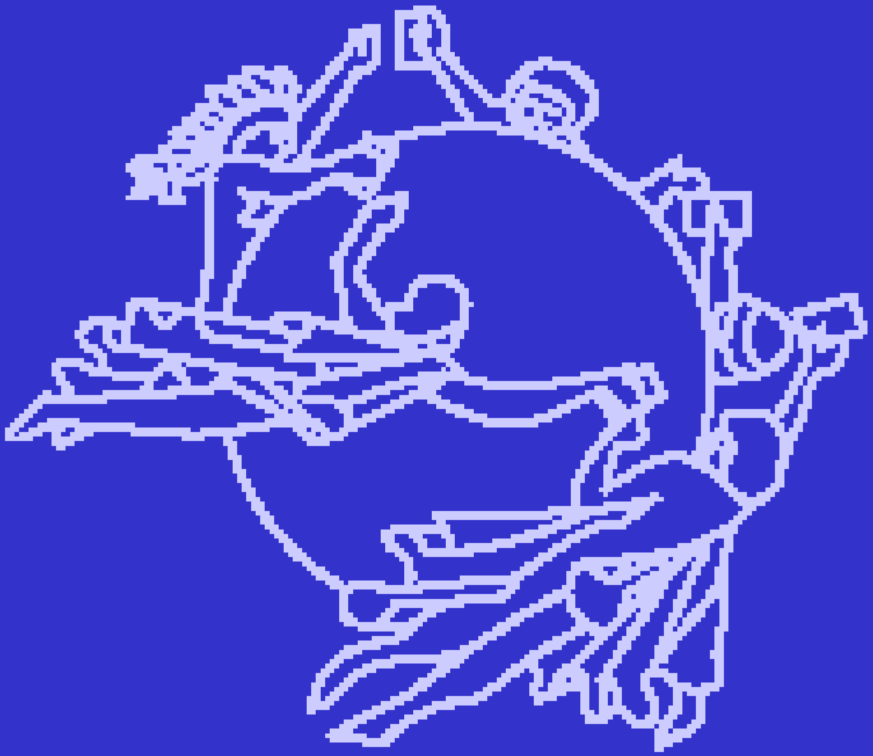
The Universal Postal Union
(The real THE Post Office)
global Postal Trust Services



