



Who's on the other end of your digital transaction?

Driving Value and Managing Risk in Online Applications

The Identrus business proposition

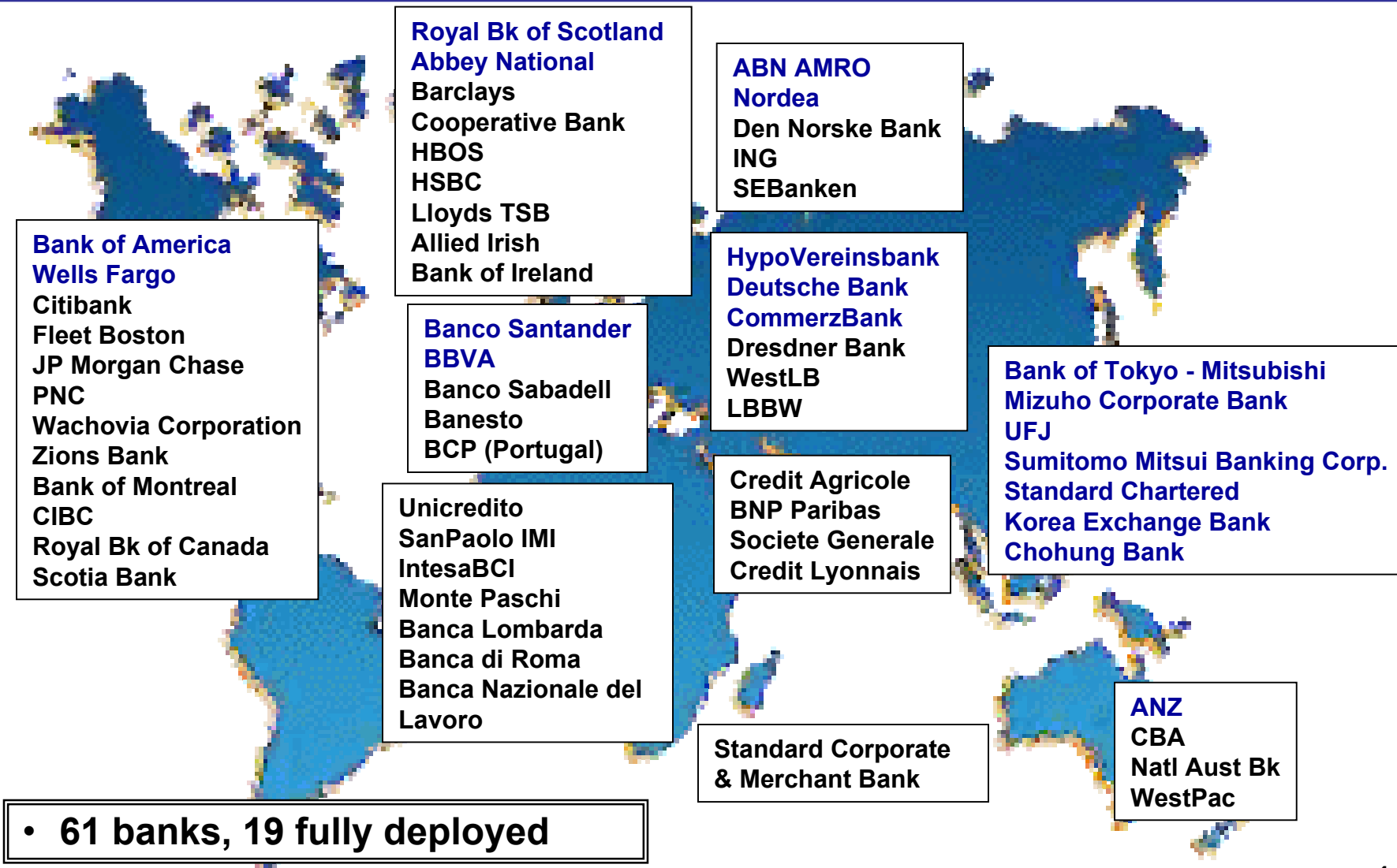
As agents of trust, managers of risk, and enablers of commerce, with local presence and global reach, financial institutions are uniquely positioned to ...

- make globally recognized digital certificates and signatures the enabling capability for secure electronic business, nationally and internationally
- provide consistent Certificate Authority services to buyers and sellers nationally and internationally

Identrus Provides. . .

