



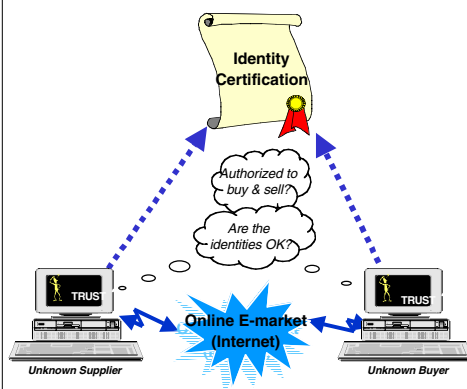
John G Bullard

Managing Director, Participant  
Relations

Identrus LLC

# Identrus Principles

## Requirements for Establishing E-trust



- **Privacy** - Prevent other from eavesdropping on confidential communications.
- **Authentication** - Verify the identity of the sending party.
- **Integrity** - Ensure that the information is not altered in transit.
- **Non-Repudiation** - Provide integrity and authentication that can be validated by a court of law.
- **Global System Interoperability** - spans geo-political boundaries for operating rules and legal environment.

# Identrus Fundamentals

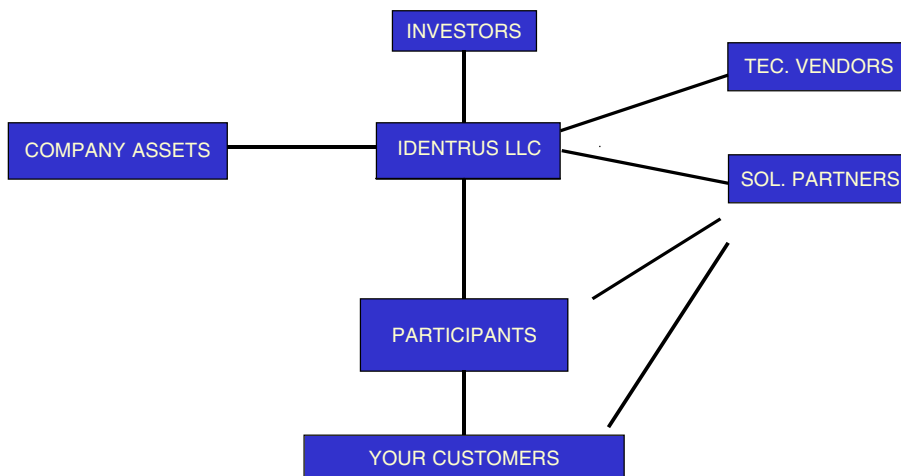
- Corporate Model
- Global scheme
- Interoperable technologies
- Interoperable risk management
- Open infrastructure and open scheme
- Infrastructure, not applications
- Scheme Operator, scheme operations
- Business-Business / Corporate Scope
- Closed System - closed by contract
- Open market - application enablement

5

Identrus Confidential

• Solution for customer

## IDENTRUS RELATIONSHIPS - Balance and level playing fields



6

Identrus Confidential



## Our Creed - Digital Identity credentials as essential territory for

FI's-

As agents of trust, managers of risk, and enablers of commerce, financial institutions are uniquely positioned to provide CA services to buyers and sellers and make digital certificates an integral part of the global electronic commerce marketplace.

7

*Identrus Confidential*



## REGULATION- United States Federal Reserve Board Order

...

### **Proposed Activities**

Identrus is a joint venture among Notificants and other commercial banks and foreign banking organizations. Under the proposal Identrus would act as the global rulemaking and coordinating body for a network of financial institutions that would act as CAs and thereby provide services designed to verify or authenticate the identity of customers conducting financial and non-financial transactions over the Internet and other "open" electronic networks. To provide these services, Identrus and its network of participating financial institutions (the "Identrus System") would utilize digital certificates and digital signatures created through the use of public key cryptography.

...

