International Telecommunication Union

Higher Assurance Authentication for the Enablement of Federated On-Line Trust

Abbie Barbir, PhD
ITU-T Study Group 17
Rapporteur, Identity management
Abbie.Barbir@ties.itu.int

draft

Scope

- Overview of International Telecommunication Union(ITU-T) Study Group 17 (SG 17)
- Overview of Entity Authentication Assurance
- Enhancing Cybersecurity through Open Trust Frameworks
- Some Legal concerns
- Conclusions

I T U - T G e n e v a

ITU-T Overview

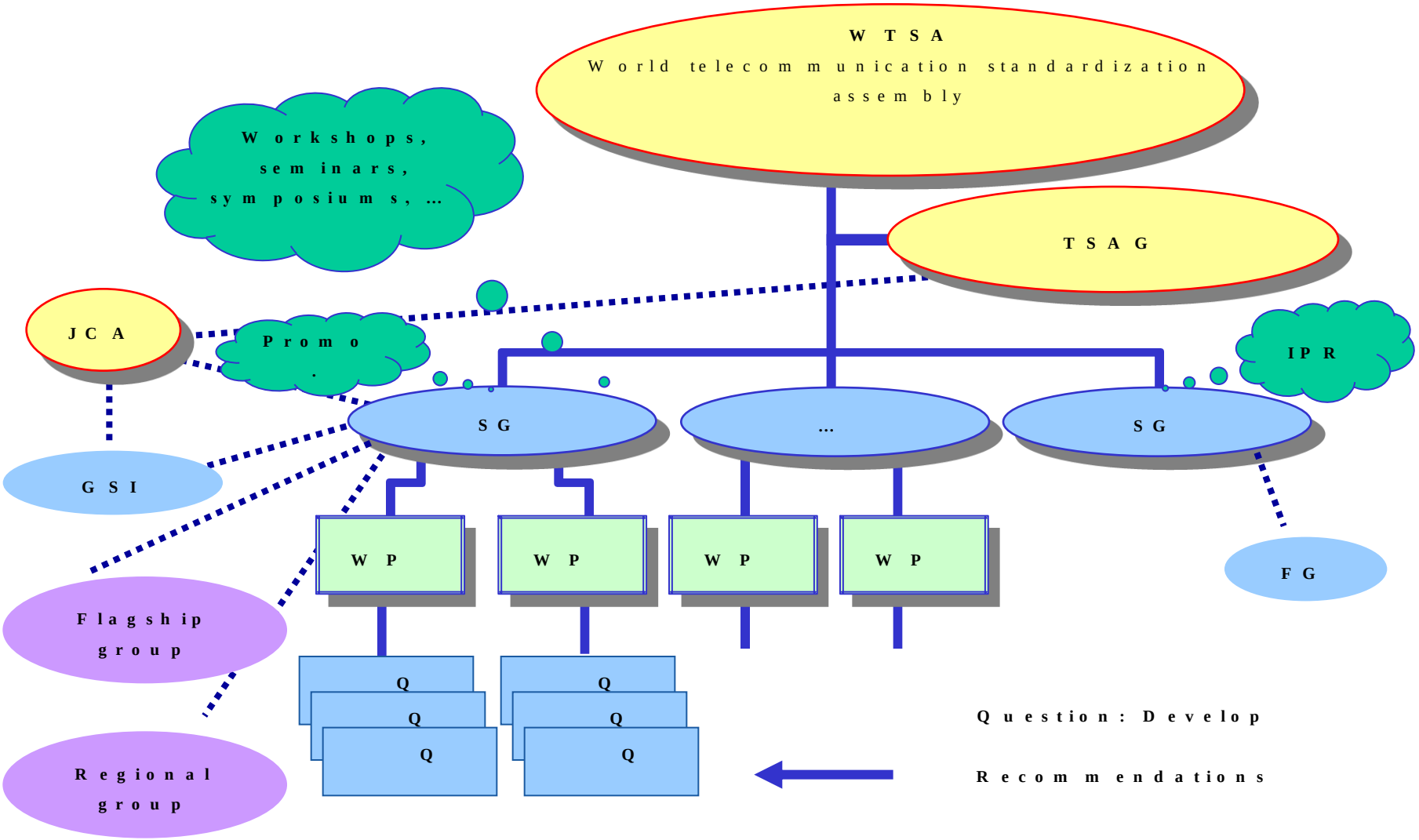
History

- Established 17 May 1865
- CCIF and CCIT formed in 1924 and 1925, merged into CCITT in 1956, became ITU-T in 1992
- Decisions by consensus (voting almost never occurs)
- Participation through national Government channels
- Telecom does not mean that focus is only on Telecom

Mission and Legal Status

- **Mission**
  - study technical, operating and tariff questions and issue non-binding international standards to ensure compatibility of standards on worldwide
- **Legal Status**
  - UN specialized agency
  - Legal base: Constitution and Convention; have treaty status among the signatory states
  - 192 UN Member States are signatory members
  - Approx. 700 Sector Members (operators, manufacturers, etc.)