- ◆ A platform for safe, secure electronic business on a domestic, regional, global scale
- ◆ The only Digital Identity Authentication scheme that is:
 - ◆ Regulated (US Federal Reserve and US OCC)
 - ◆ Bank-centric
 - ◆ Scalable
 - ◆ Interoperable
 - ◆ Policy
 - ◆ Legal
 - ◆ Operational
 - ◆ Technical
 - ◆ Complete, proven and in use today
 - ◆ Addresses critical Operational Risk issues facing financial institutions

Identrus Membership



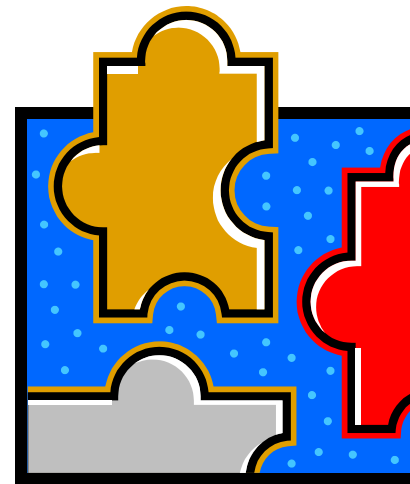
The IdenTrust Rules - The platform for global business interoperability



Global consistency and uniformity are provided through - legal, policy, operational and technology components

- Operating Rules
- Technology standards
- Contract Infrastructure
- Legal dispute resolution procedures
- Arbitration procedures
- Certificate Policies, Practice Statements etc.