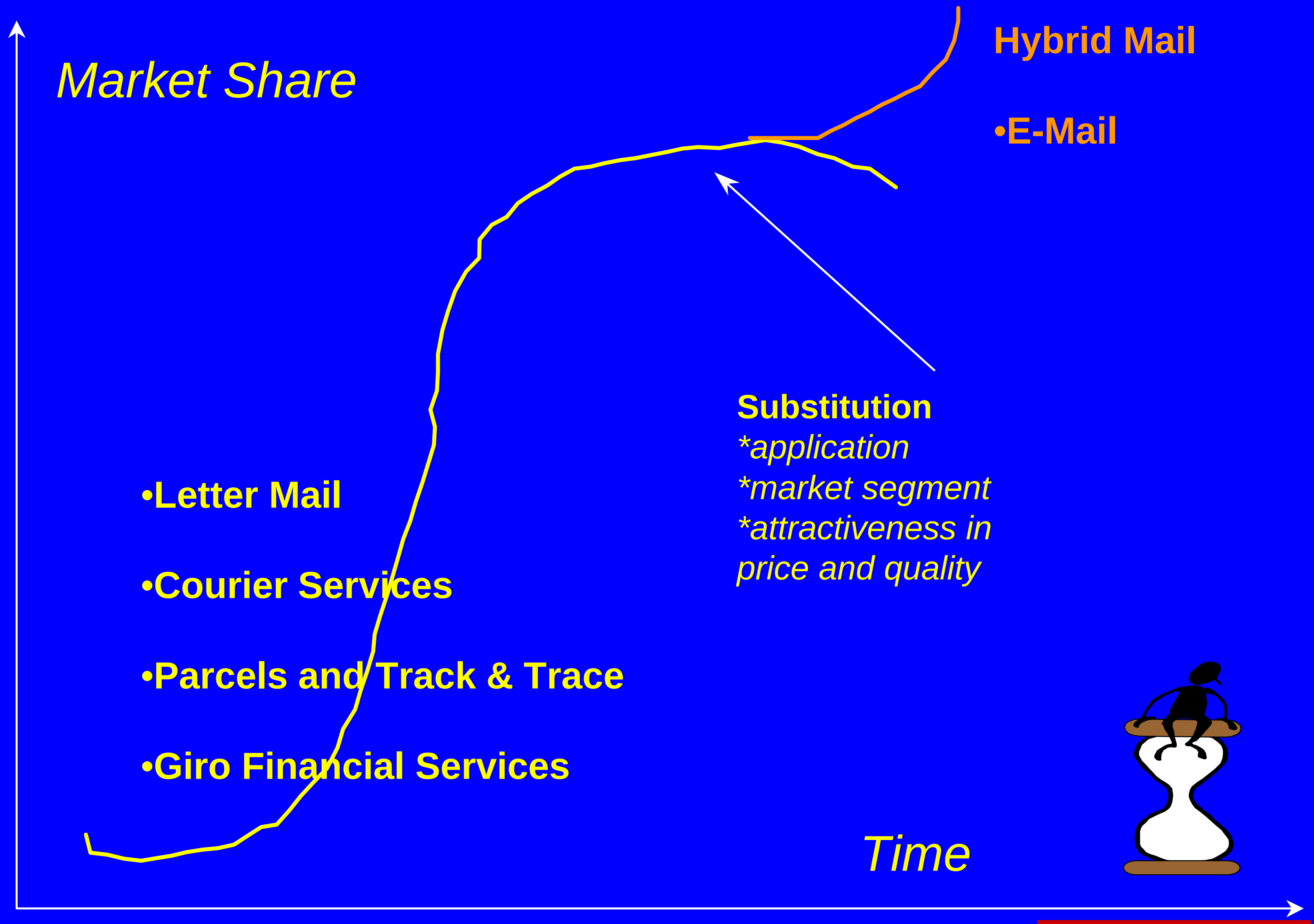
Martin Roe
roem@postoffice.co.uk

Presentation Objective

To provide an understanding of current Postal Joint Electronic Commerce and Trust Service initiatives.

Developed by individual Post Offices; facilitated and supported by the UPU

Why? Current Services and Business Issues



Hybrid Mail

- **E-Mail**

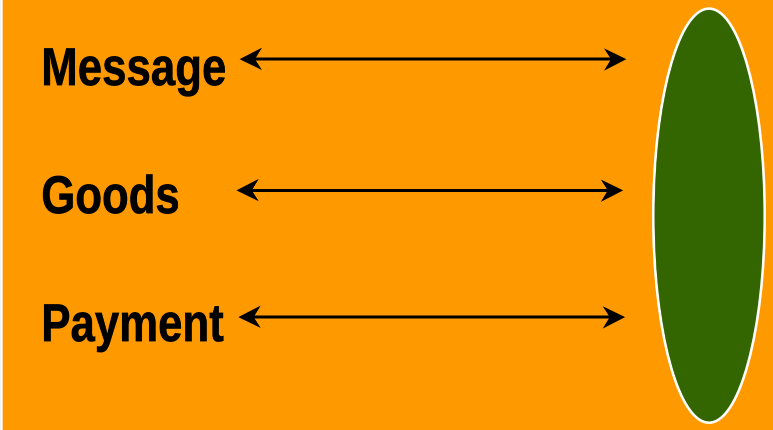
- **Letter Mail**
- **Courier Services**
- **Parcels and Track & Trace**
- **Giro Financial Services**

Substitution
**application*
**market segment*
**attractiveness in price and quality*

Example Postal Electronic Services Strategies

Business model examples from members

Sweden, Eire, Nordic Bloc



Full integration of messaging, financial transactions and logistics fullfillment of delivery and distribution

