



BALTIMORE

*global
e-security*

www.baltimore.com

Baltimore Presents:

*ABN AMRO Bank's Corporate
Cryptographic Infrastructure*





BALTIMORE

*global
e-security*

www.baltimore.com

Baltimore Technologies

- 20 years experience in cryptography and PKI
- 20 years experience in design and deployment of e-security solutions
- World class PKI technology
- Breadth of product offering
 - ◆ Certificate Authority
 - ◆ Toolkits
- Commitment to open standards

Market-leading innovation, features and flexibility





BALTIMORE

*global
e-security*

www.baltimore.com

ABN Amro Bank

- One of the leading universal network banks
- Headquartered in the Netherlands
- Locations in 76 different countries and territories
- More than 3,500 offices
- Total assets exceed 464 billion Euro
- Ranked the world's sixth largest bank (based on total assets)
- Over 105,000 full time employees





BALTIMORE

*global
e-security*

www.baltimore.com

ABN Amro IT Infrastructure

- Global and distributed infrastructure
- Great variety in platforms
- Multi-vendor environment
- Complex systems
- Growing integration
- External connections
- Use of public networks
- High value payment transactions





BALTIMORE

*global
e-security*

www.baltimore.com

What Is The CCI Project?

- Corporate Cryptographic Infrastructure
- Security system based on secret and public key cryptography that provides security to ABN AMRO banking activities around the world
- Objective of CCI is to deliver cryptographic services to any user of ABN AMRO application that needs it, on any platform, anywhere in the world in a common and consistent way
- Project delivers a full operational PKI combined with a standard set of cryptographic services
- Partnership with Baltimore and IBM (Solution Provider)





BALTIMORE

*global
e-security*

www.baltimore.com

Why Does ABN AMRO Need CCI?

- Need for secure storage and transport of data with bank's infrastructure
- Need for secure communications with customers, partners, and other banks
- Cryptography can make security independent of the complexity of the banks IT infrastructure
- Cryptography is the only known practical method for delivering end to end security