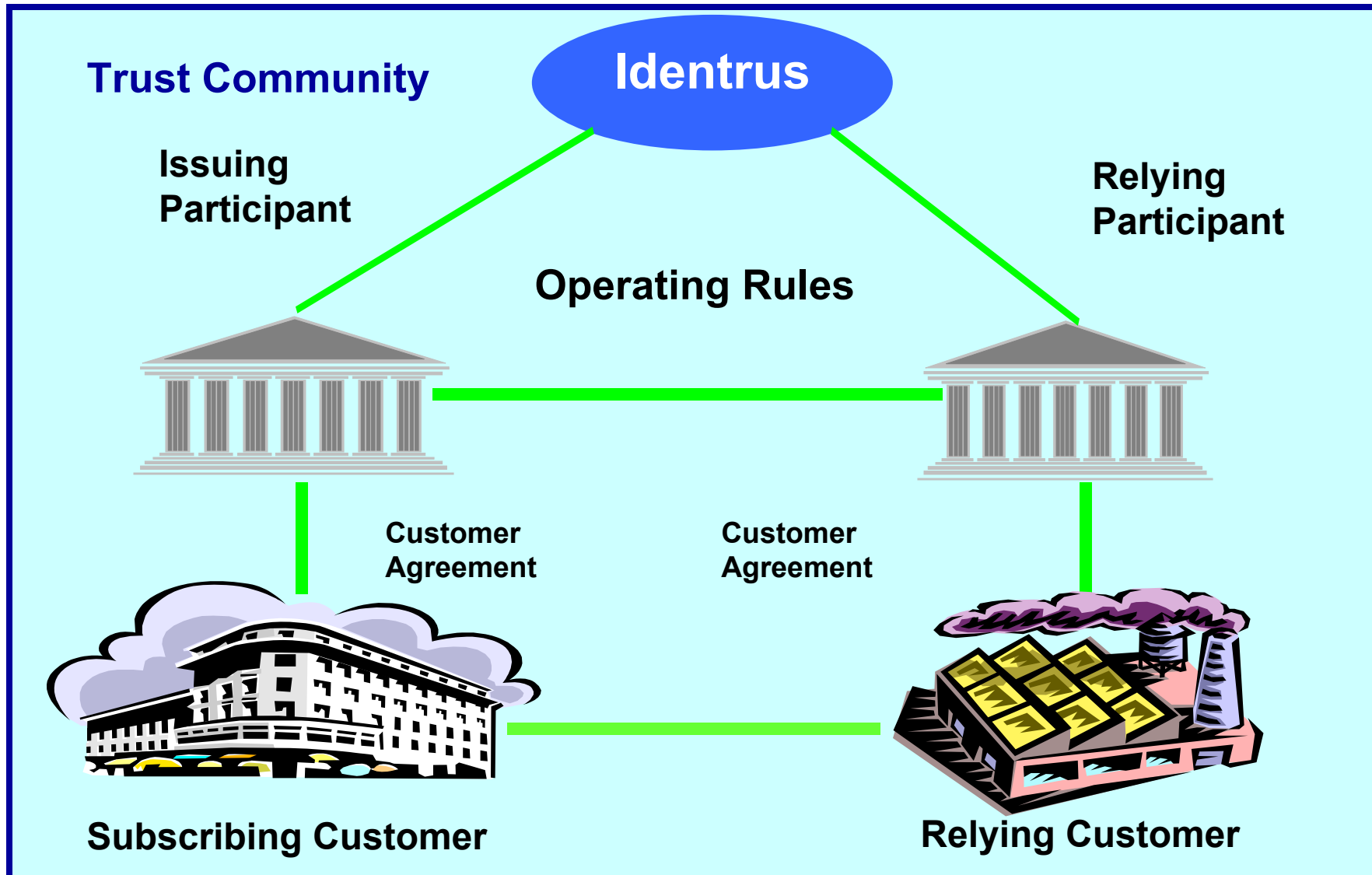
Legal Responsibilities/ Liabilities



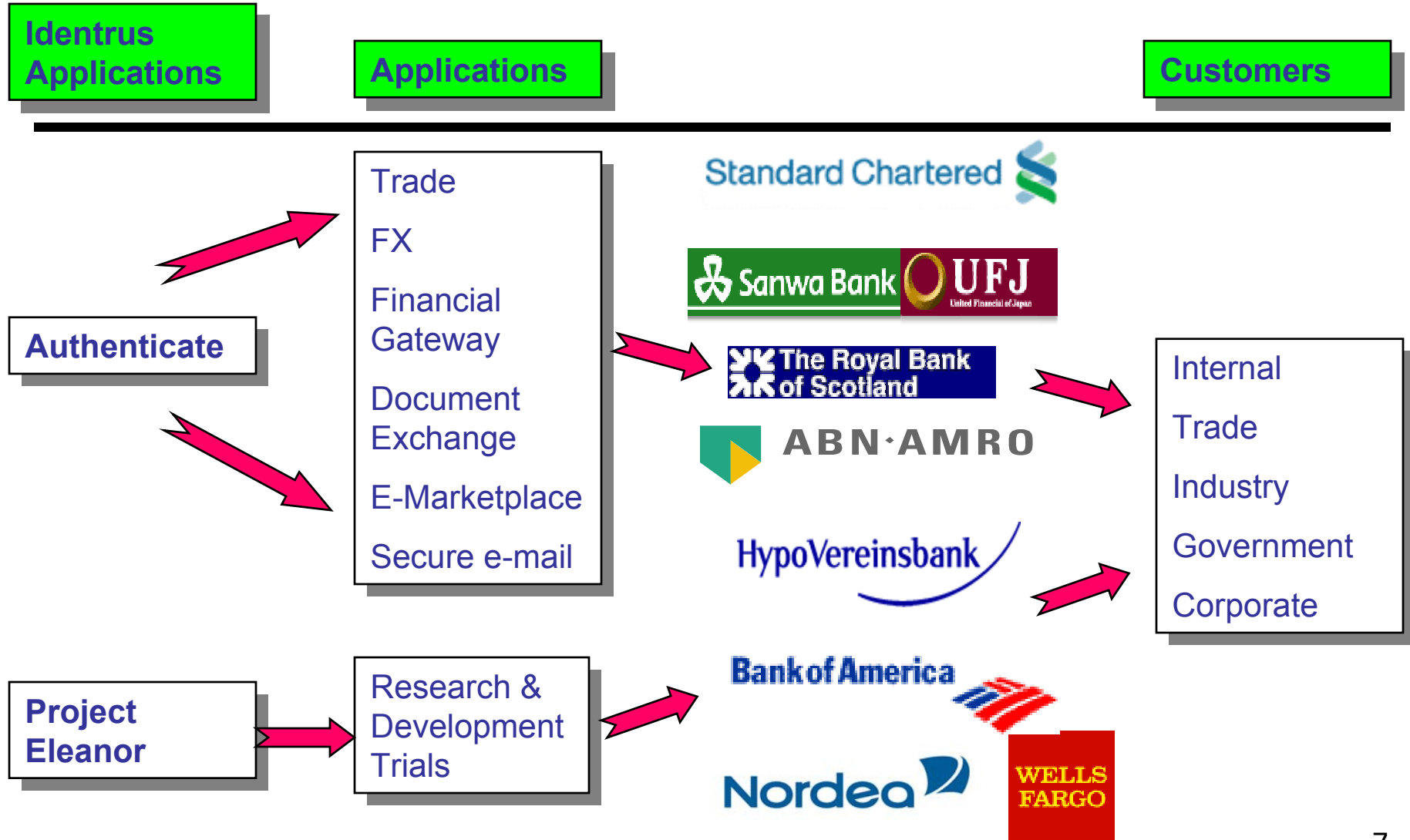
Security/ Technology

Operational Procedures & Practices

Legal interoperability - uniform contract law – domestic, regional, and global



Examples of applications currently being deployed



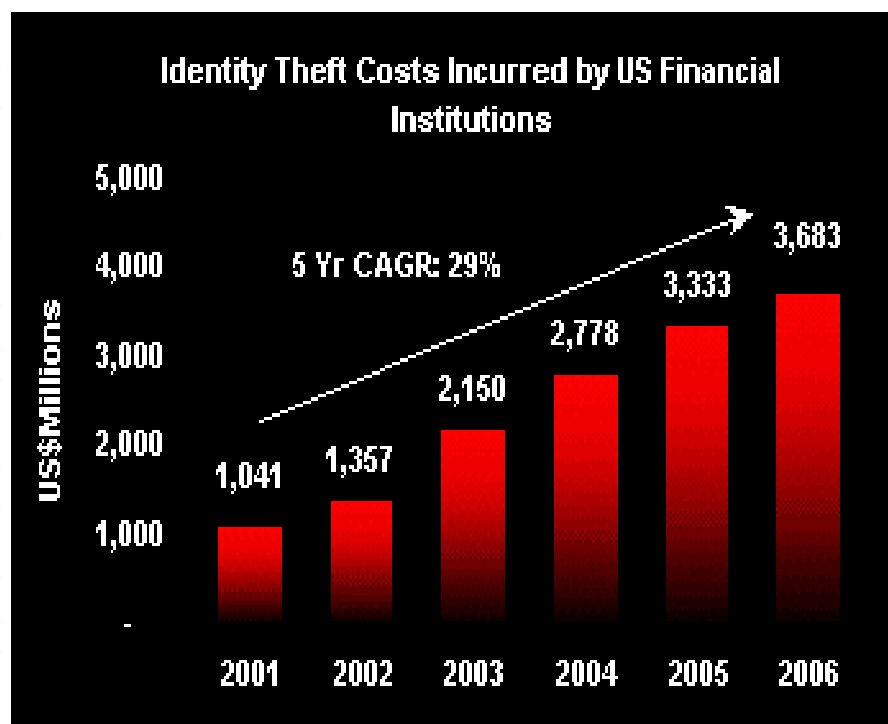
Even traditional bank – customer relationships are not immune to fraud



“At the end of 2001, the financial services industry incurred costs over to \$1 Bn due to Identity theft. We expect this to rise to \$3.4 Bn by 2005”

Source: Celent Communications

Identity Theft in the US



- **Identity theft will cost US financial institutions over \$3 Bn by 2005.** The primary result of the crime is payment fraud, which costs financial institutions billions of dollars a year.
- **The attention presently paid to identity theft on Capitol Hill will ultimately have ripple effects throughout the financial services industry.** Two years ago, the Identity Theft and Assumption Deterrence Act of 1998 established identity theft as its own crime with penalties. Today, regulators are addressing identity theft's impact on the nation, and the role of the financial services industry in preventing it.

Source: Celent Communications: Identity Theft: Protecting the Customer Protecting the Institution
July 31, 2002