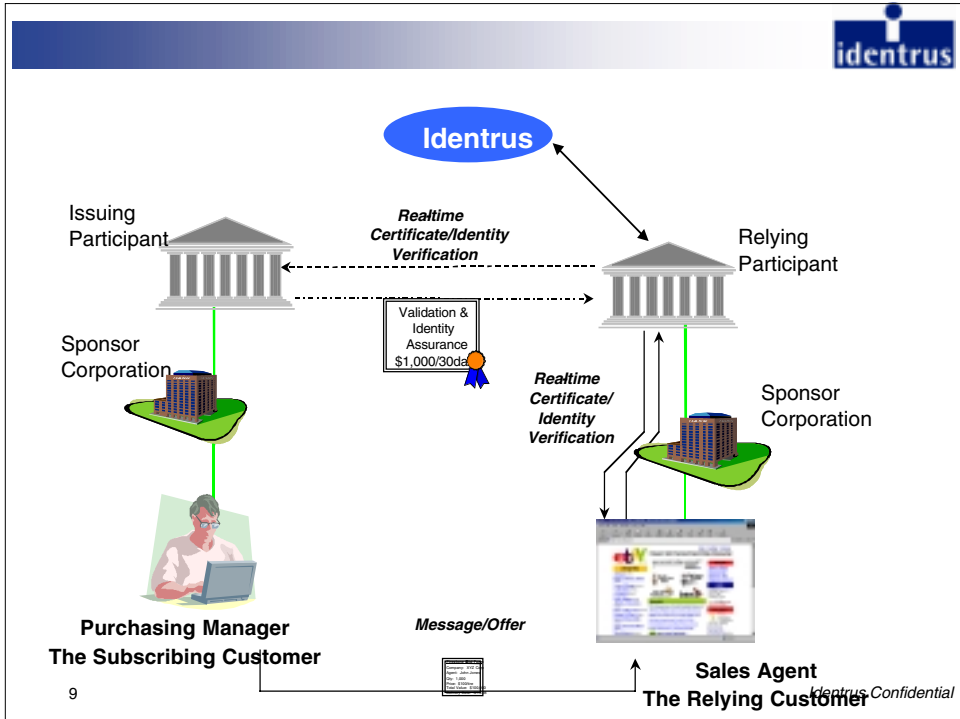
### **Conclusion**

Based on the foregoing and all the facts of record, the Board has determined that the proposal should be, and hereby is, approved.

...

**By order of the Board of Governors, effective November 10, 1999**

<sup>8</sup> Voting for this action: Chairman Greenspan, Vice Chairman Ferguson, and Governors Kelley, *Identrus Confidential*