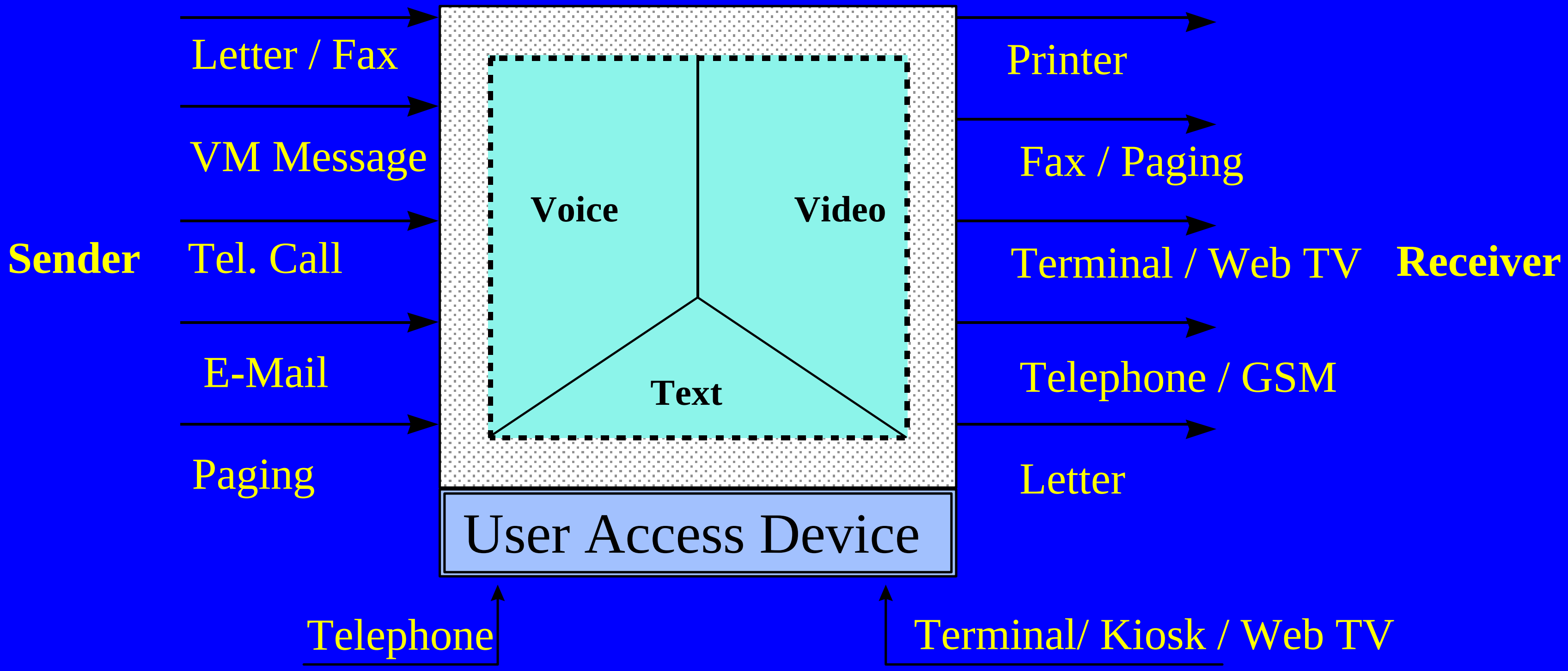
our common business context

End-to-End Communication distribution & Electronic Commerce

THE POST OFFICE

Trend 1 - End to End Communications
Our Functional View

THE VIRTUAL MAILBOX



Sender

Letter / Fax

VM Message

Tel. Call

E-Mail

Paging

Voice

Video

Text

User Access Device

Printer

Fax / Paging

Terminal / Web TV

Telephone / GSM

Letter

Receiver

Telephone

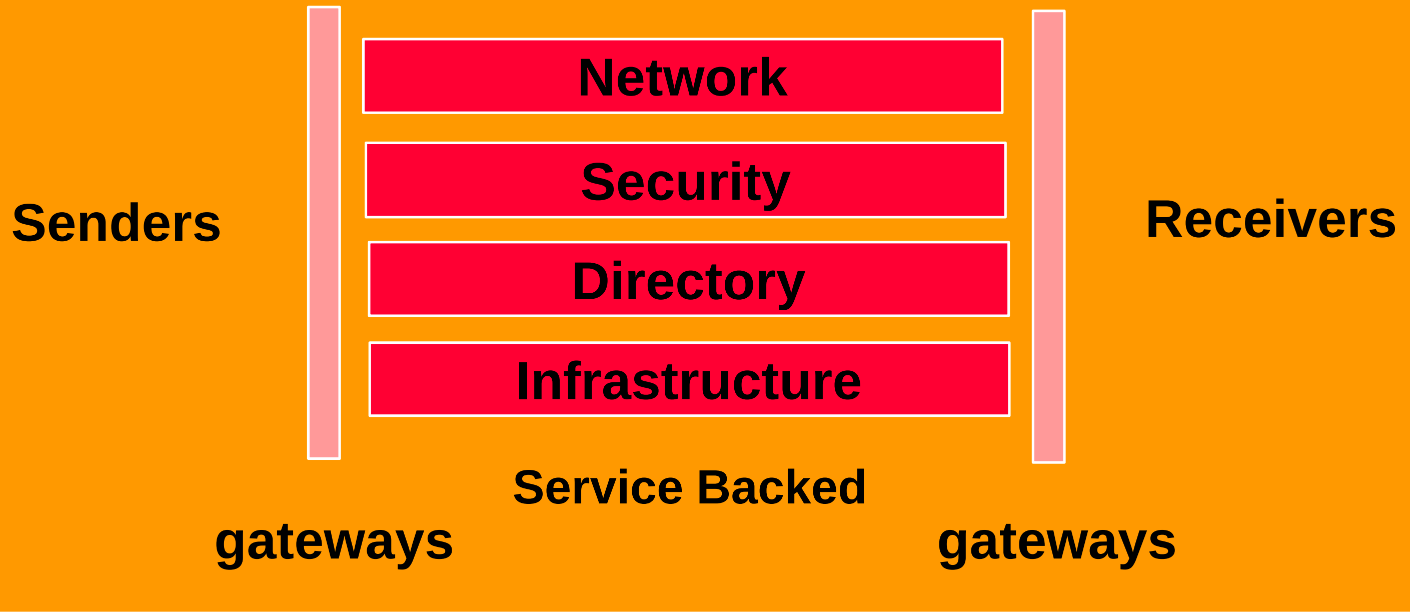
Terminal/ Kiosk / Web TV

INTEGRATION INTEGRATION INTEGRATION

Example Postal Electronic Services Strategies

Business model examples from members

UK , Canada, Australia, and probably many more



Senders

Network

Security

Directory

Infrastructure

Receivers

Service Backed

gateways

gateways

our common business context

End-to-End Communication distribution & Electronic Commerce

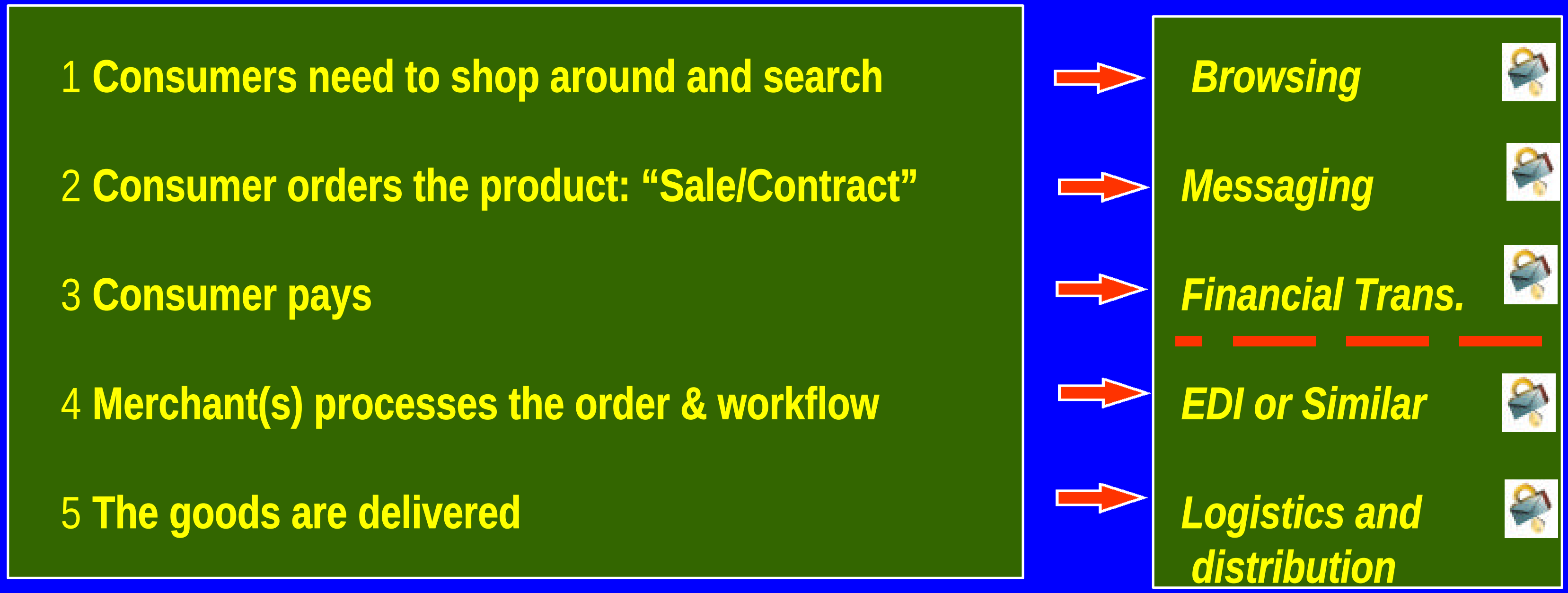
Trend 2 - Electronic Commerce
Our Functional View

Fully integrating the display, finance, workflow & logistics of a business transaction electronically.

The general business processes of commerce

Traditional Commerce

Electronic Commerce



1 Consumers need to shop around and search

2 Consumer orders the product: “Sale/Contract”

3 Consumer pays

4 Merchant(s) processes the order & workflow

5 The goods are delivered

Browsing

Messaging

Financial Trans.

EDI or Similar

Logistics and distribution

– – *Customer visibility line*

= *Trust Services*

Elements in theTrust Chain

People

- Usually represented by their names.
- Can make assertions through the use of digital signature

Computers

- Verify transmissions and authenticate the origin

Organisations

- Collections of the above by granting memberships and credentials; bind names to addresses

Weaving a Web of Trust: Kahre and Rifkin

The Challenge

The overall challenge facing all of us is the globalisation of end to end communications and global electronic commerce frameworks.

There is a need for harmonisation of business practicies and compatability between systems.