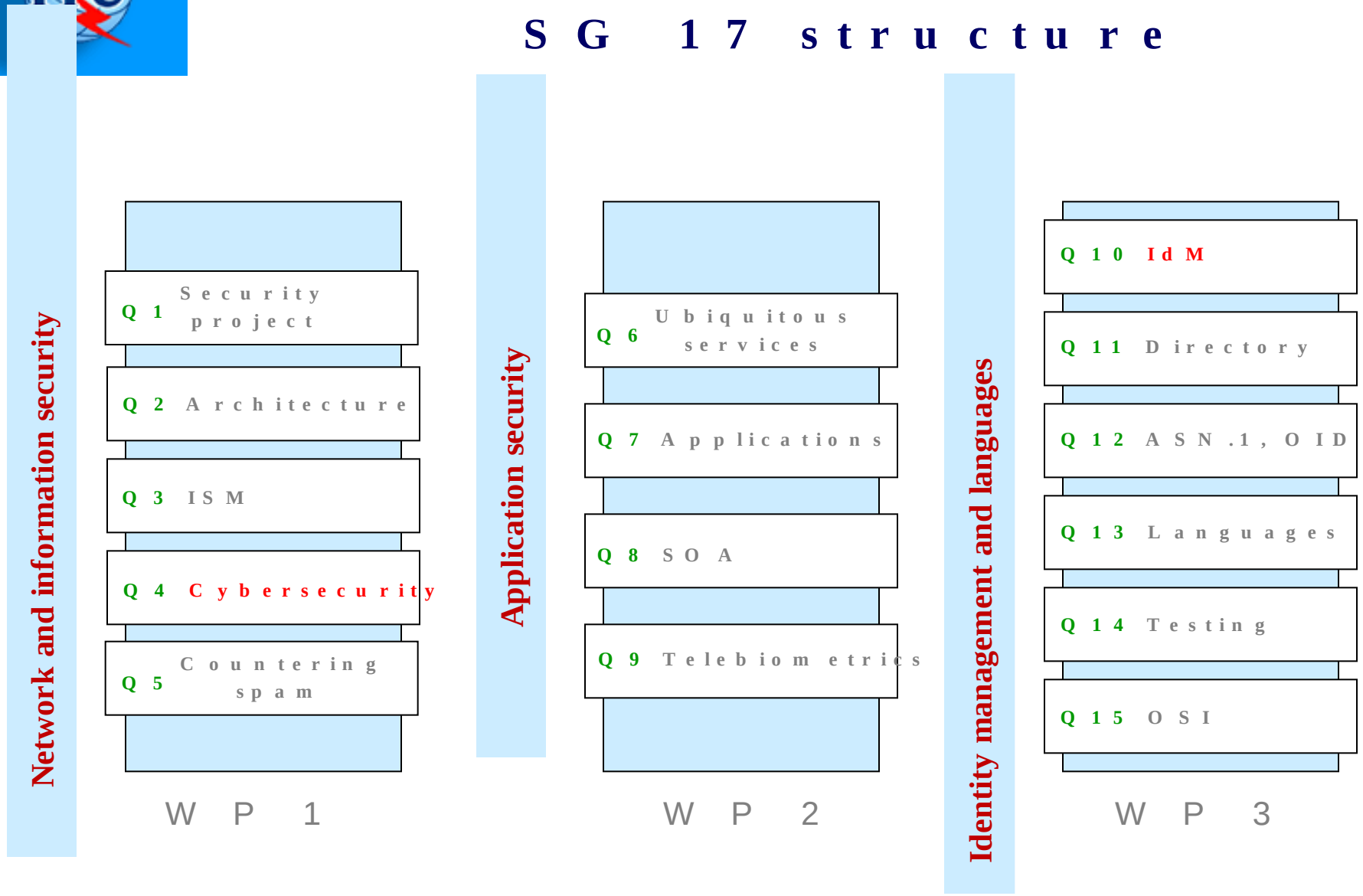
ITU-T Structure



Study groups (2009-2012)

