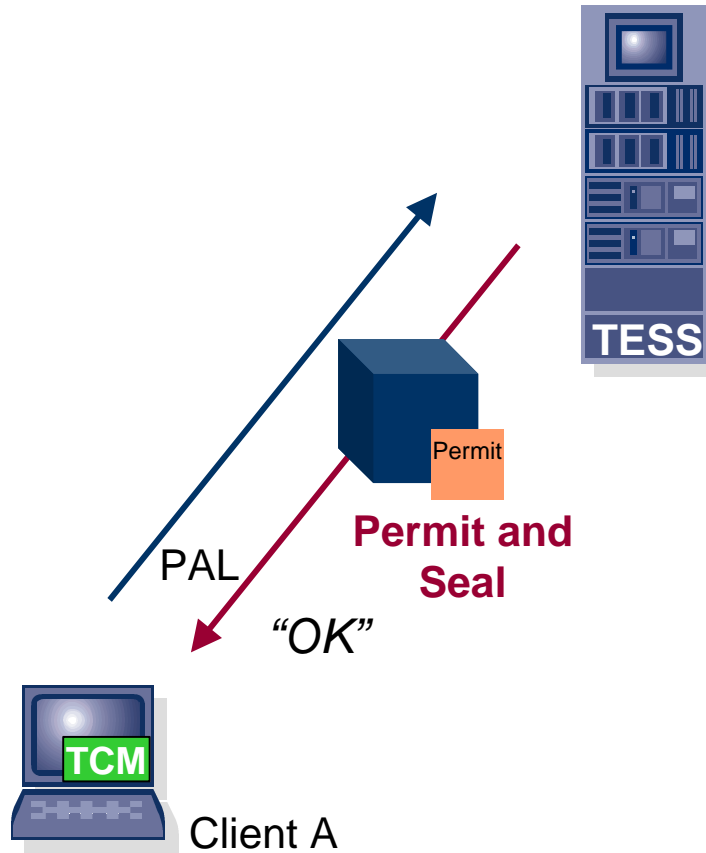**Contains permit and policy information**