The OECD Guidelines

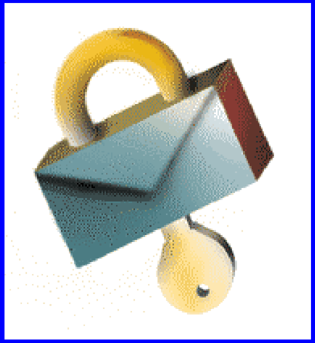
States:

Cryptographic methods and Services should be trustworthy in order to generate confidence in the use of information and communications systems.

The Challenge

Trust is therefore a major foundation of eCommerce.

UPU role and Objective:
To facilitate the establishment of global Postal Electronic Commerce Infrastructures and ensuring the compatability between Postal systems.



Working Group Participants

global Postal Trust Services Project, using PKI and Cross Border Cross Certification Services.

Australia	Belgium	Canada	Finland
France	Indonesia	Ireland	Italy
Netherlands	Norway	Singapore	Sweden
UK	USA	Hong Kong	

In the process of joining:

Japan, Spain, Germany, Malaysia and Portugal

Areas addresed by the group

Policy:

to secure a minimum level of authentication policy comptatbility

Legal:

to ensure legal recognition and validity

Technical:

to establish standard interfaces to the global Postal Trust Services

Business:

to address applications, market intelligence and standards

Legal issues

What we have done:

* Scanned and reported findings about the current government legislations, working parties and international projects such as ABA, ICC, UNCITRAL & OECD.

* Provided an an implementation check list to avoid legal liability.

What we have learned:

- The Trust Model is critical.

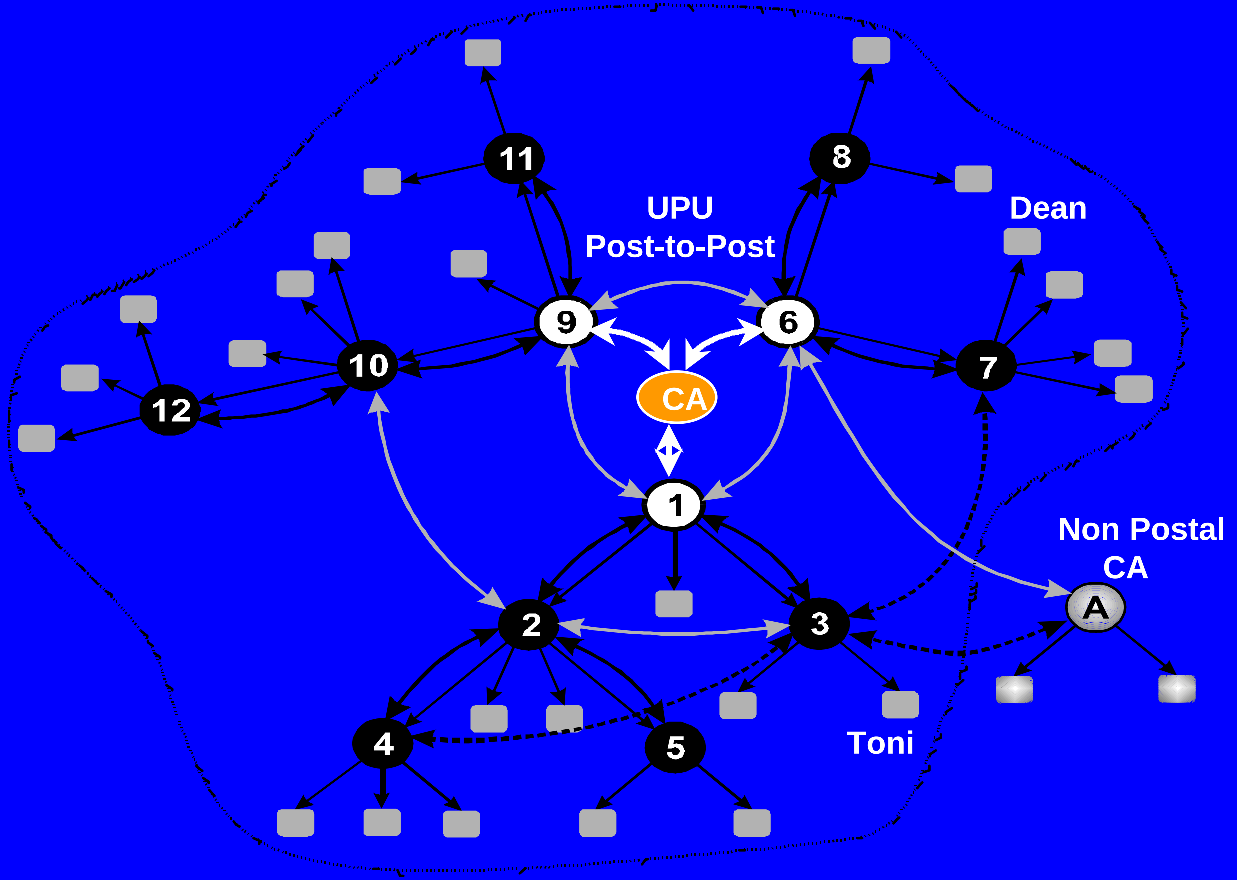
Different laws apply to the design of our "Network-of-Trust"