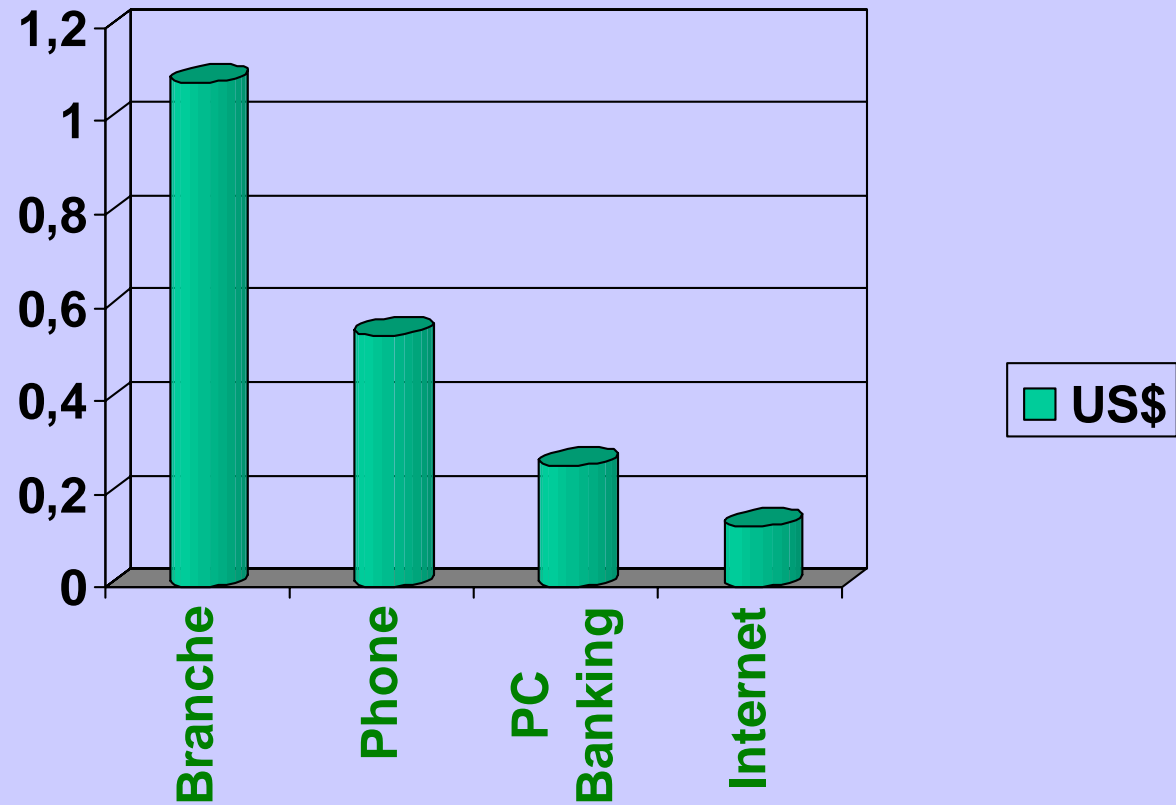


BALTIMORE

Banking Costs Per Transaction

*global
e-security*

www.baltimore.com





Situation Before CCI

- Different security solutions for basically the same security requirements
- Security solutions integrated into the applications, which makes re-use of solutions a problem
- Variety of different tools is inefficient to manage
- Integration of partial solutions is difficult and parts of the infrastructure are not protected



BALTIMORE

CCI – Security Services

*global
e-security*

- Peer Entity Authentication
- Data Integrity
- Origin Authentication
- Data Confidentiality
- Software Integrity
- Message Sequence Integrity
- Non-repudiation with proof of Origin
- Non-repudiation with proof of Delivery

www.baltimore.com





BALTIMORE

CCI – Requirements

*global
e-security*

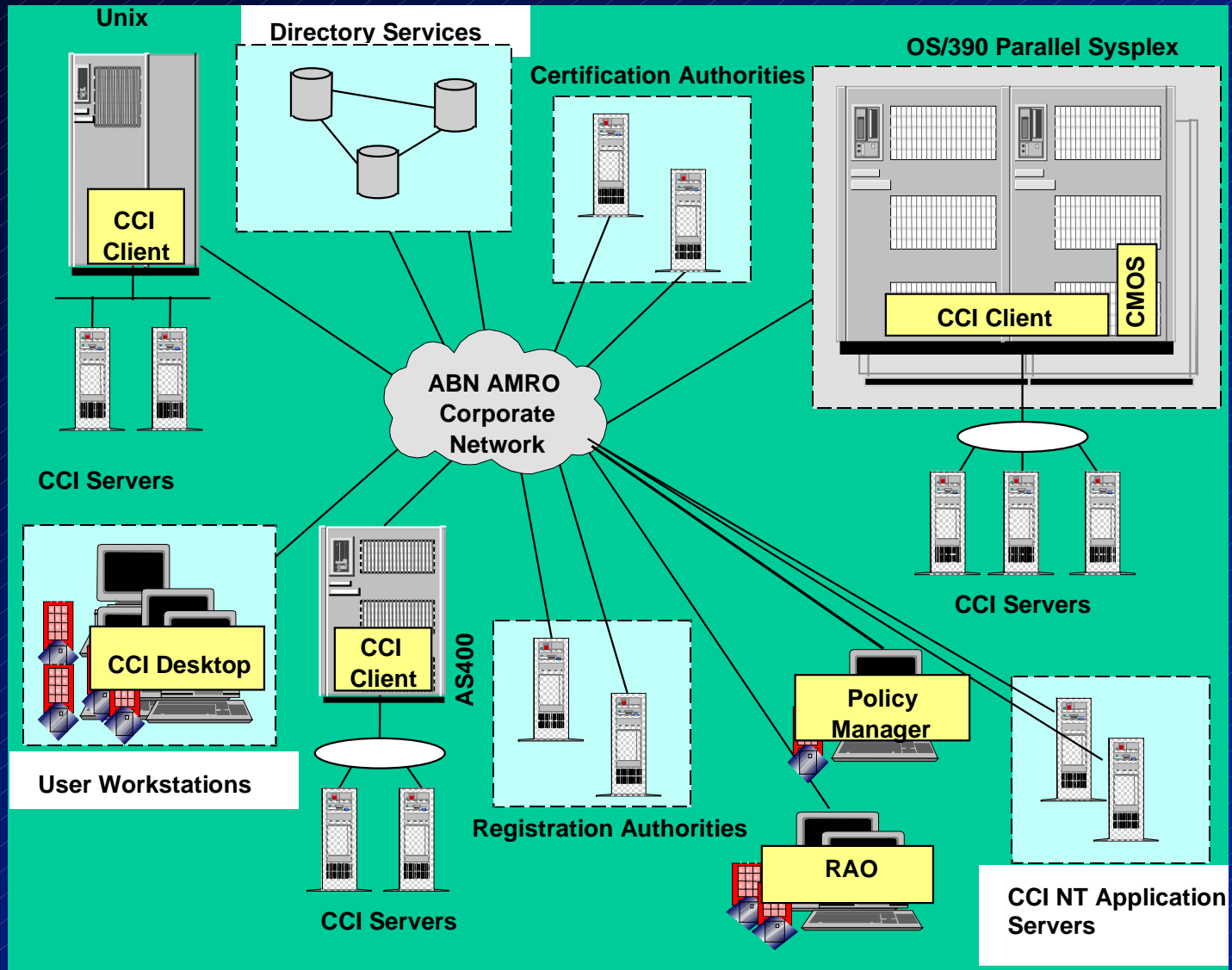
- Secure implementation
- Standards based/ Interoperability
- Multi-platform support
- Performance scalability
- Hardware independent
- Highly automated key management
- Proven technology
- Selectable level of security
- Ease of use
- High availability