Attached to encrypted objects
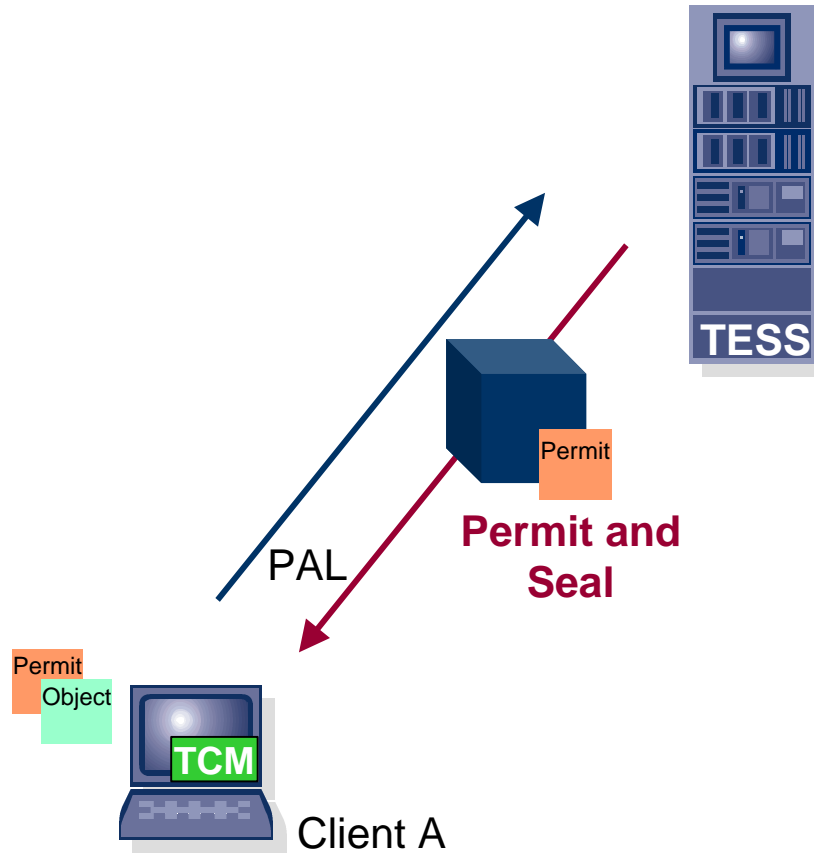
TriStrata Operation
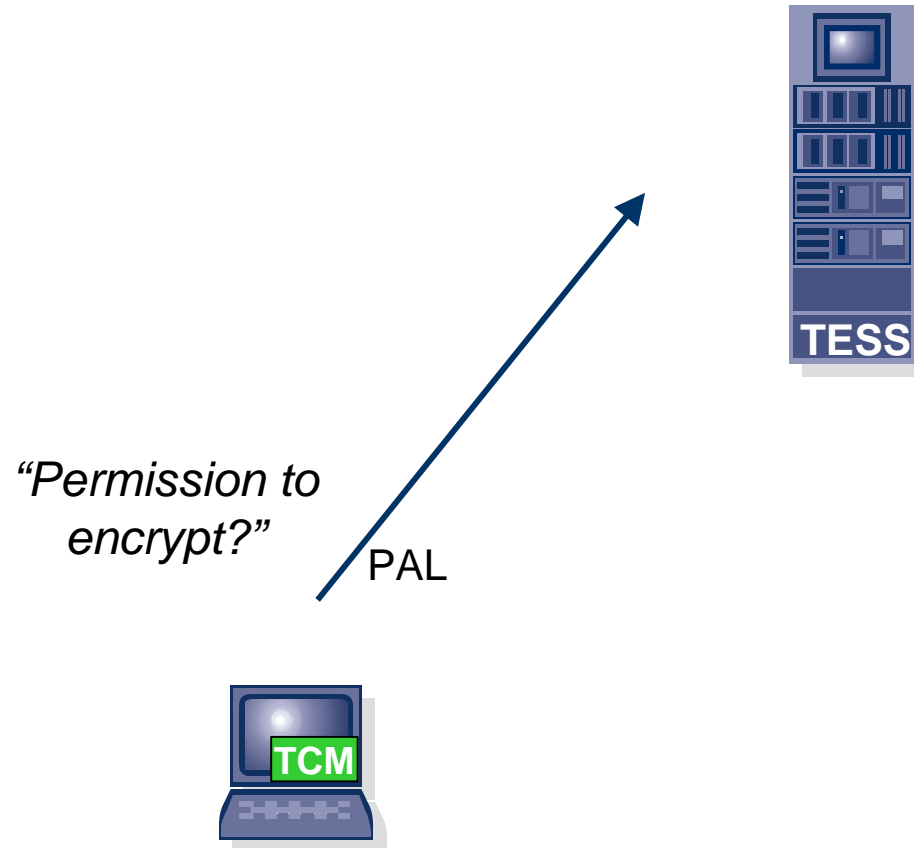
TESS

"Permission to encrypt?"

PAL

TCM

TriStrata Operation

TESS

Permit

Permit and Seal

PAL

"OK"

TCM

Client A

TriStrata Operation

TESS

Permit

Permit and Seal

PAL

Permit
Object

TCM

Client A

TriStrata Operation

TriStrata Operation

TriStrata Operation

TESS

Permit

Seal

Permit

PAL

Permit and Seal

Permit

"OK"

PAL

Permit
Object

TCM

Client A

TCM

Client B

Seal and Secured Object (Any Encryption Method)