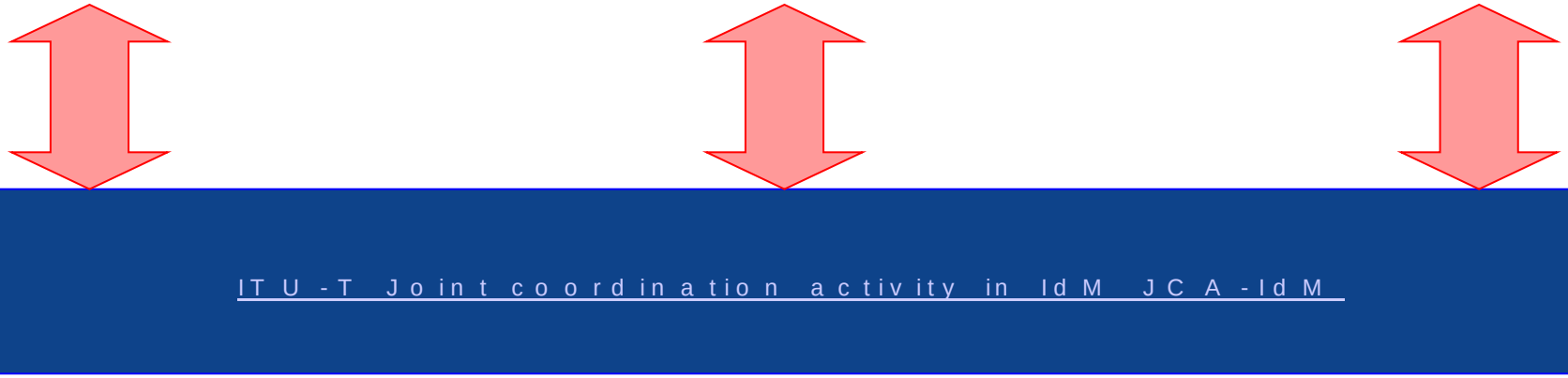
SG 2	Operational aspects of service provision and telecommunications management
SG 3	Tariff & accounting principles including related telecommunication economic & policy issues
SG 5	Environment and climate change
SG 9	Television and sound transmission and integrated broadband cable networks
SG 11	Signalling requirements, protocols and test specifications
SG 12	Performance, QoS and QoE
SG 13	Future networks including mobile and NGN
SG 15	Optical transport networks and access network infrastructures
SG 16	Multimedia coding, systems and applications
SG 17	Lead study group on telecom security, identity management (IdM) and languages