9

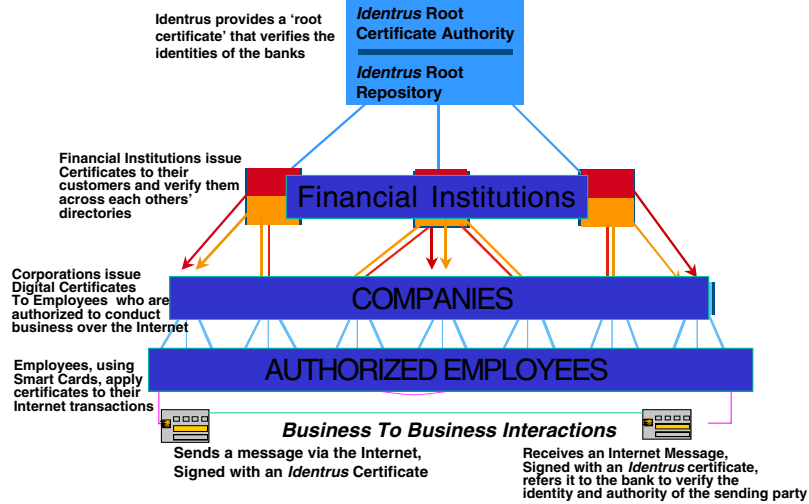
Identrus Confidential

Delivering on the Identrus principles

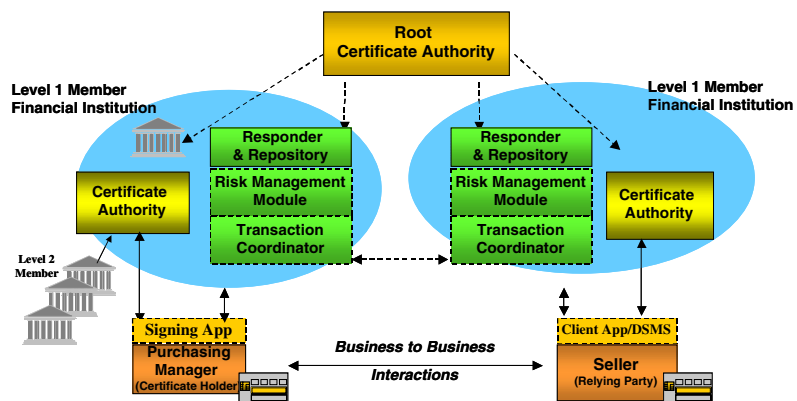
10

Identrus Confidential

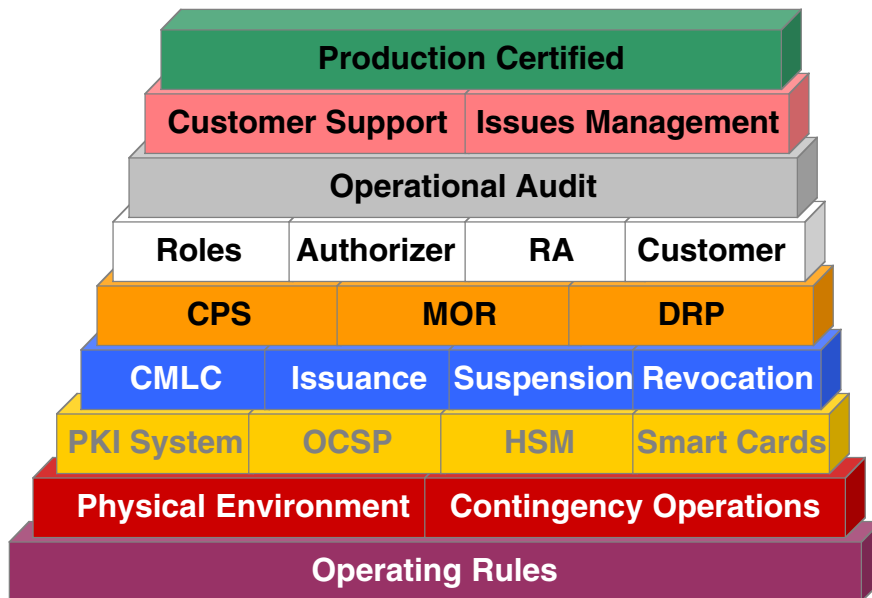
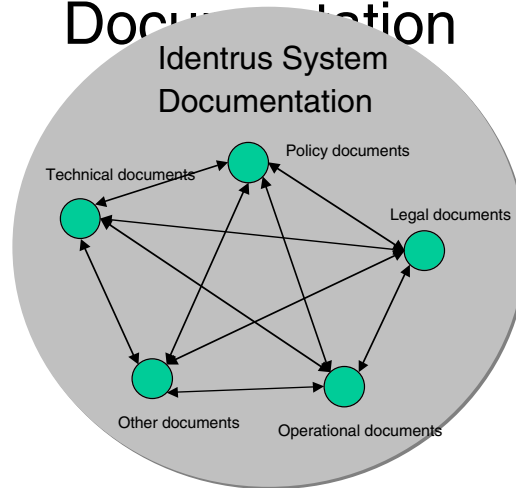
# Trust Architecture