www.baltimore.com

CCI – Architectural Overview

*global
e-security*

www.baltimore.com





CCI – Components

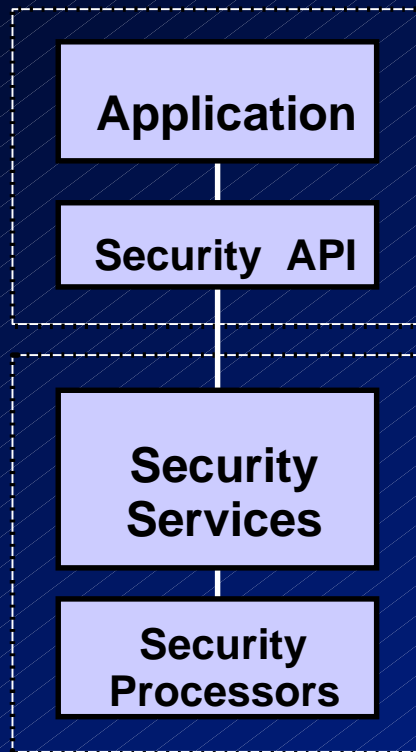
- Smart Cards as personalized tokens for user authentication and for generation of digital signatures
- PC-software modules for workstations
- Cryptographic Adapters (IBM 4758, nCipher) for servers and critical workstations
- Security servers and CMOS technology (on-board crypto) on IBM mainframes



CCI Security Architecture

*global
e-security*

www.baltimore.com



A Range of Options:

- Software only
- SmartCard
- SmartCard Reader
- PCMCIA
- Smart Disk
- PC Cryptoboard
- Host Security Module