SG 17 structure



Q 10/17 collaboration on identity management

Advancing open standards for the information society



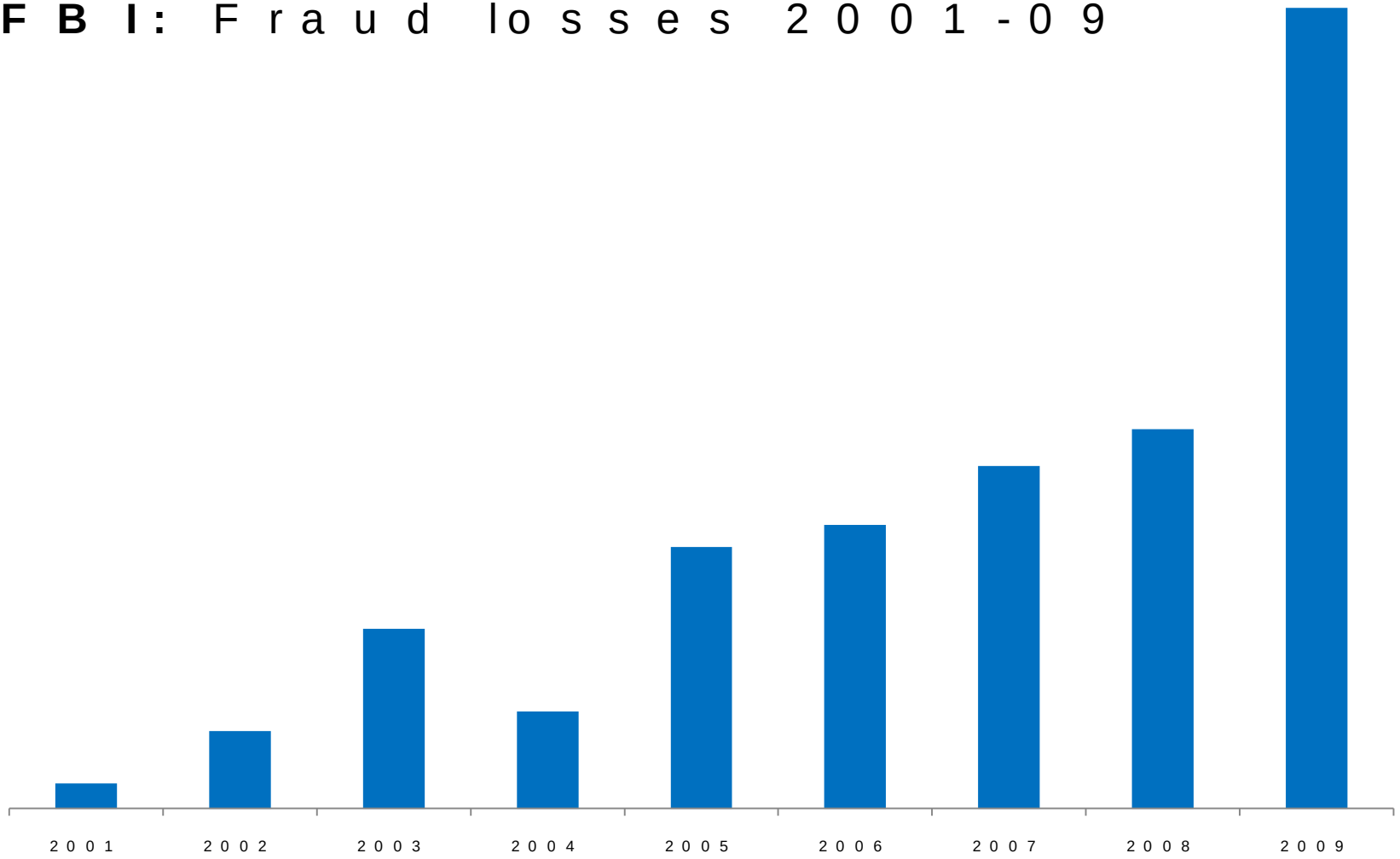
IdM Drivers

- For Financials
- Meeting customer needs
  - Safe, secure
  - Simple, seamless, convenient access
  - Active customers