# Technology Architecture



# Identrus System Documentation



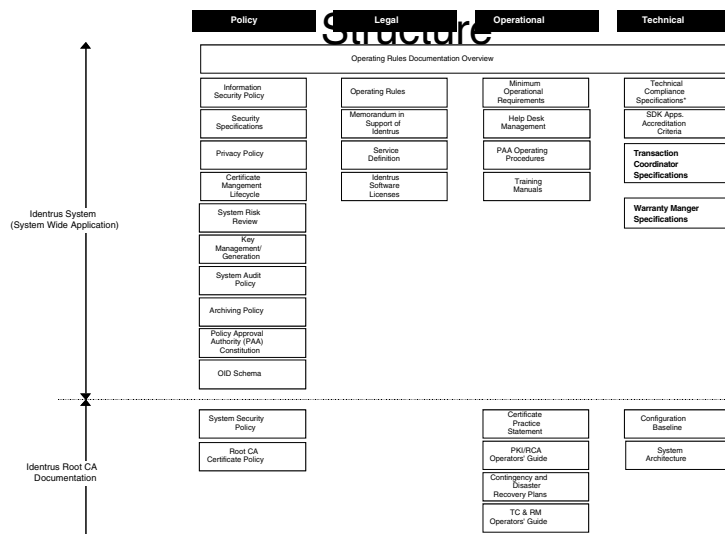
## Operating Rules - Objectives

- Defines the baseline compliance procedures (operating and security practices) for both Identrus and participating Financial Institutions.
- Defines risk management practices and procedures to ensure soundness of the system.
- Creates a framework of legally binding contracts to ensure global legal interoperability.
- Specifies the minimum eligibility for participants.
- Incorporates all aspects of the Identrus system into a consistent set of user documents covering:
  - Policy
  - Legal
  - Operations
  - Technical