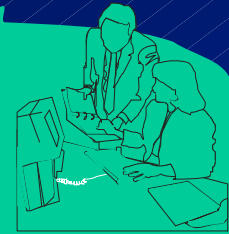


BALTIMORE

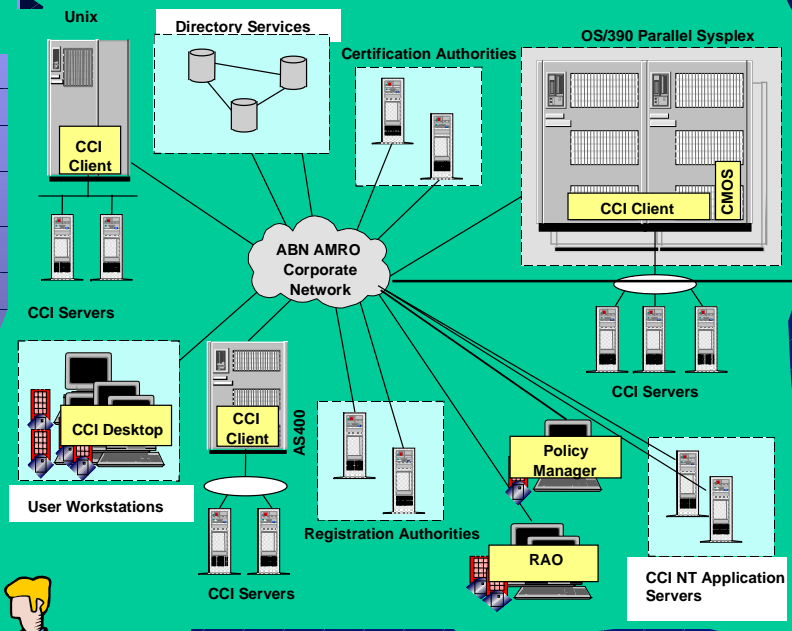
The Extended Network



Partners



Corporate Clients



Firewall



Internet

Information Servers

Offices

Registration Authorities

Users



Suppliers

www.baltimore.com



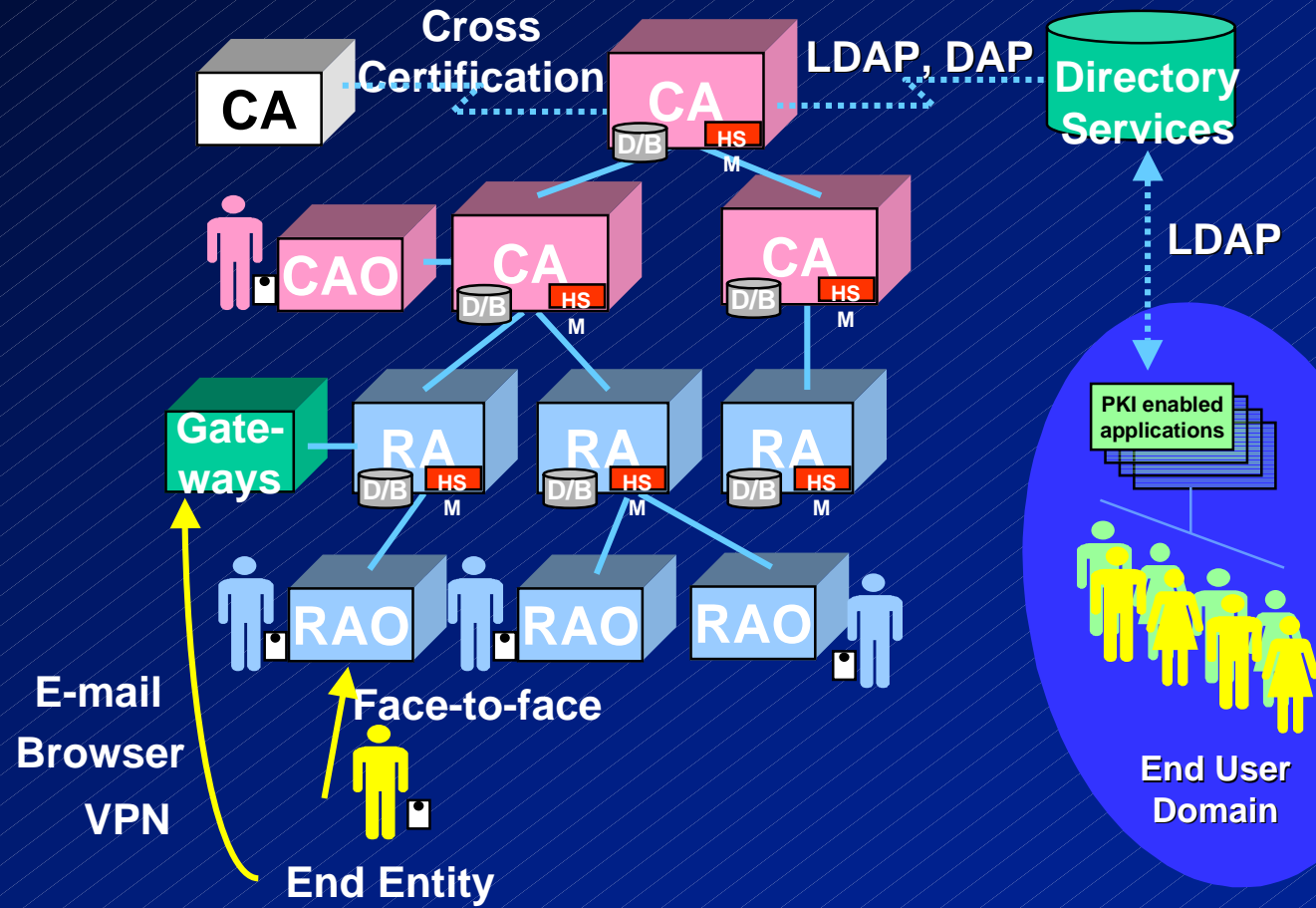
Summary of Standards

- Cryptographic algorithms (DES, triple-DES, RSA, SHA-1, ANSI X9.9, etc)
- ISO 9796 format (SHA-1 and RSA) digital signatures
- ISO/IEC CD 11770-3 key management mechanisms using asymmetric techniques
- ISO/IEC 9798-3 entity authentication using a public key algorithm
- X.509 v3 Public Key Certificates with extensions
- CRL v2 Revocation Lists
- X.500 Directory Services
- PKIX standards (RA/CA & CA/CA)
- GSS-API, IDUP GSS-API, LDAP v2, PKCS, OCSP

CCI PKI Architecture

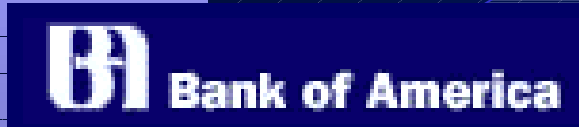
*global
e-security*

www.baltimore.com

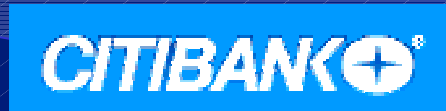


Who is IDENTRUS?

*global
e-security*



IDENTRUS



(Situation early 1999)