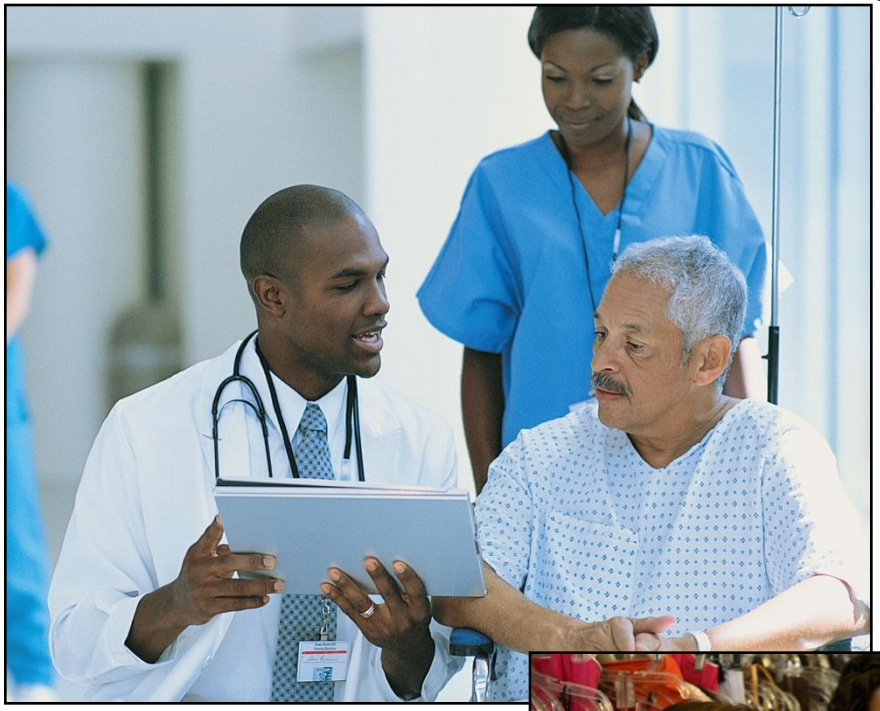
The threat: Cyber crime

Cyber crime losses are growing

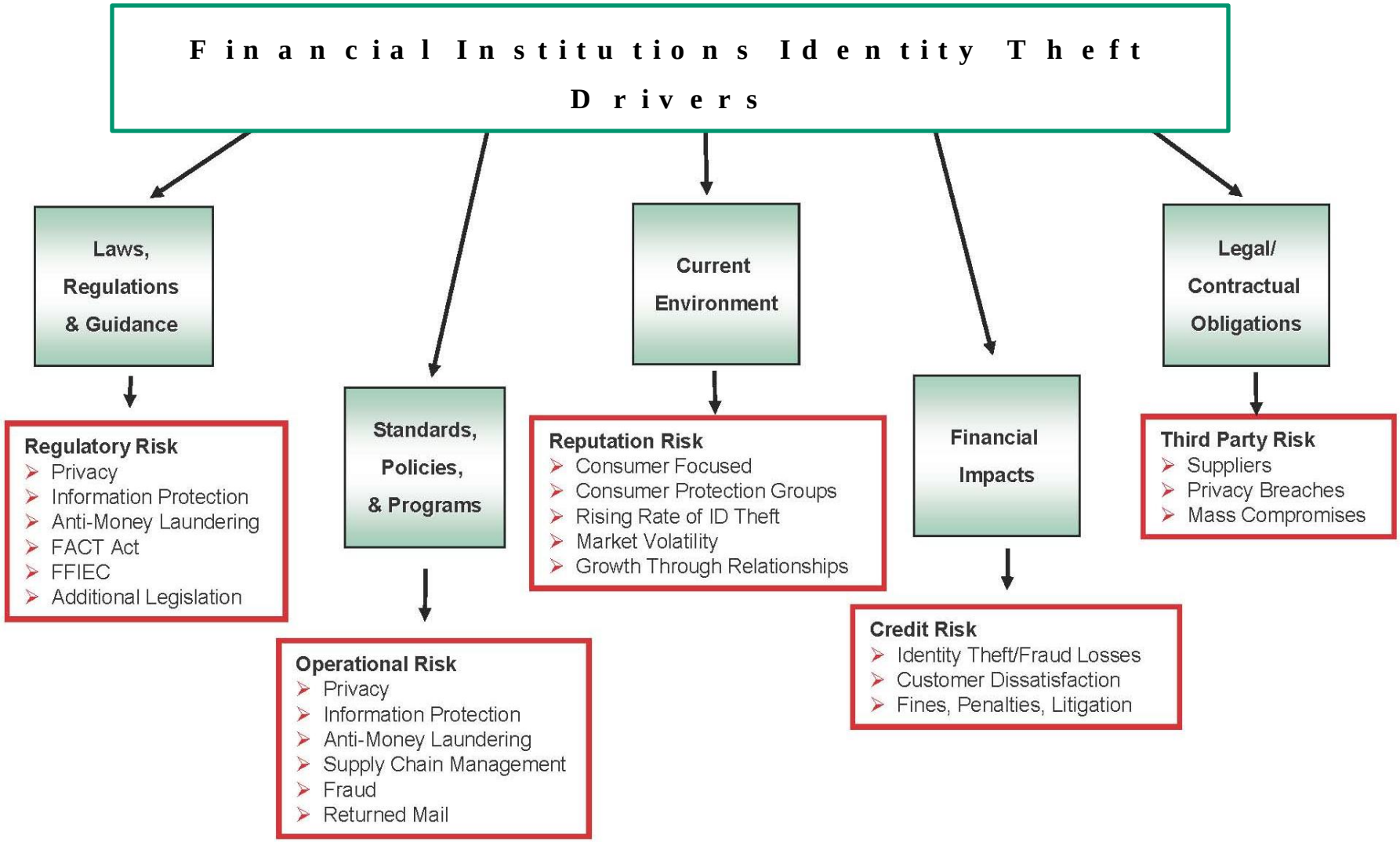
FBI: Fraud losses 2001-09



Identity crime affects all sectors



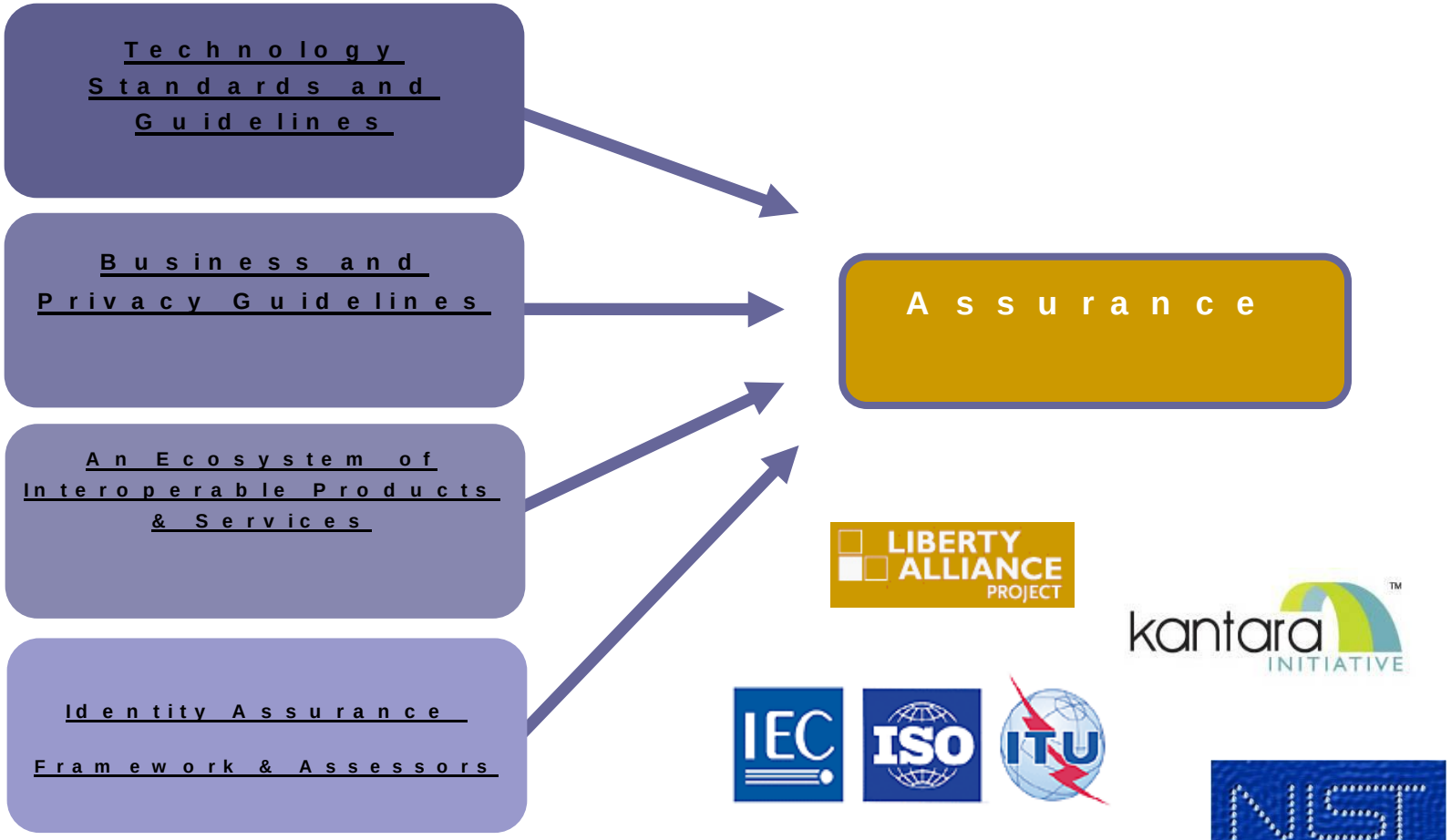
Identity Management Drivers



Q 1 0 focus is Towards

Strong Identity, Portable Reputation and Enhanced Trust

Need for Better Identity Assurance



Q 10/17

Entity Authentication Assurance

- Joint work with ISO JTC 1/SC 27/WG 5 and ITU-T SG 17/Q 10
- Standardizes four Levels of Assurance (LoAs)
  - to promote trust,
  - improve interoperability, and
  - facilitate identity federation across organizations and borders

Why do the work?

- Provides a consistent basis for trust
- Promotes identity federation
- Enables credential re-use in different contexts
- Promotes efficiency and reduces costs
- Enables cross-organization and cross-border services
- Provides framework for further standardization
- Establish foundation for liability and other legal aspects
- Brings together existing work in this area and will not "re-invent the wheel":
  - Kantara Initiative, ITU-T, NIST standards efforts
  - New Zealand, Australian, U.S., European, and Canadian e-government efforts
  - EU research efforts (STORK, IDABC, etc.)

Case Study: The Problem

- Most U.S. government agencies want to offer more online applications to citizens:
  - Research, grant proposals, taxes, benefits, data sharing
- Authentication is a large barrier to deployment:
  - There is no universal citizen credential
  - Application-specific credentials are difficult and expensive:
    - Identity proofing
    - Forgotten passwords from infrequent usage
    - Help desks and other maintenance overhead
