



Trusted Communication Platform for Electronic Documents

Oct. 2013

**National IT Industry Promotion Agency
(NIPA)**



Table of contents

1. Introduction

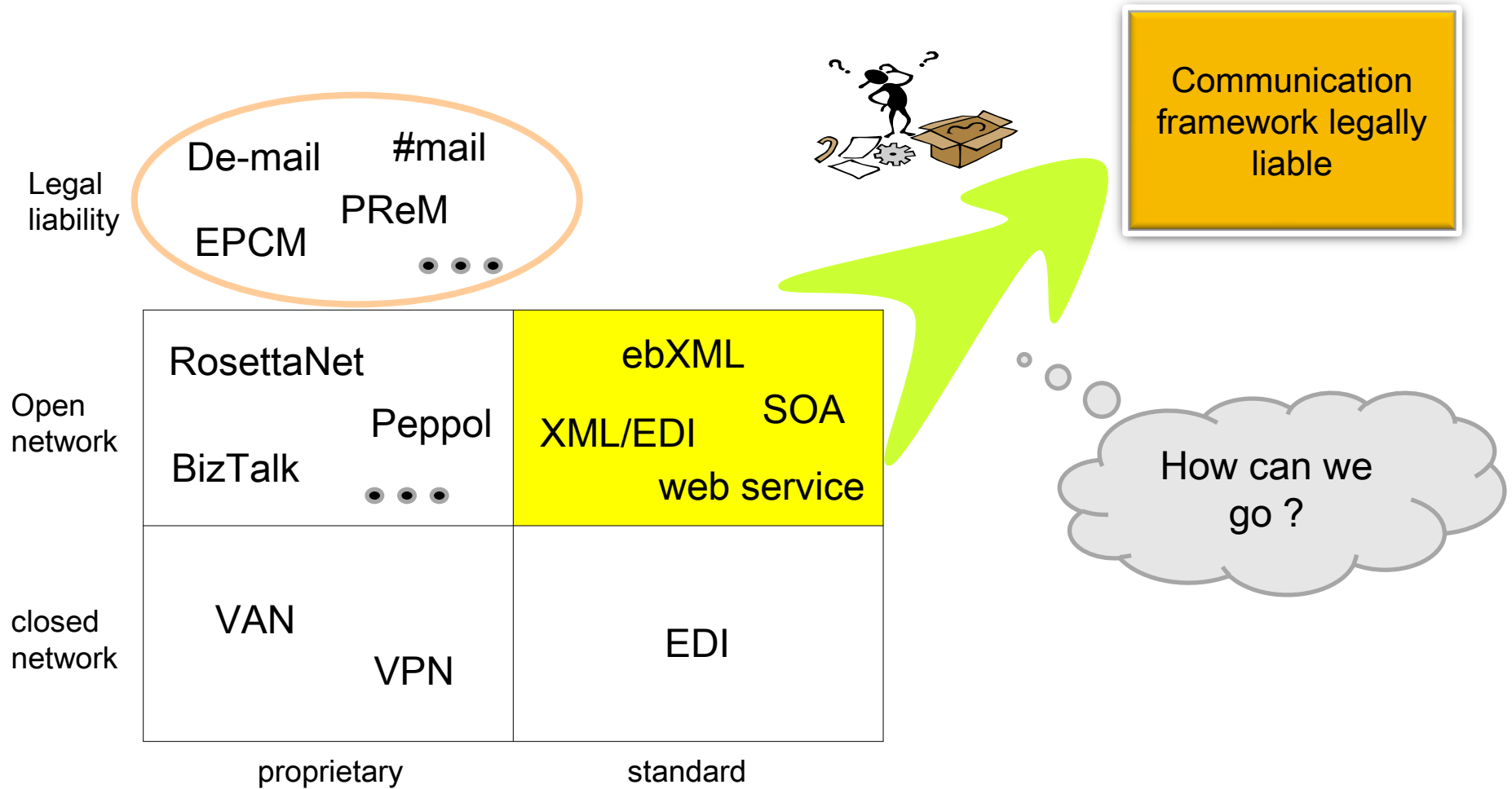
2. Required Properties of TCP

3. Mechanism for TCP

1.1 Background

- Legal and social responsibility for communicating electronic documents (ED)
- Needs for trusted ED communication framework enabling legal liability on open network and by open architecture
 - ➔ EDI: formalized data in closed network, ebXML: weak legal liability
 - ➔ RosettaNet, BizTalk: limited domain, weak legal liability
 - ➔ De-mail, #mail, EPCM, PReM: not standard, legal liability