BALTIMORE

Strategy Of IDENTRUS

*global
e-security*

- Facilitate electronic commerce through the establishment of trusted certificate authorities owned and operated by leading global banks
- Bank certificate authorities to be independent but interoperable
- Standards-based, vendor neutral, global scope, legal framework

www.baltimore.com





BALTIMORE

IDENTRUS Four Corner Model

*global
e-security*

Buyer's Bank

Seller's Bank



TRUST



TRUST



NO Trust



Buyer

Seller

www.baltimore.com





BALTIMORE

Trust enables E-Commerce

global e-security



**IDENTRUS
Root CA**

**Buyer's Bank
Certificate Authority**

**Legal/Contract Framework
Define standard operating and
liability rules for corporations**

**Seller's Bank
Certificate Authority**



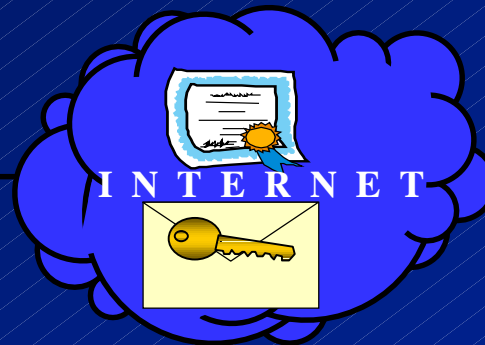
**Certificate Validation/Warranty
Request and Reply**



**On-Line Certificate
Validation / Warranty
Request**



Buyer



INTERNET



Seller

**Smart Cards
with certificates**

purchase order (Signed Data)