    - Multiple collections of personally identifiable information (PII)

Possible Solutions

- Government agencies can act as the Relying Party (RP) rather than the Identity Provider (IdP) and accept credentials issued by "trusted" external organizations
- Standard is used to develop Trust Framework Adoption Process, that defines IdSP requirements for the LoAs
  - Started an IdP certification program based on the Trust Framework
- NIH pilot studies to use open standards credentials from several certified IdPs

X.eaa Scope

- ISO/IEC 29115 | ITU-T X.eaa provides a framework for managing entity authentication assurance in a given context. In particular, it:
  - specifies four levels of entity authentication assurance;
  - specifies criteria and guidelines for each of the four levels of entity authentication assurance;
  - provides guidance concerning controls that should be used to mitigate authentication threats;
  - provides guidance for mapping the four levels of assurance to other authentication assurance schemes;
  - provides guidance for exchanging the results of authentication that are based on the four levels of assurance.

Structure and Contents

- Four Levels of Assurance
- Entity Authentication Assurance Framework
  - Human and non-human
- Management and Organizational Considerations
- Threats Based on Framework Components
- Required Controls for Each LoA
- Privacy and Protection of PII
- Operational Service Assurance Criteria

4 Levels of Assurance

Level	Description
1 - Low	Little or no confidence in the asserted identity
2 - Medium	Some confidence in the asserted identity
3 - High	High confidence in the asserted identity
4 – Very High	Very high confidence in the asserted identity