15

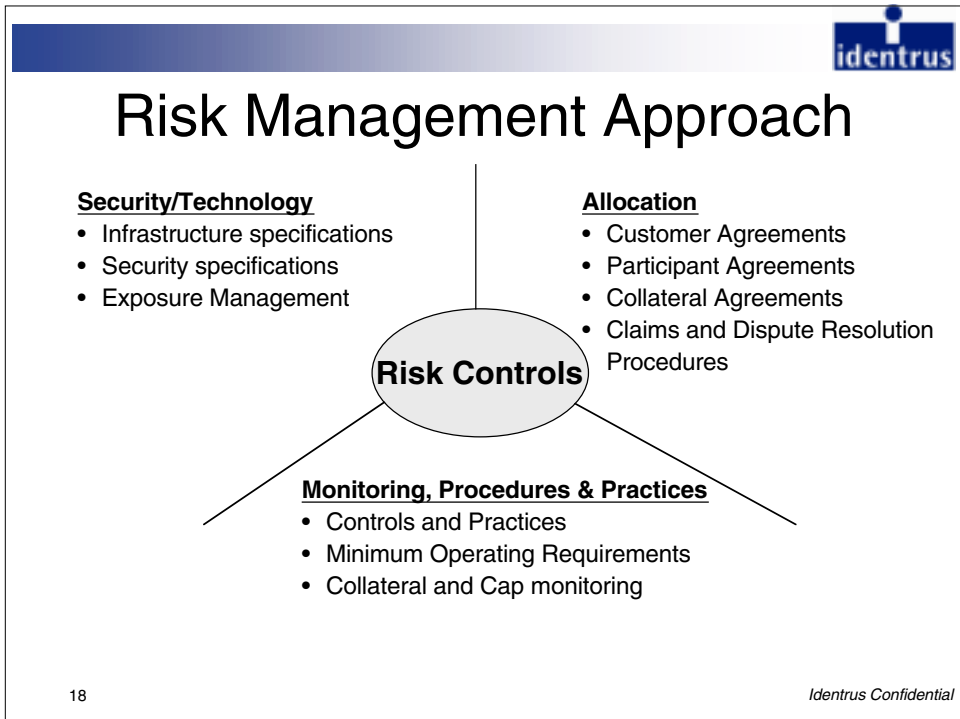
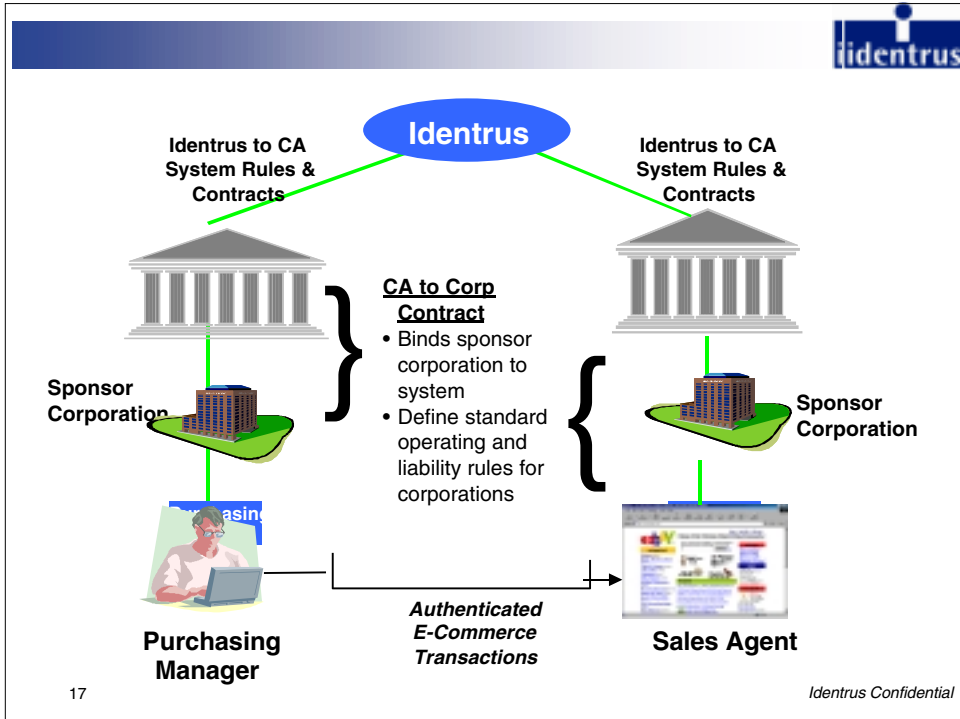
Identrus Confidential