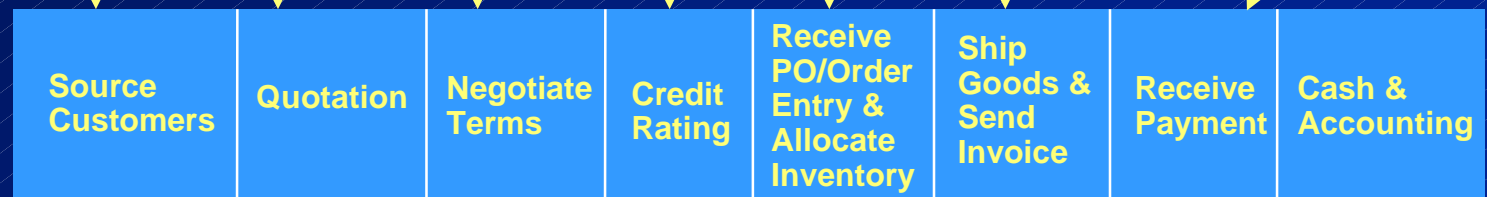
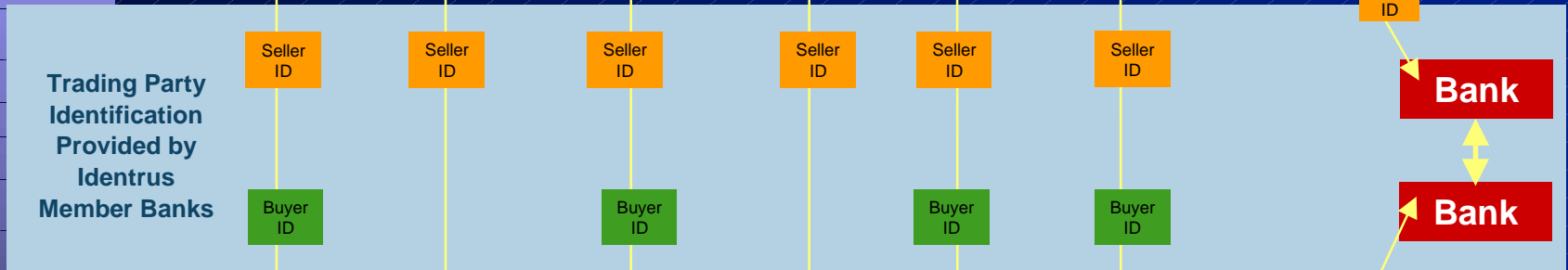
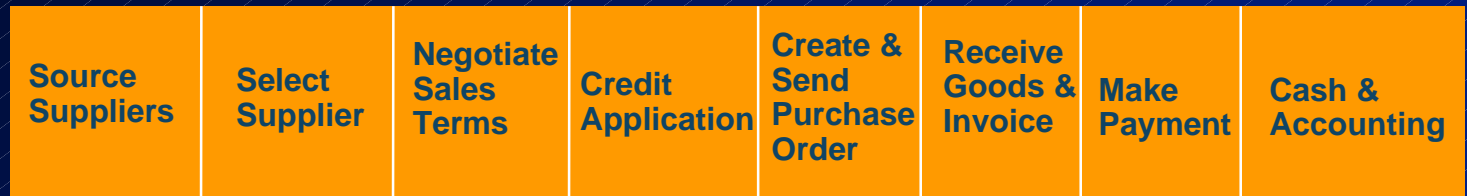
www.baltimore.com

Value Throughout The Transaction Life Cycle

global
e-security

Buyer

Purchasing Process



Seller

Selling Process



CCI Public Key Infrastructure

- PKI will be based on UNICERT (Baltimore)
- PKI supports all ABN AMRO public key based solutions
- Key generation is responsibility of applications
- Secure transport of public key certificate requests via public networks using smart cards
- Generation of smart card keys during personalisation



CCI Future Directions

*global
e-security*

- More focus on Internet/Intranet
- Automatic certificate renewal
- Bulk certificate issuing
- Encryption of stored data
- Key recovery
- Attribute certificates
- Time stamping
- Secure Single Sign-on
- New algorithms and Protocols
- More use of products on the market
(instead of own developments)