(Global Hierarchy, Networked or Hybrid Structures)

- Critical Compatibility issues

Policies, Procedures and Practices

The Postal Trust Model - Hybrid Network of Trust



Certificate points issuer to subject
Requiered Hierarchical Cross Certificate
General Cross certificate
Special Cross certificate
● Certification Authority (CA)
▭ User Certificate

THE POST OFFICE

Trust Principles

Be Specific

- Who is in the trusted group and what are they trusted fo

Trust Yourself

- Be the master of your own domain

Be Careful

Rigourously justify every single trust decision

Weaving a Web of Trust: Kahre and Rifkin

Some Scenarios & Legal issues

1- Applicability of the Law:

Q.: **What is the applicable law to the postal PKI (the root) ?**

A.: **The Applicable law is the UPU law "the UPU constitution" NOT the country law (*see UNCITRAL)***

2- Becoming a TTP and Joining the Postal PKI

Q.: **How to become an effective TTP nationally in absence of law**

A.: **General principles of cryptography are to be respected (OECD)**

Authentication, integrity and non-repudiation processes are to be effective (ICC)

Some Scenarios & Legal issues

3- Including a Postal operator in the Postal PKI

Q.: **How does a postal root include a postal operator in the PKI ?**

A.: **By applying and respecting an Accreditation process & areement (ABA)**

4- Certificate Validation and Recognition

Q.: **Are certificates issued from country 1 or country 2 professional TTP valid ?**

A.: **Yes, but the validation process has to be evaluated by the Postal PKI root** ***(see UNCITRAL)***

Some Scenarios & Legal issues

5- Concepts, Problems and Legal Solutions

Concept	Circumstances	Legal Solution
PKI	Creation	UPU
TTP in PKI Crypt.	Law Yes No	 Apply law & UPU Agreements &Const. UPU Rules + OECD principles
X Certification	Cross certification Cross border	UPU Rules & Agreements & Const. UNICITRAL principles & UPU
Electronic signature	If a law exists No existing law	Apply law & UPU Rules UPU rules and agreements for contractual managment

©

Certificate Validation and Recognition

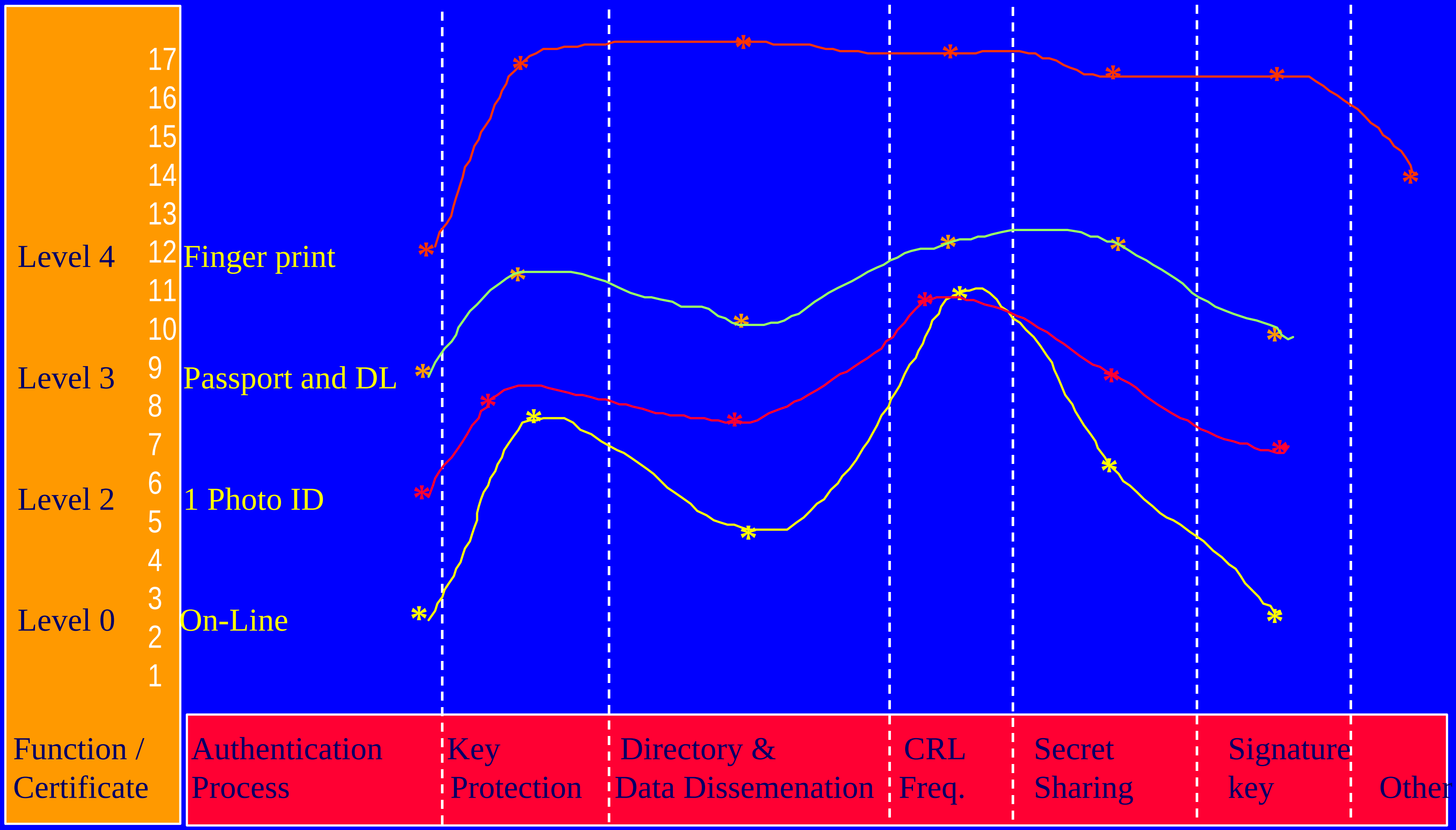
4- Certificate Validation and Recognition