TriStrata Operation

TESS

Seal

Permit and Seal

Permit

PAL

PAL

Permit
Object

TCM

Client A

Permit
Object

TCM

Client B

Seal and Secured Object
(Any Encryption Method)
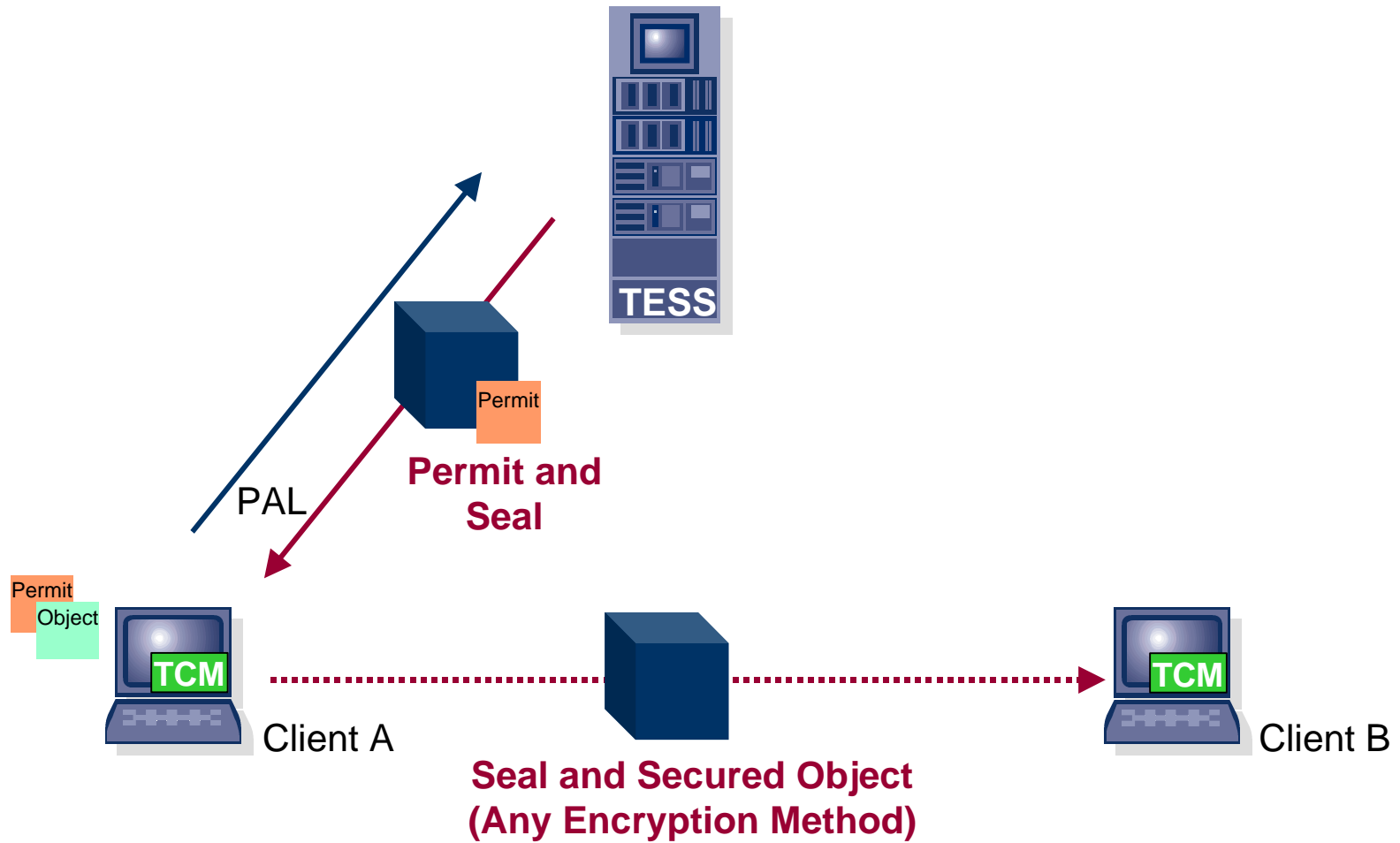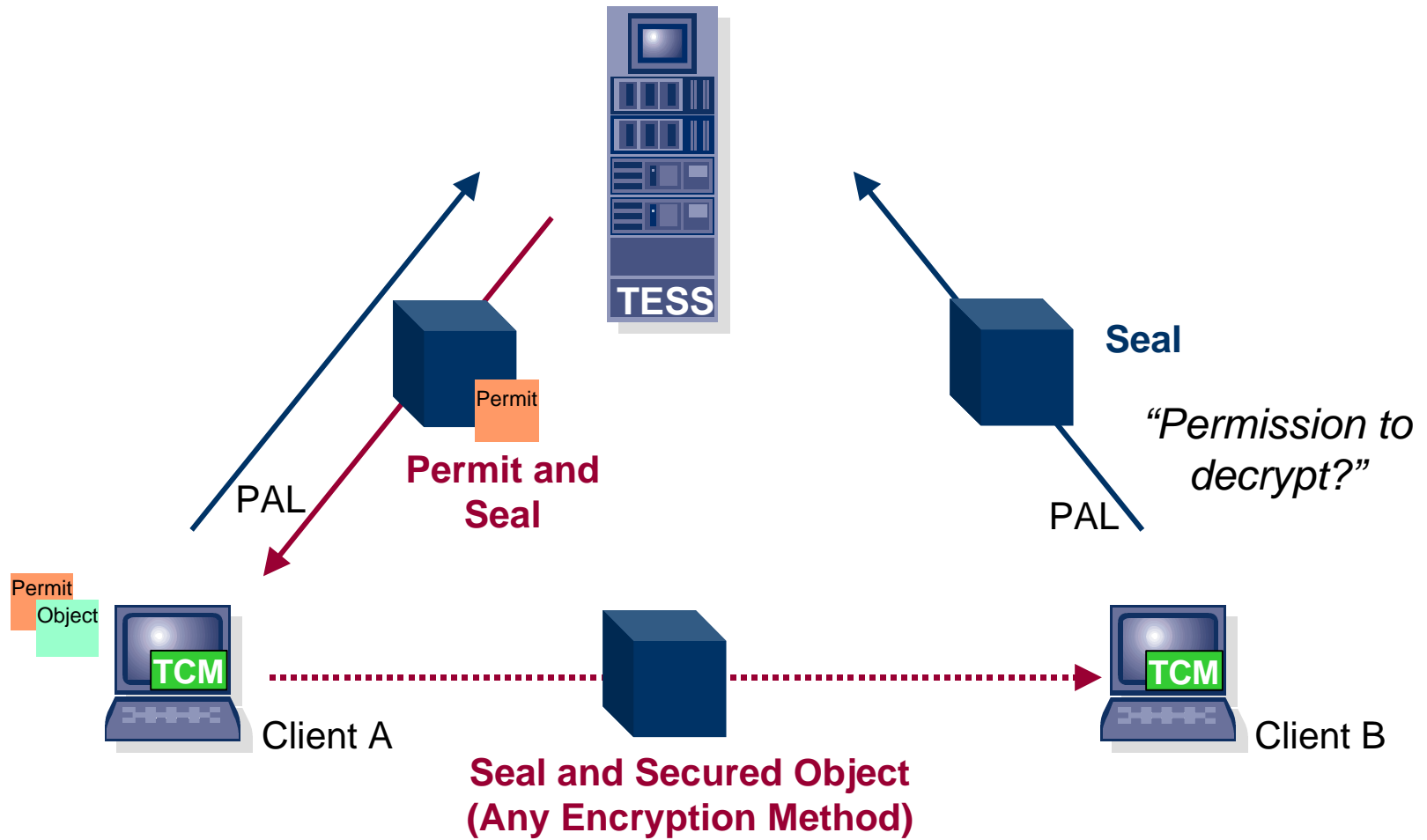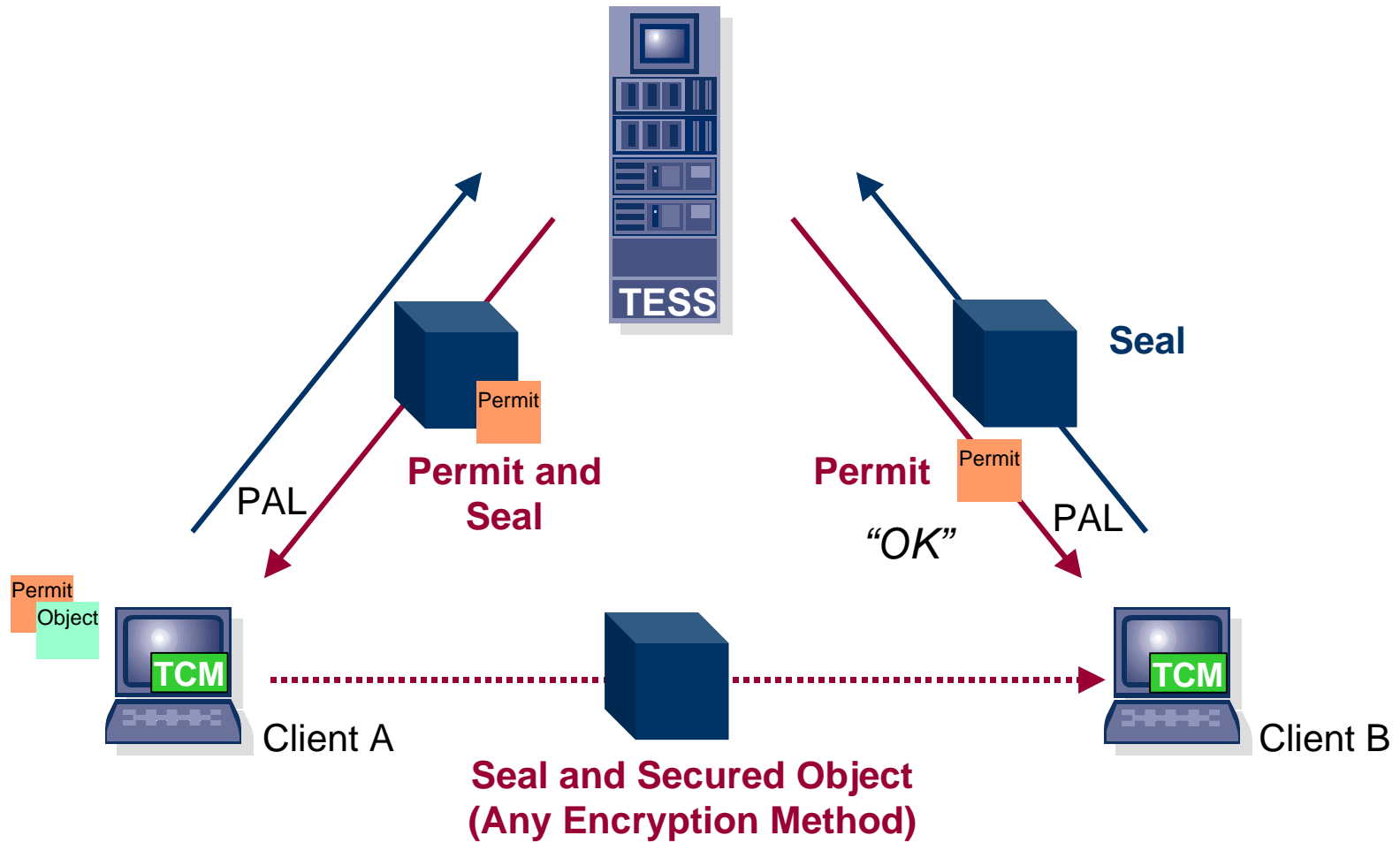