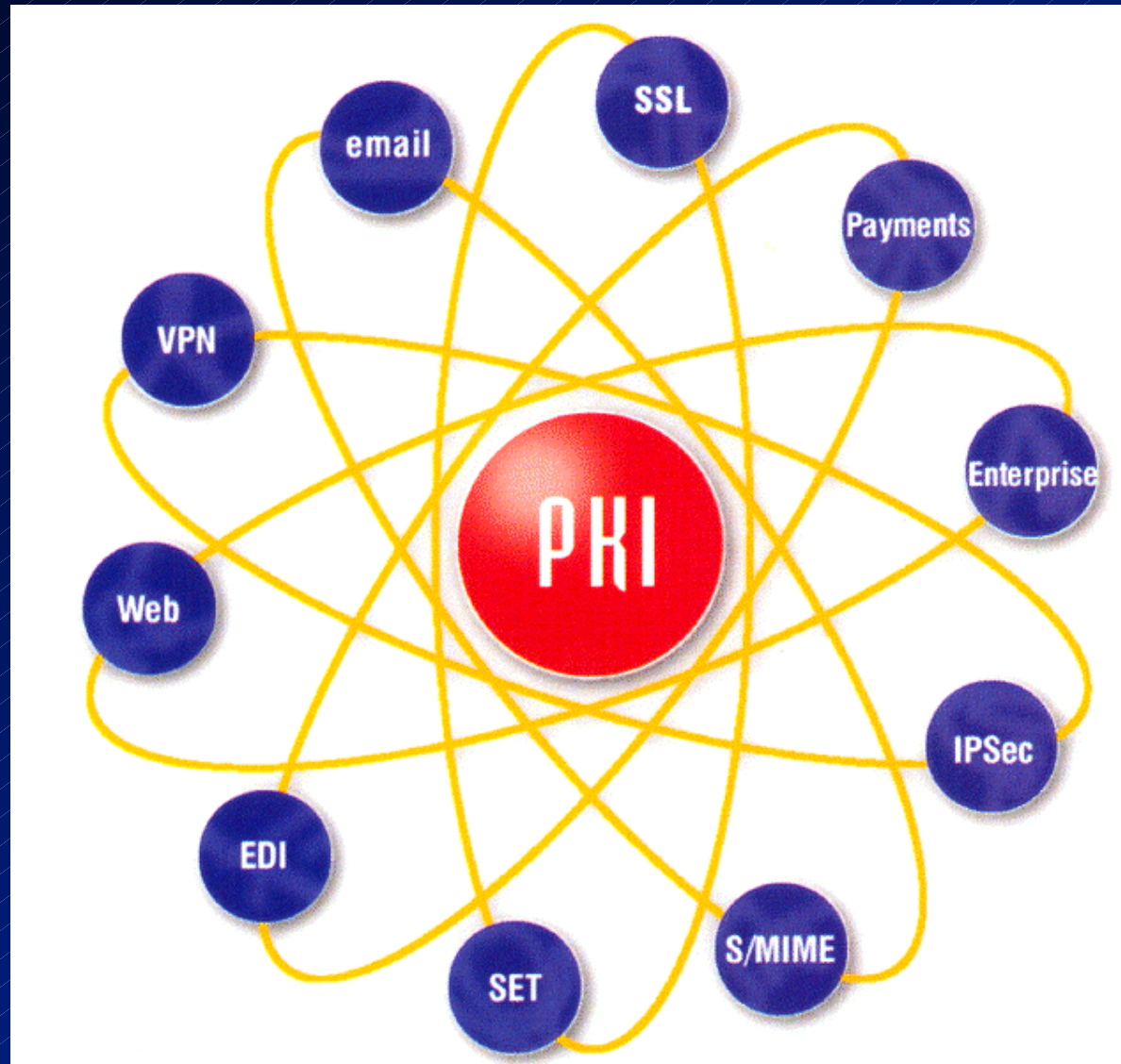


BALTIMORE

PKI At The Heart Of ABN AMRO Security

*global
e-security*

www.baltimore.com





BALTIMORE

*global
e-security*

www.baltimore.com

ABN AMRO and Baltimore

We selected Baltimore because of their understanding of the security needs of the banking sector. We expect their PKI and their systems integration capability will give us exactly the solution we require.

Eric Koop

VP, IT Solutions Division - ABN AMRO Bank



ABN•AMRO • *The Network Bank™*