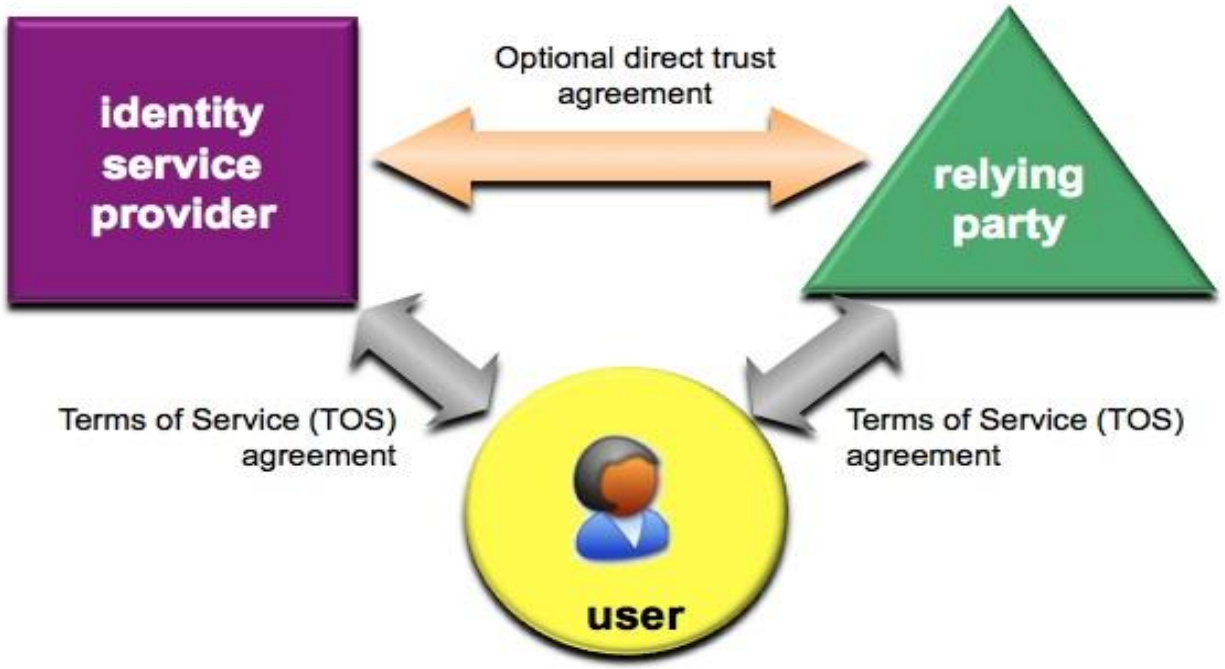
What consumers are willing to give-up

- Move from anonymous to identity enabled
- Internet transactions are still anonymous or low trust
- Value transactions are widely identity based
- Enable Identity while protecting privacy (PII)
  - Isolation of Issuer and target Identity
  - Enable the right to forget
  - Identity dashboard for user to keep control identity
- Enable audit, accountability and policy enforcement

Some Implications

- Simplify the Task of Authentication
  - who are you (context based)
- Attributes
  - what are you
  - This is where the beef is
- Proof of validity
  - ID Source and/or Reputation
- Towards Open Identity Trust Frameworks
- Need better understanding of |Legal Issues and liabilities
- How about consumer protection?

Current Basic "Trust Triangle"

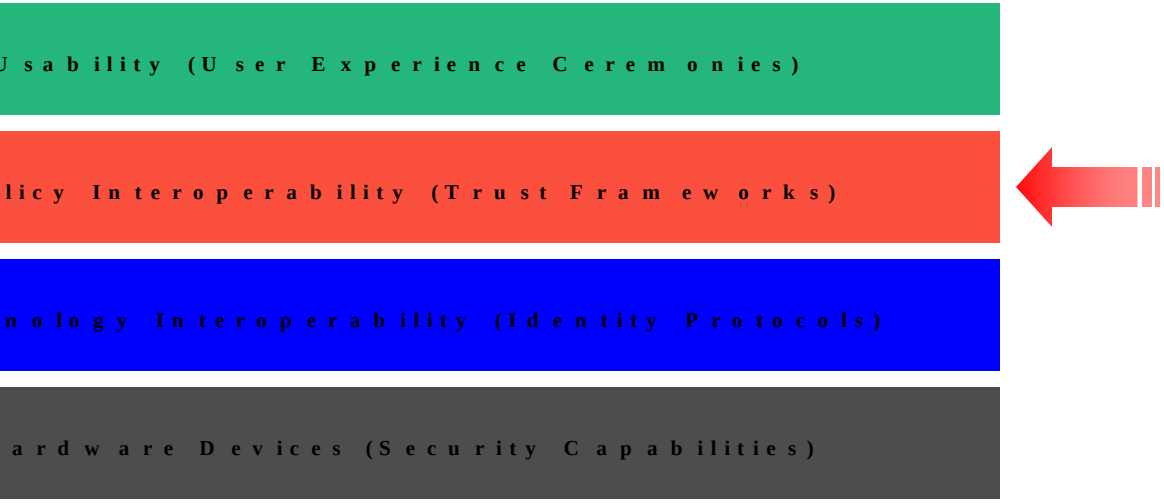


- User has direct trust relationship with IDSP and RP
- How can the IDSP and RP trust each other?