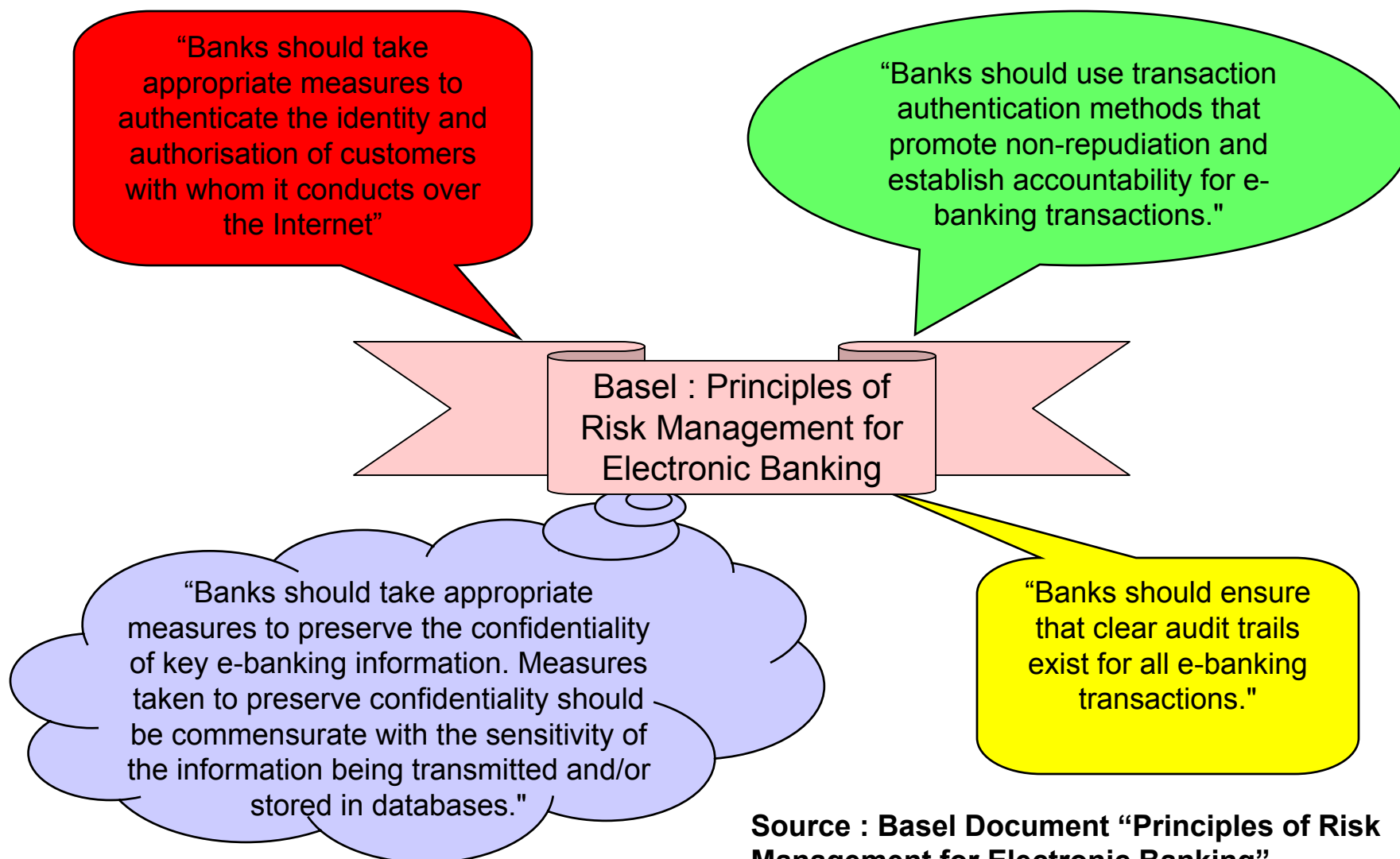
Addressing Risk

- Financial institutions (especially banks) are uniquely placed to address 'risk'
- Risk increases rapidly with the number and diversity of 'schemes' embraced
- Complexity costs money – if the solution isn't simple, reliable and easy to use – it won't be
- The Internet doesn't recognise geographical boundaries and legal jurisdictions

Risk, Nothing New to Financial Services

- Credit Risk
- Market Risk
- Basel Accord of 1988
 - Established the standards for credit risk and market risk across entire banking sector
 - Standardized capital reserve requirements
- Basel II
 - Addresses risks associated with automating processes
 - Operational Risk Management