## Operating Rules – Documentation



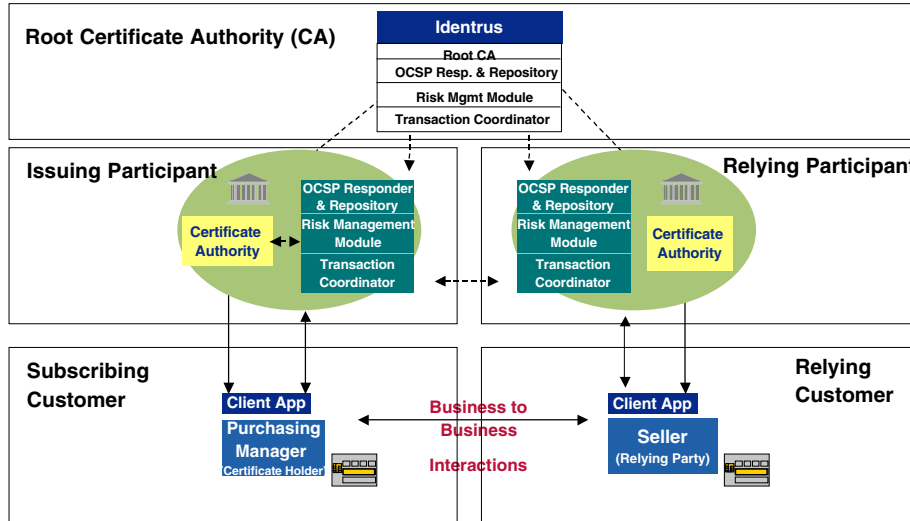
16

Identrus Confidential



# System-wide Roles & Responsibilities

*Contracts & Procedures*



# Participant Update

# Current Participants

- ABBEE NATIONAL GROUP
- ABN AMRO
- AUSTRALIA NEW ZEALAND BANK
- BANCO SANTANDER CENTRAL HISPANO
- BANK OF AMERICA
- BANK OF SCOTLAND
- BANK OF TOKYO-MITSUBISHI
- BARCLAYS
- BBVA
- BNP PARIBAS
- CHASE
- CIBC
- CITIBANK
- COMMERZBANK
- CO-OPERATIVE BANK
- CREDIT AGRICOLE
- DEUTSCHE BANK
- DRESDNER BANK
- HONG KONG SHANGHAI BKG GROUP
- HYPOVEREINSBANK
- INDUSTRIAL BANK OF JAPAN
- ING GROUP
- LLOYDS TSB
- MERITANORDBANKEN
- NATIONAL AUSTRALIA BANK
- ROYAL BANK OF CANADA
- ROYAL BANK OF SCOTLAND
- SANWA BANK
- SEB
- SCOTIA BANK
- SOCIETE GENERALE
- SUMITOMO/SAKURA
- WELLS FARGO

## Key statistics

- 30+ financial institutions
- 133 countries
- 40 million customers
- 100s of technology partners
- 9 participants moving to production
- Multiple end-user pilots
- 30+ end-user applications enabled

# Identrus enabled Applications and Services Alignment

## Current Applications

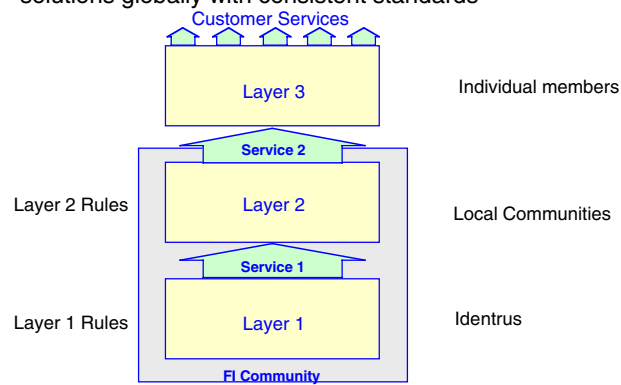
- Pilots underway
  - Cisco – Commercial Leasing
  - Allianz – Insurance Contract Administration
  - Siemens – Online Procurement & Computer Sales
  - ComLease – Equipment Leasing
  - SAP – MySAP – Single Sign-on and STP for ERP
  - eBx – Bill Presentment and Payment

## SIBOS Applications

- 22 applications were demonstrated at SIBOS
- Full product and provider showcase is available at [www.identrus.com](http://www.identrus.com)

# Services Layers

- ❖ Layering of business and application rules on top of Trust to minimize duplication and extend reach as broadly as possible
- ❖ Partnering with providers worldwide to trust enable payments solutions globally with consistent standards