* Source OIX

Where trust Frameworks Fit

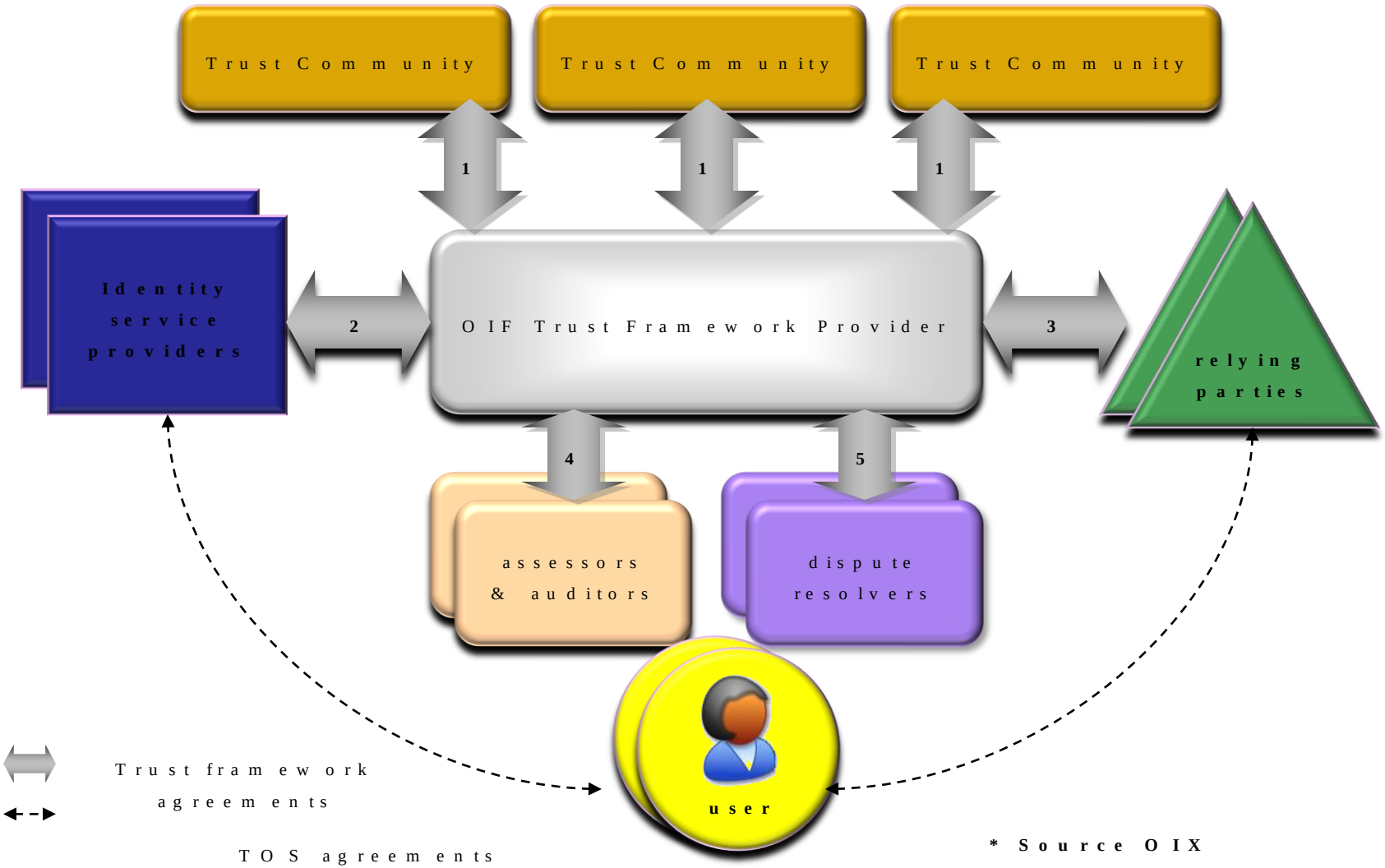
Market Expansion & Adoption



Internet Identity Layer

* Source OIX

Open Identity Framework Model



* Source OIX

How Can UNCITRAL Help

- Identify possible legal issues and determine how they relate locally and internationally
- What are the liabilities of IdSP and RPs
- What are the legal requirements for trust among the participants
- How can this be enforced across international boundaries

Conclusions

- Strong Identity and higher assurance authentication is key for enabling online trust and enhancing Cybersecurity
  - Interoperable federated frameworks
  - Multiple methods
  - End-to-end identification
  - Higher-level authentication
- Need for better National and International understanding legal and assume liabilities and polices

Acknowledgements

- Some slides are based on presentation on X.eaa by the editor ISO editor Erika McCallister and the ITU-T Editor Richard Brackney
- Some Slides are based on presentation on OIX by Don Thibeaux