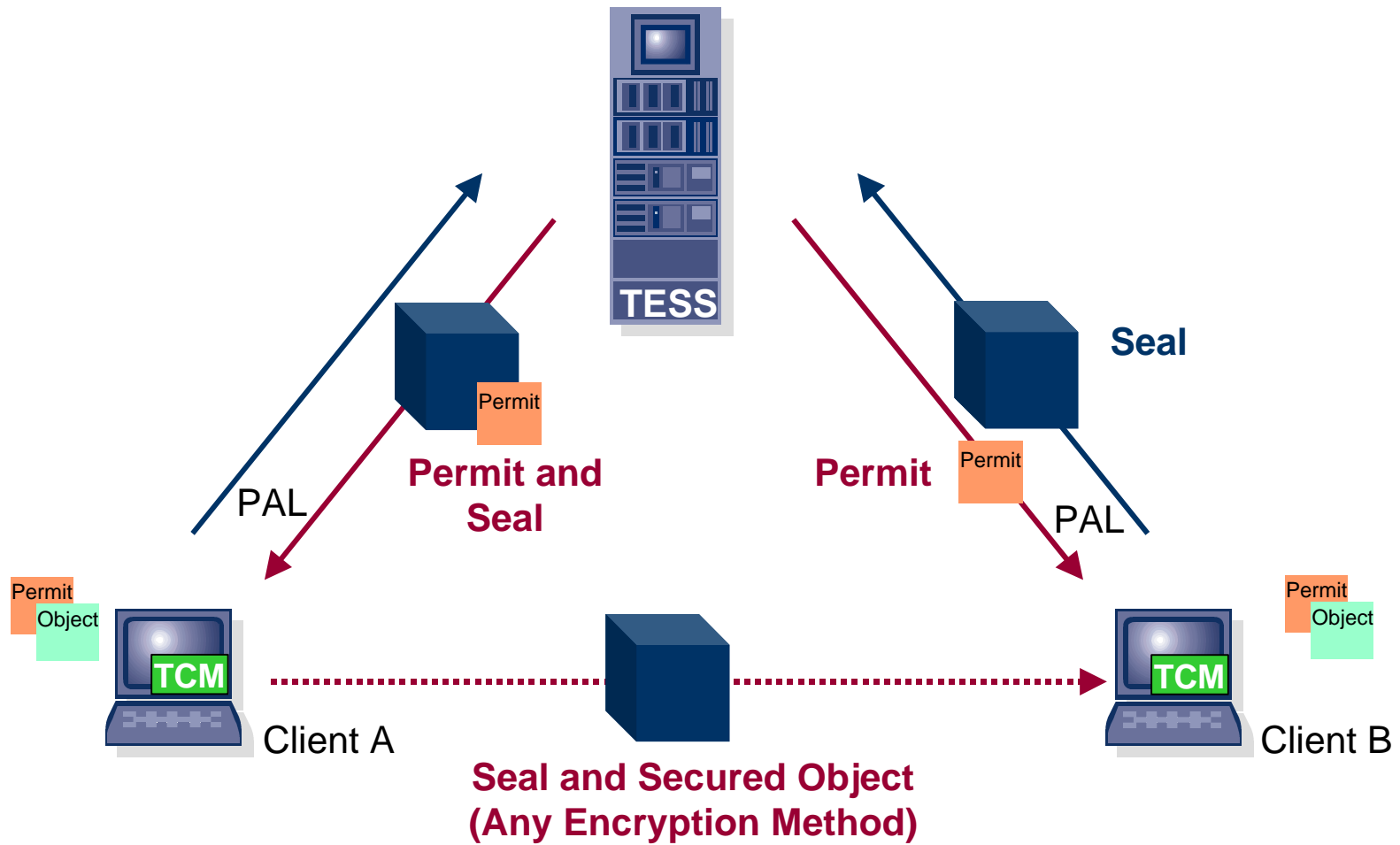
Comprehensive Information Management