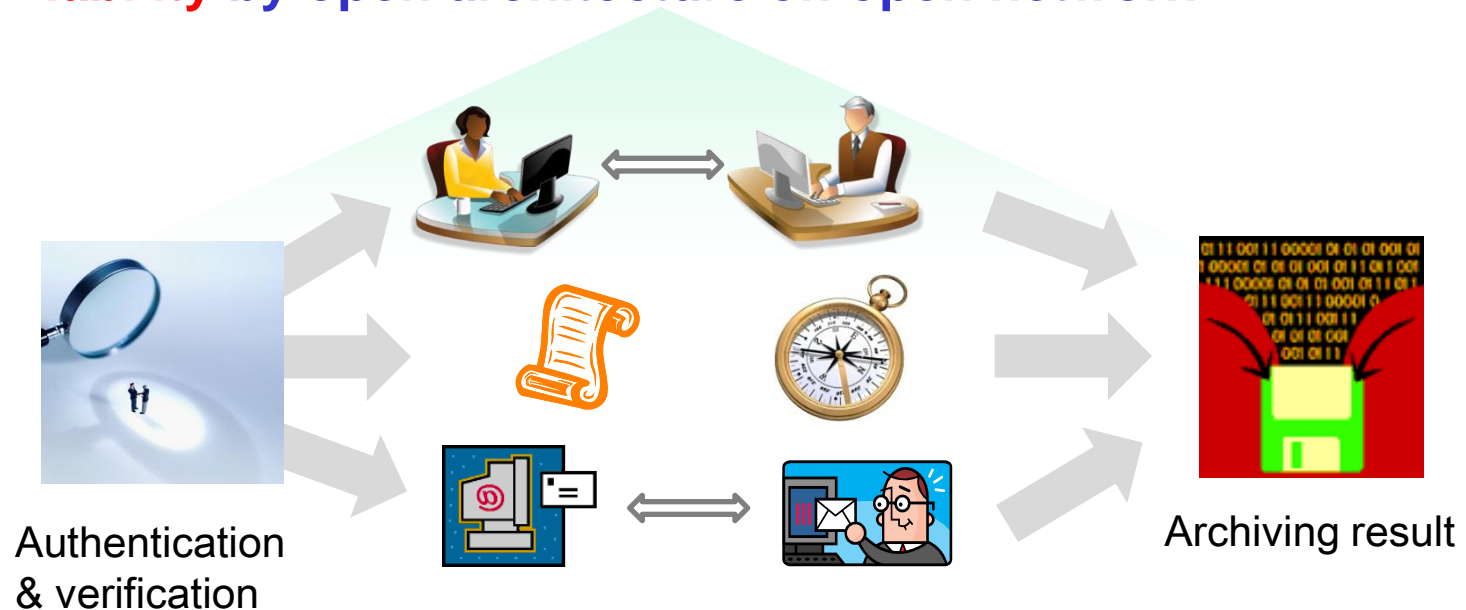
1.1 Background



1.2 Purpose

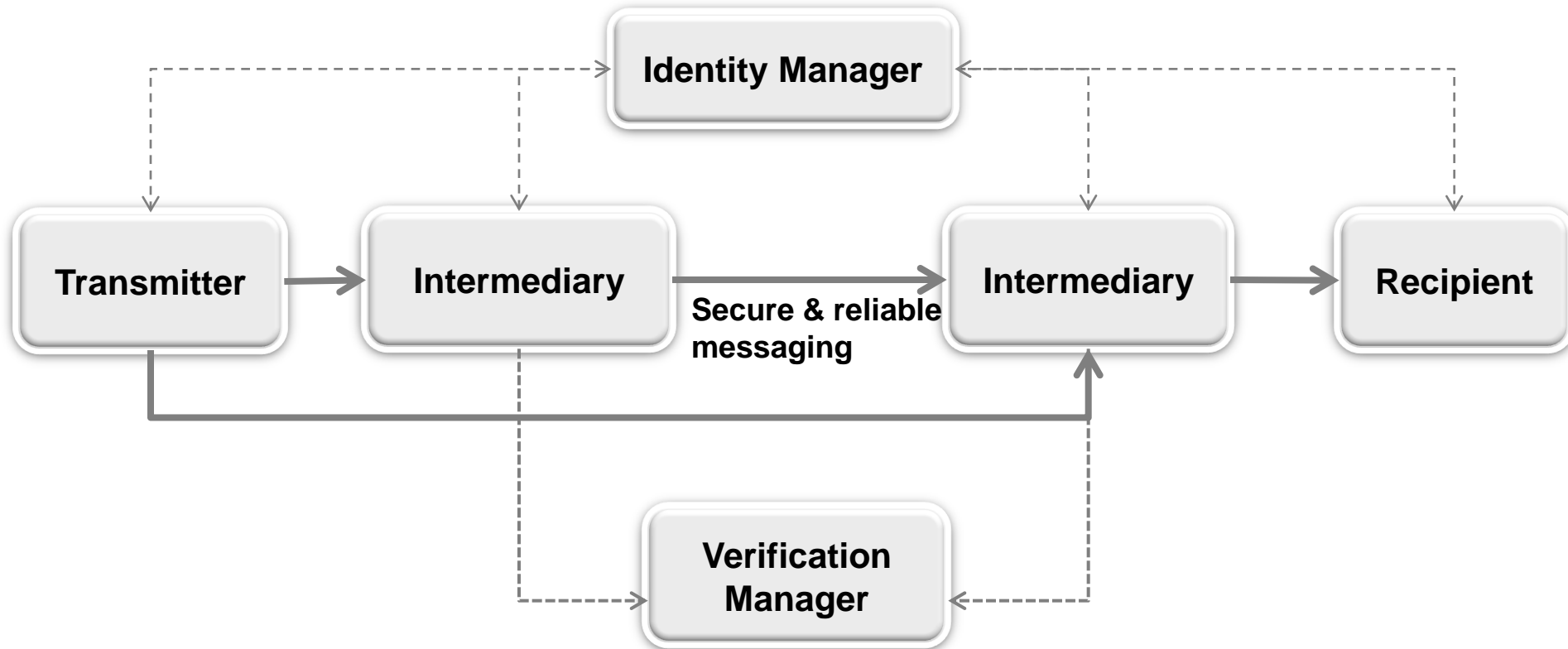
Define trusted communication platform (TCP) for electronic document

A platform enabling communication of electronic documents on
legal liability by open architecture on open network



1.2 Purpose

Provide stakeholder model for TCP





1.2 Purpose

- Describe the legal requirements for trusted communication platform (TCP) for electronic document
 - **identified** and **authenticated** users
 - information items for verifying ED communication
- Specify mechanism and specification for components and functionalities of TCP



1.3 Scope

- All the stages in lifecycle for ED communication
 - identification and authentication for users
 - creation, transmission, reception, evidence activity for ED
- Major functionalities and processes for ED communication
- Persons concerned
 - transmitter/recipient, intermediary, identity manager



1.4 Effect & Audience

- Provide the standard legal framework for open network communication
- Guideline for implementing TCP for ED
- Improve interoperability of trusted communication platform
- Audience
 - planner, developer, service provider, identity manager for TCP

2.1 Secured

- TCP should be able to transmit ED confidentially and safely without breaking data integrity.
- Target of security
 - Message including ED
 - Transport channel (network)
 - TCP server (especially, strong security in cloud environment)

2.2 Authenticated

- Users on TCP should be identified and authenticated.
- Documents should be prevented from forgery and alteration at all the stages of document lifecycle.
- Transmission/reception time should not be changed by anybody at anytime.