Q.: Are certificates issued from country 1 or country 2 professional TTP valid ?

A.: Yes, but the validation process has to be evaluated by the Postal PKI root *(see UNCITRAL)*

Need for, not only definitions, but a SYSTEM to represent the generic components of assurance for Legal recognition and value of a certificate-class across domains / borders.

Concept System for
Certificate trust level attributes and impact on legal value



Level 4 Finger print

Level 3 Passport and DL

Level 2 1 Photo ID

Level 0 On-Line

Function / Certificate

Authentication Process

Key Protection

Directory & Data Dissemenation

CRL Freq.

Secret Sharing

Signature key

Other

example

Lev1Assur. = x AP + y KP + Z CrlFreq + ...

x, y, z are variables

THE POST OFFICE

Trust services and Legal Issues

Conclusion

We CAN provide cross-border certification services without definitive legal restrictions

BUT

We have to define the rules and policies under the UPU constitution and contractual umbrella

The OECD Guidelines

States:
Whether established by contract or legislation, the liability of individuals or entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.

Liability: What is it For?

Failure of trust services is in no-ones interest.

Liability will therefore be a ‘proof of trust’.

Liability: What is it For?

Failure of trust services is in no-ones interest.
Liability will therefore be a ‘proof of trust’.

Nonetheless it is a critical enabler.
Therefore liability MUST be backed by positive measures to support the service.

Liability: What is it For?

Failure of trust services is in no-ones interest.
Liability will therefore be a ‘proof of trust’.

Nonetheless it is a critical enabler.
Therefore liability MUST be backed by positive measures to support the service.

Expect varying degrees of liability linked to the type of service offered.
Possibly be linked to the level of certificate.

Implementing Liability

A few observations:

- Trust service availability will outrun legislation in most countries.

Implementing Liability

A few observations:

- Trust service availability will outrun legislation in most countries.
- This will lead to contractual liability being established first.

Implementing Liability

A few observations:

- Trust service availability will outrun legislation in most countries.
- This will lead to contractual liability being established first.
- Legal responsibilities are likely to fall on the supplier at a later date.

Implementing Liability

A few observations:

- Trust service availability will outrun legislation in most countries.
- This will lead to contractual liability being established first.
- Legal responsibilities are likely to fall on the supplier at a later date.
- Good practice will be needed anyway. This should form the basis of a voluntary code of practice.

Implementing Liability

A few observations:

- Trust service availability will outrun legislation in most countries.
- This will lead to contractual liability being established first.
- Legal responsibilities are likely to fall on the supplier at a later date.
- Good practice will be needed anyway. This should form the basis of a voluntary code of practice.
- This ideally should be established world-wide.