- ■ **Information policies can be electronically enforced**
  - Policies can be defined and monitored across applications, systems, and networks

- ■ **All operations are tracked in real-time**
  - System wide records answer key questions: who, what, when, where, why, and how?

- ■ **Global user enrollment and revocation**
  - User privileges can be added or removed from any workstation
  - Full data recovery available

Performance and Scalability

- **One system supports 1 million users**
 - Many organizations and departments can be defined

- **Industry-leading transaction processing performance**
  - Each TESS operates at 2,000 transactions/second
  - Up to 8 replicas add capacity and availability

- **All types of information - e-mail, documents, data, voice, video - are easily protected**
  - Random KeyStream™ encryption operates at 96 Mbits/second
  - Other customer-specified encryption can be used

Region 1

Region 2

TESS
Relay

Region 3

Region 4
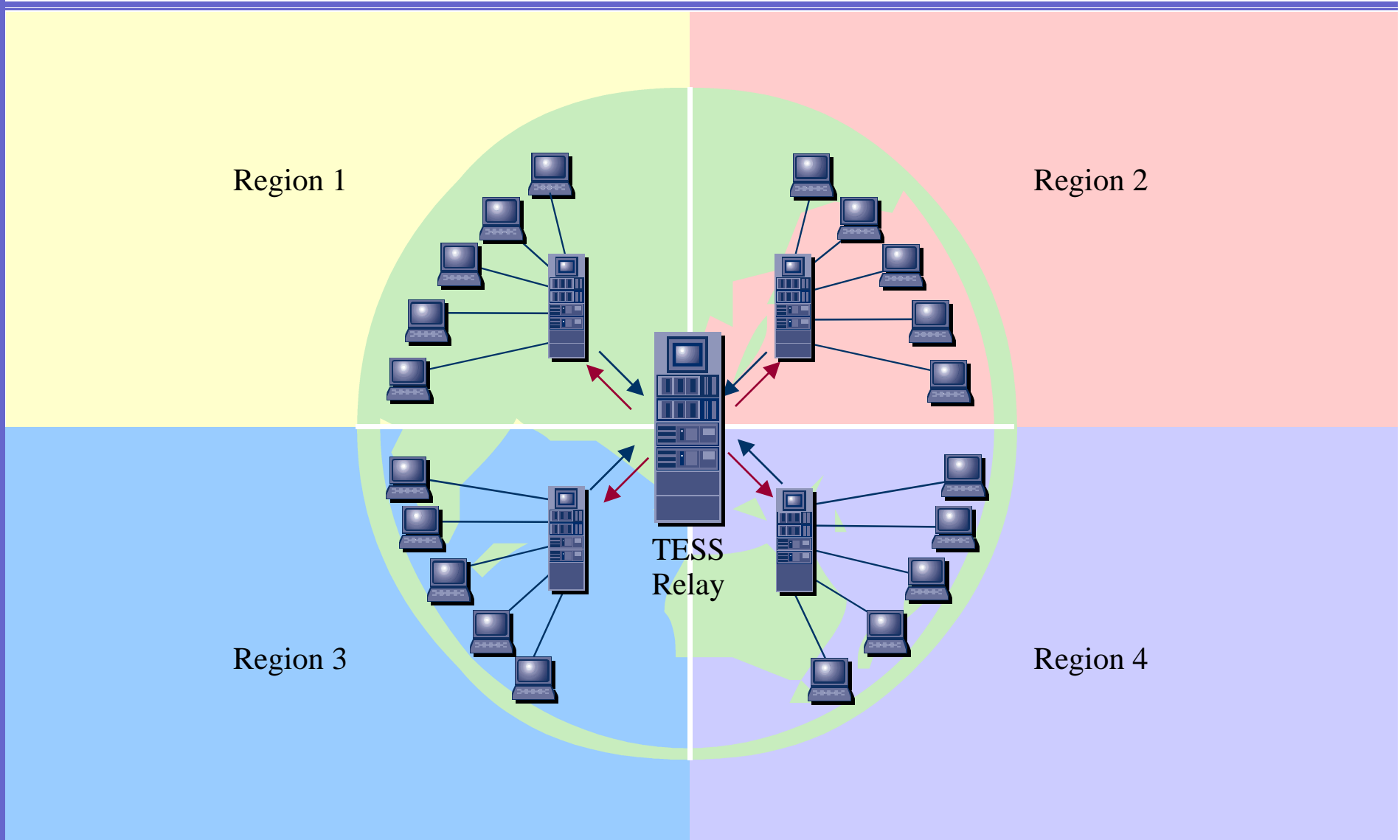
End-to-End Solution

- **One system provides information protection and management**
  - Authentication, authorization, data integrity, confidentiality, digital signature, and auditing
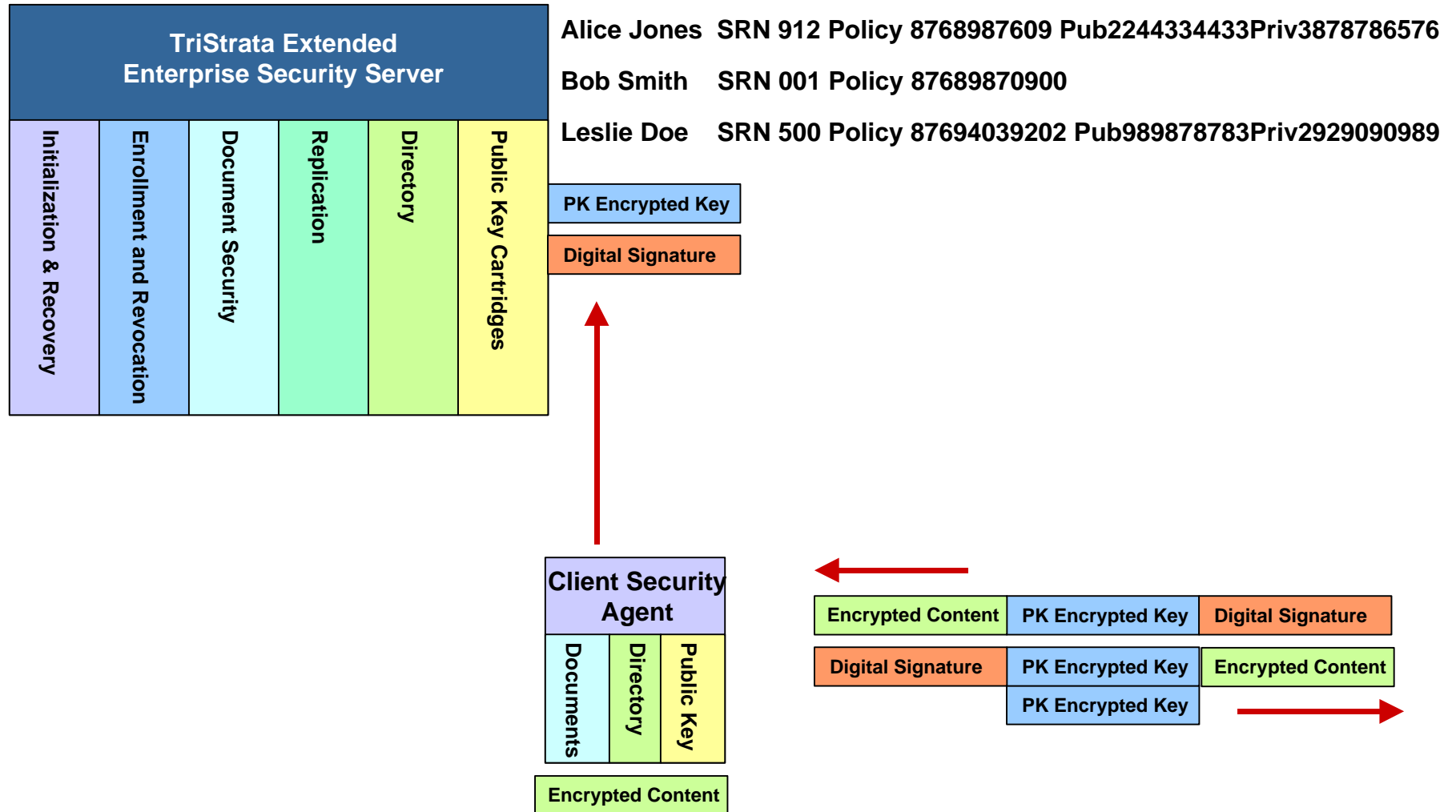
- **Globally exportable**
  - Based on self-escrow key management and recovery, approved for worldwide export

- **Readily integrates with current IT infrastructure**
  - SDK available for enterprises and ISVs
  - Designed to interoperate with PKI

TriStrata-PKI Interoperability

TriStrata Extended Enterprise Security Server