2.3 Accountable

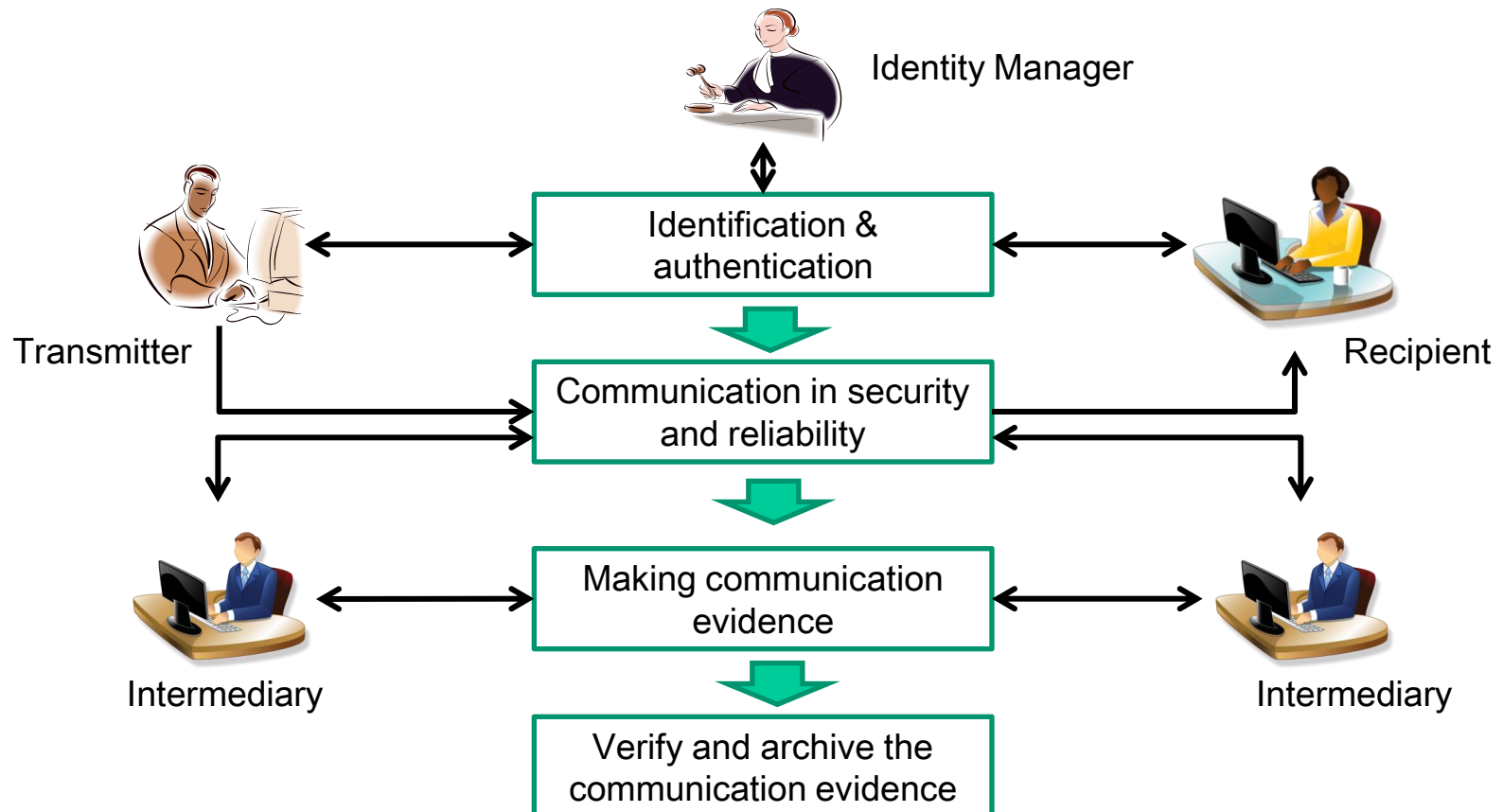
- The communication activities of transmitter & recipient should be traceable.
- For legal accountability for ED communication, communication evidence should be archived in repository.

2.4 Reliable

- Message should be transmitted without any errors as transmitter and recipients intended.
- TCP should be reliable and fault-tolerant against any unpredictable accidents.

3.1 Mechanism for TCP

- Mechanism for enabling secured and **reliable** ED transmission with legal admissibility between authenticated partners



3.2 Legal Requirements

- Ensure the legality of users
- Information items for ensuring ED communication:
 - digital signature for transmitter/recipient,
 - time on transmission/reception,
 - hash value of ED

3.3 Authentication

- Identification and authentication functionalities
 - ID/PW, digital signature, additional authentication by personal device (SMS, OTP, NFC, etc.)
- Authenticity ensured ED
- Communication Evidence
- Incommutable records for transmission/reception time

3.4 Security

- Mechanism for enabling TCP to be secured and safely operated
 - **Confidentiality**: preventing the disclosure of message to unauthorized persons or systems.
 - **Integrity** : maintaining and assuring the accuracy and consistency of messages
 - **Availability** : protecting electronic communication systems against malicious messages in order to allow only authorized consumers to access services whenever they need
 - **Non-repudiation** : assuring that senders and receivers in message transmissions cannot deny having received or sent messages

3.5 Reliability

- In order to guarantee the reliable messaging, TCP should be reliable by reliable messaging technique.
- The kinds of reliable transmission is
 - Transmitting at least once
 - Transmitting at most once
 - Transmitting precisely once
 - Transmitting sequentially

3.6 Verification & Archiving

- Verify communication evidence
- Archive the communication evidence verified



Thank you !!