Achievements to Date

1- E. Commerce framework Policies

* Completed a UPU Notional policies and Practice Statement (PKIX 4)

2- E. Commerce Legal framework

* Derived a “checklist” to ensure legal validity of exchanges across border   with corresponding agreements between postal administartions

THE POST OFFICE

Achievements to Date

3- Global Postal E. Commerce Technical Profile

* Completed the technical profile necessary for global Trust Service provision

4- Postal E. Commerce Business Applications

* Identified 2 “start-up” applications to validate the framework and business revenue streams between Posts

Next Phases

1- Postal E. Commerce Business Applications

* Requires a global business case for applications to validate the framework and business revenue streams between Posts

2- Global Postal E. Commerce Technical Profile

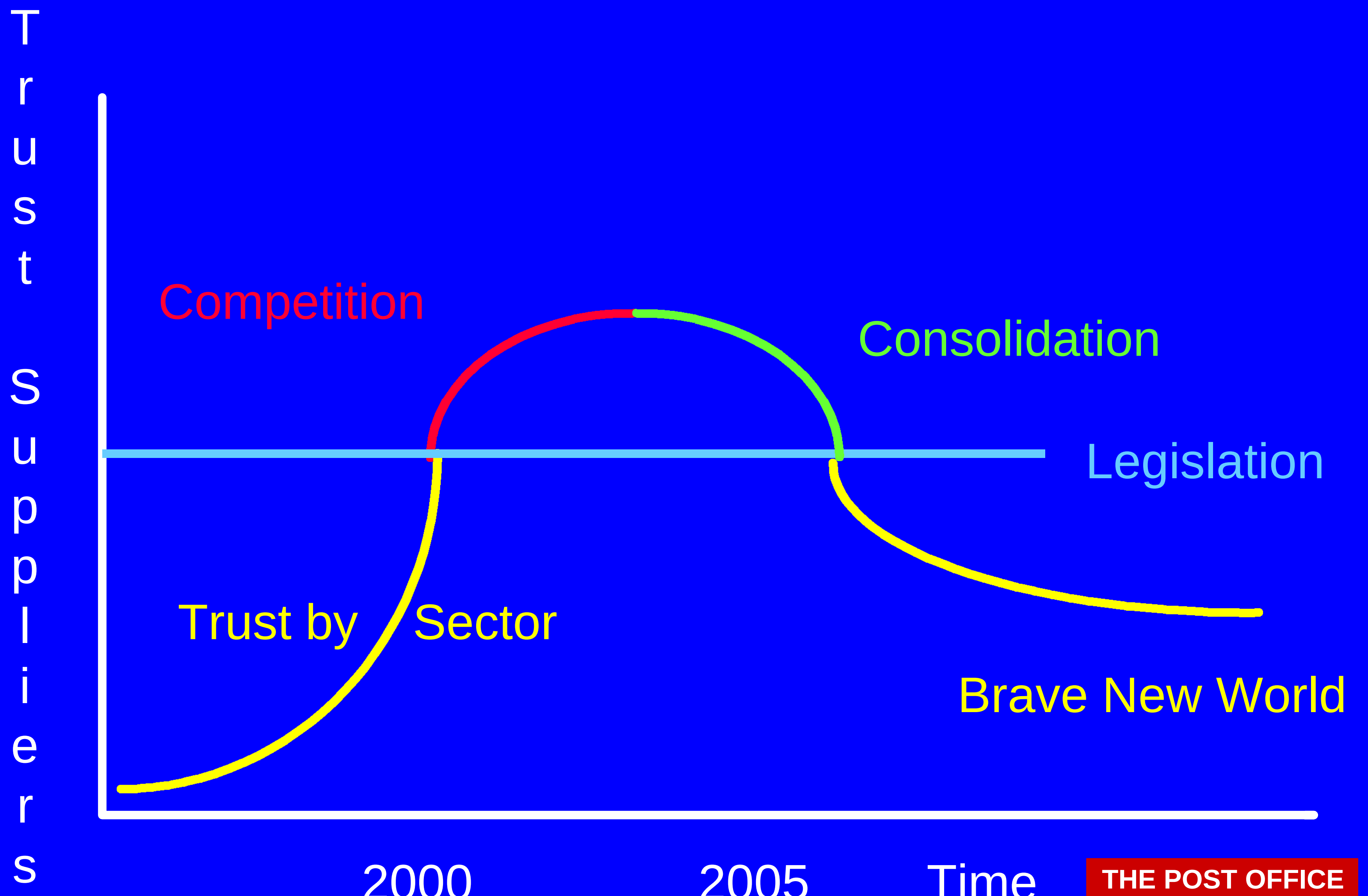
* Requires technical standards to be developed by an appropriate body. Should this be The Open Group?

Enablers to Deliver Appropriate Trust for EC

The following is needed as a minimum:

- **Interoperable technology; standards**
- **Agreed best practice; Certificate Practice Statements; External Audit**
- **Good commercial practice; sustainable partnerships**
- **Robust legal framework**
- **Strong Government commitment and understanding; partnership with industry**
- **This won’t happen overnight. Expect this to take at least 10 years.**

Enablers to Deliver Appropriate Trust for EC



THE POST OFFICE

The Universal Postal Union
and
global Postal Trust Services

Contact:
elmanawy@ptc.upu.org