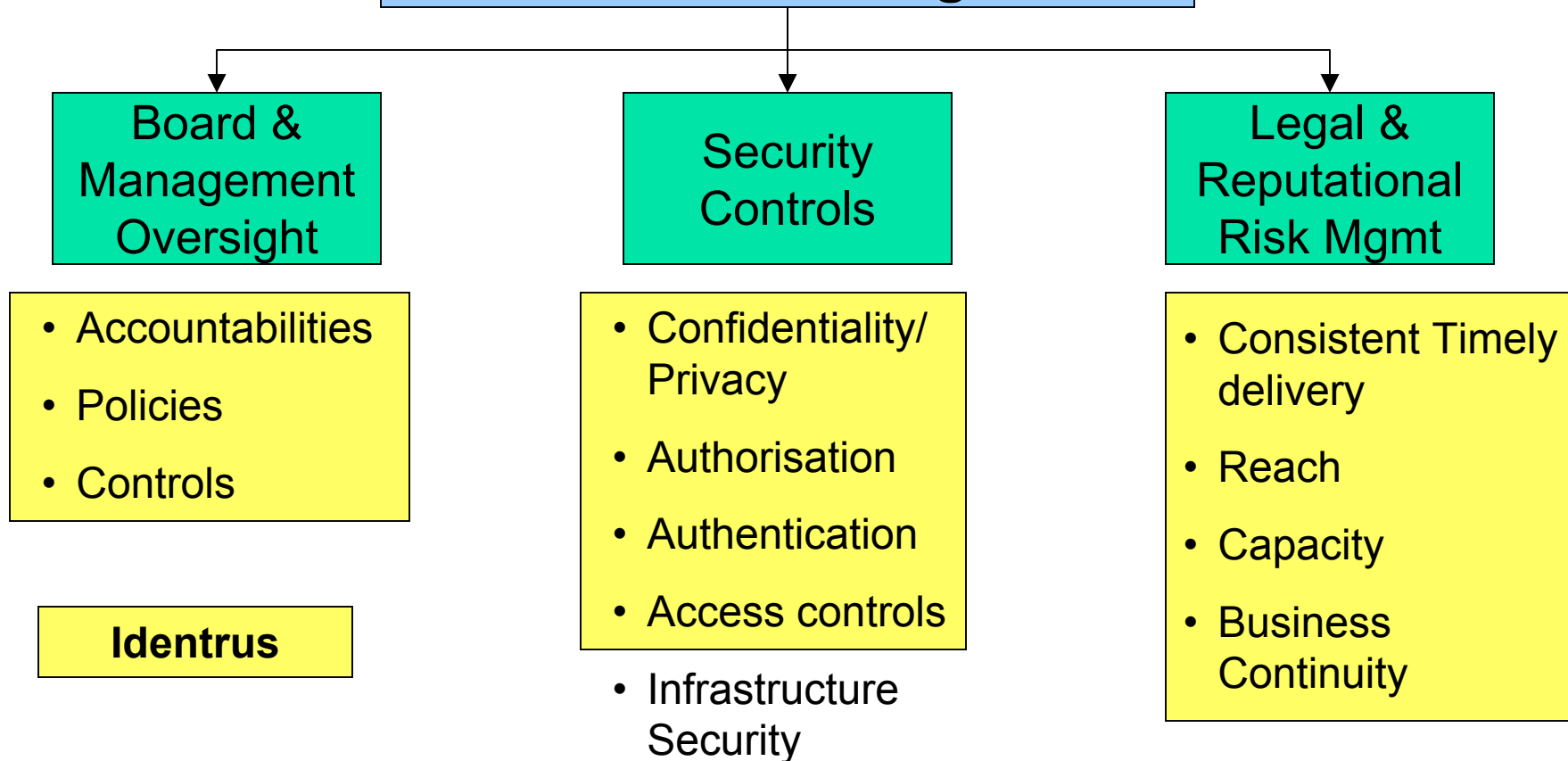
The complementary nature of Identrus, Basel and Operational Risk Management



Source : Basel Document "Principles of Risk Management for Electronic Banking"

The Impact of the Basel Accord

Risk Management Principles for e-banking



Identrus...

- Provides banks and their national regulatory agencies with the framework for managing identity risk
- Provides a truly global business infrastructure, within a closed system, with liability allocated by contract and system-wide risk management
- Provides a scalable infrastructure eliminating the need to “bridge” different, bank-centric PKIs and the ongoing audits of each individual scheme
- Provides framework to address Operational Risk
- Is complete, proven and in use
- Offers cost-effective options to begin moving today

In conclusion...

- ◆ Banks understand
 - ◆ There is significant value in a regulated and standardized framework for digital identity management
 - ◆ There is little competitive advantage at the infrastructure level
 - ◆ Real value comes from focus on usage, customer acquisition and service
 - ◆ Not moving toward standardization has a price
 - ◆ Replication of effort
 - ◆ Increased risk profile
 - ◆ Greater capital reserve requirements



Clay.Epstein@identrus.com