Initialization & Recovery	Enrollment and Revocation	Document Security	Replication	Directory	Public Key Cartridges

Alice Jones SRN 912 Policy 8768987609 Pub2244334433Priv3878786576

Bob Smith SRN 001 Policy 87689870900

Leslie Doe SRN 500 Policy 87694039202 Pub989878783Priv2929090989

PK Encrypted Key

Digital Signature

Client Security Agent

Documents	Directory	Public Key

Encrypted Content

Encrypted Content	PK Encrypted Key	Digital Signature

Digital Signature	PK Encrypted Key	Encrypted Content

PK Encrypted Key

TriStrata Applications

- **Enterprise security**
  - **E-mail**
  - **Files**
  - **Fax**
  - **Video**

- **E-commerce**
  - **Transactions**
  - **Electronic content distribution**

TriStrata Applications

- **Secure virtual office services**
  - **E-mail, fax, voicemail, videoconferencing**

- **Applications outsourcing**

- **Virtual private networks**

- **Trusted third-party services**

TriStrata System Delivery

- **Pre-defined system implementation**
  - Predictable delivery, whether from TriStrata or partner
  - Result: working system with baseline policies

- **7x24 global system support**
  - Heavy emphasis on web-based resources, for self-service and quick reference

- **Optional Secure Transaction Server (STS) services**

New Features 2.0 Release

- **Open Cryptography**
- **Up to 8 TESS Replicas**
- **Fully integrated SDK**
- **Organizations**
- **Dynamic Membership Groups**
- **Notes, Exchange, Outlook 97/98**
- **Fully integrated in desktop**

TriStrata

Thank you!