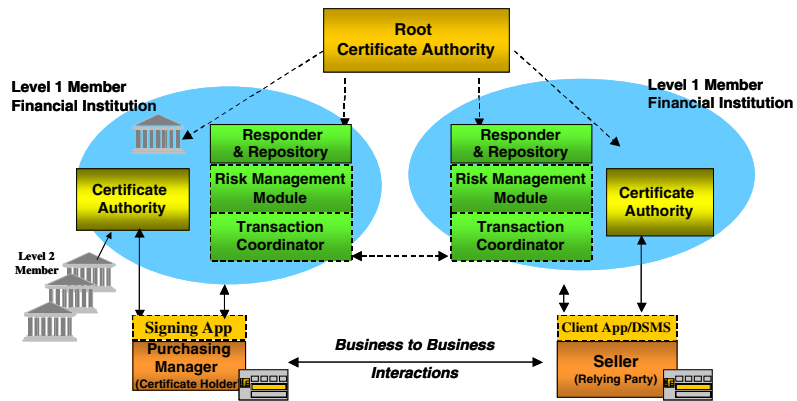


25

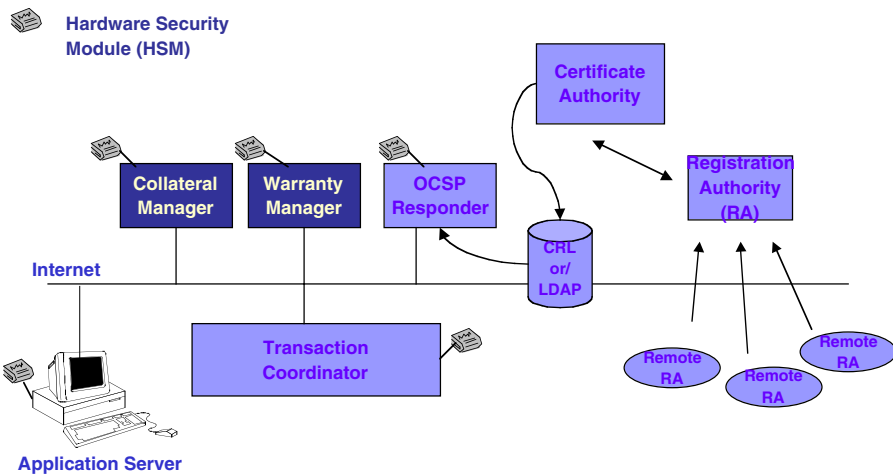
*Identrus Confidential*



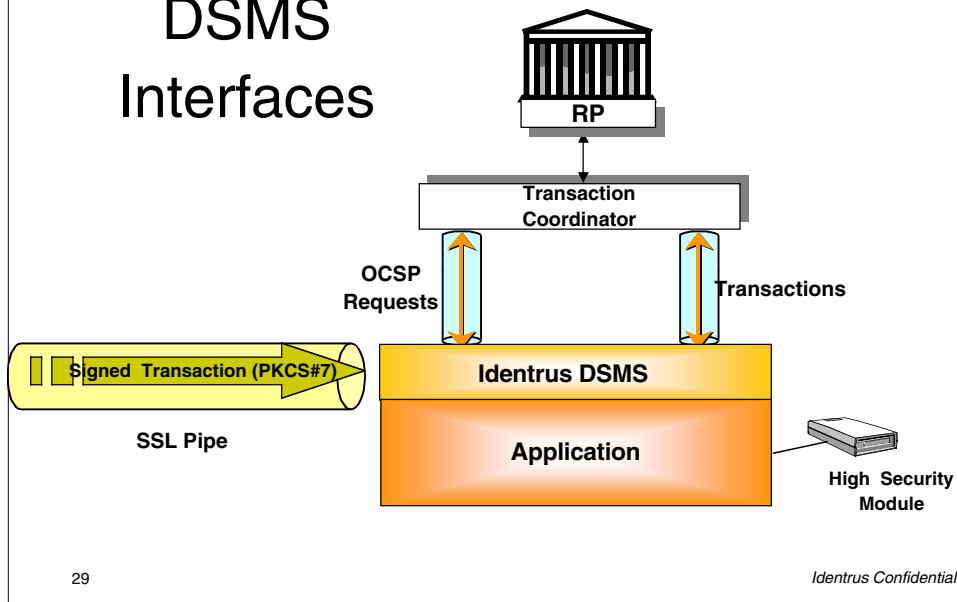
# Technology Architecture



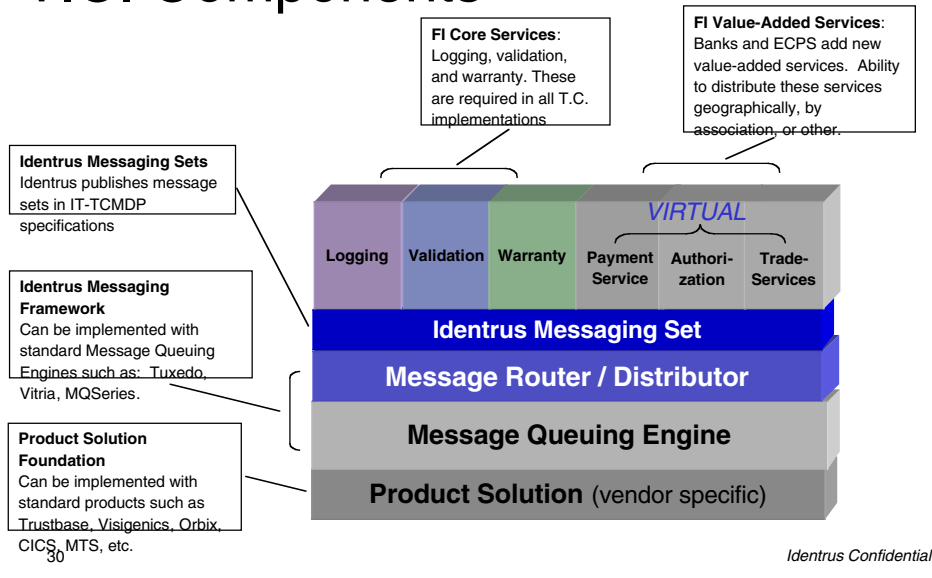
# Level One Participant CA



# DSMS Interfaces



# T.C. Components



# Technology Component Provide

## **HSM**

Chrysalis and nCipher

## **SmartCard Solution with SIR**

Gemplus, Oberthur, Secude, Litronic, ID2

## **OCSP responder**

ValiCert, CA, CertCo

## **TC**

iPlanet, KyberPASS, ValiCert/IBM

## **SecureMail**

Secude, Celo, Entegrity, ValiCert

## **DSMS**

Entegrity, Baltimore

# Infrastructure Components

## **Certificate Authority**

- Provides the core certificate generation and management system for members. These systems, among other things, provide for the secure registration, issuance, and revocation of end-user certificates.

## **OCSP Responder**

- Enables each Level 1 Participant to provide relying parties globally, a real-time status validation on its customers' certificates.

## **Transaction Coordinator**

- Provides the basis for inter-participant messaging, offering a messaging framework that can be leveraged to develop and use value-added Layer 2 services, such as certified payments. The TC further provides the necessary components to capture logging and billing information for participants and Identrus.

## **Warranty/Risk Manager**

- Enables Participants to process, price, and respond to requests for identity assurance by relying parties globally. This system provides the base liability risk tracking and management components for a Participant's customers, its own internal controls, and for reporting into the Identrus Risk Management

## Infrastructure Components

### **Collateral Management Interface**

- Interfaces between Warranty/Risk Manager and Collateral Agent systems to ensure adequate/appropriate levels of collateral are maintained.

### **Hardware Storage Devices for Certificates and Keys (Smart Cards,**

### **HSM's, etc.)**

- Ensures the secure storage of digital certificates and the private keys for customers and end-users. They are used to provide the base signing and signature validation functions at each level within the Identrus system. For end-users, it is envisioned that smart cards will be the dominant form factor.

### **Customer Application Interfaces**

- Enables the secure validation and clearing/processing of certificates received by relying customers from their trading partners. The specific requirements of this system is detailed in the Identrus Digital Signature Messaging Software (DSMS). Identrus Participants are licensed to either build the capability internally or alternatively may obtain an Identrus compliant SDMS from one

