Trusted Communication Platform for Electronic Documents

신뢰기반의 전자문서 유통플랫폼

전자문서 ISO국제표준 프로젝트
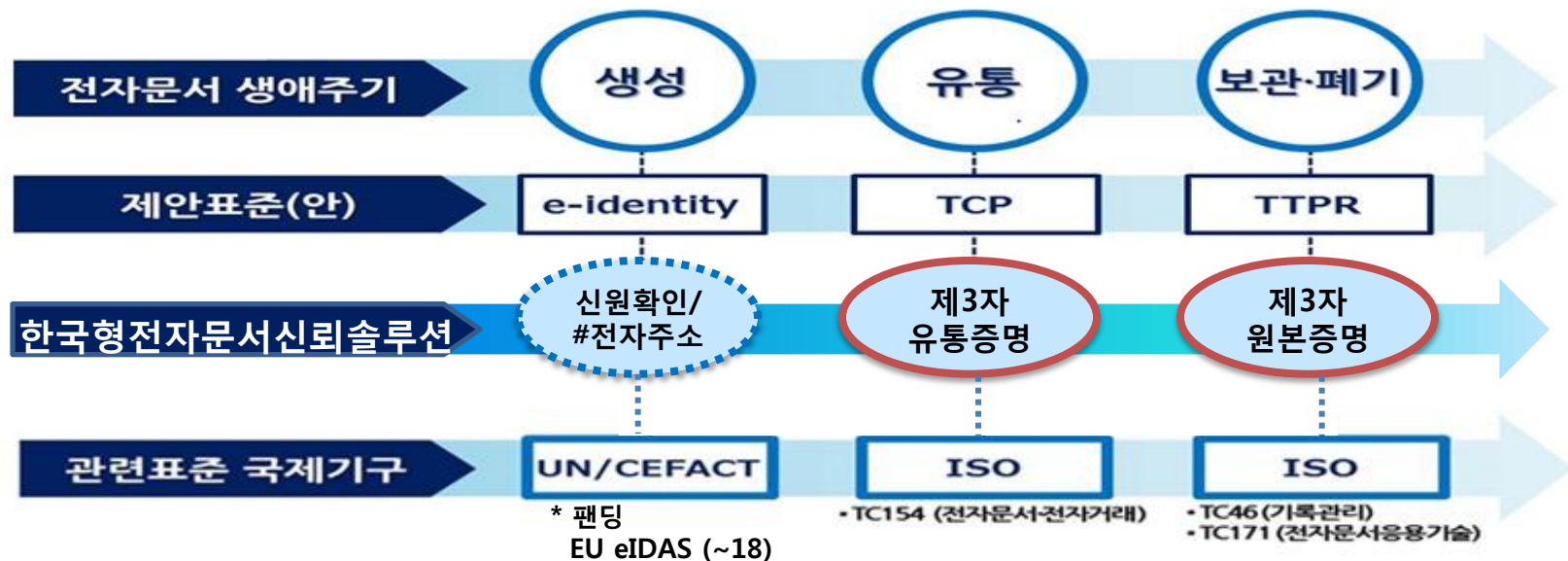
Dr. Jasmine Jaegyong Chang

Project Leader

nipa

NIPA, 전자문서 국제표준화 추진현황 및 성과

NIPA 주요 성과

1. ISO/DIS 17068 Trusted Third Party Repository for digital records (단독과제)
2. ISO/PWI 19626 **Trusted Communication Platform for electronic documents** (단독과제, 진행)
3. ISO/PWI 22957 Analysis, Selection, & Implementation of Electronic Content Management (ECM) Systems --- 공동작업 진행 (w/미국 AIIM)

전자문서 생애주기	생성	유통	보관·폐기
제안표준(안)	e-identity	TCP	TTPR
한국형전자문서신뢰솔루션	신원확인/ #전자주소	제3자 유통증명	제3자 원본증명
관련표준 국제기구	UN/CEFACT * 팬딩 EU eIDAS (~18)	ISO -TC154 (전자문서전자거래)	ISO -TC46 (기록관리) -TC171 (전자문서응용기술)

문서의 유통
– 종이문서 vs. 전자문서

종이서류
(선하증권)

전자문서
(선하증권)

OSI 7 layer

Application Layer — 7th

Presentation Layer — 6th
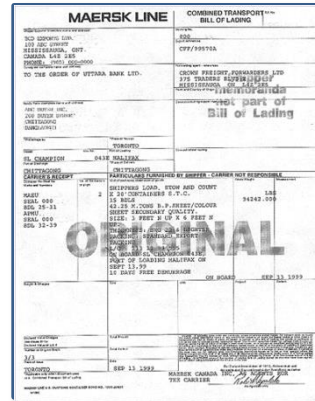
Session Layer — 5th

Transport Layer — 4th

유통문서 사본의 증거력

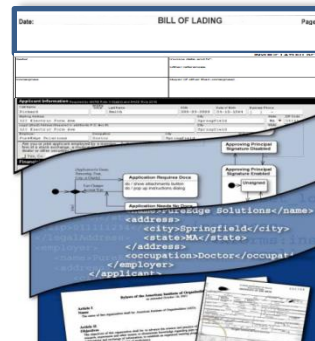– 종이문서 vs. 전자문서

Custody

선하증권(예)

◆ **종이 서류 증거력**
- Vienna CISG ('80,'88)
- Hague-Visby Rule ('68)
- Hambrug Rule ('92)

◆ **비차별 원칙 (종이, 전자문서)**
- UNCITRAL Model law (1996, 2001)
- UNCITRAL ECC (2007)

전자선하증권(예)

원본성?
무결성?

TTPR
**신뢰기반의
제3자 보관소**
(보관문서의
원본성)
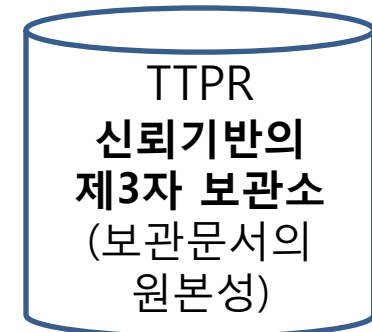
ISO 17068

· 문서 유통의 비용

- 해외 수출 화물 컨테이너 비용 (ICC 국제상공회의소, 2015)

> ○ 싱가포르 :　4개문서,　400달러,　　5일소요
> ○ 모로코　 :　4개문서,　595달러,　 10일소요
> ○ 차드　　 :　8개문서, 5500달러,　 100일소요
> ○ 서부 사하라 아프리카 국가 :　 평균 30일 소요

- 통관업무처리 비용 (WCO 세계관세기구, 2013)

> - 10년간 통관업무를 관찰한 결과, 전자문서는 종이문서 대비 15~20% 비용절감

- 무역업무처리 비용 (미 NCITP, 국가전자무역문서위원회, 1975)

> -　문서처리 비용은 수입품의 가치 중 7.5% 차지
> -　향후 10~15%까지 증가 예상

· 신뢰기반 전자문서 유통의 필요성

'Trusted communication'
신뢰기반전자문서유통
국제표준기술

? ?

'dematerialization'
증거력 있는 전자적 업무처리

"기존업무시스템에 추가 비용
최소화 차원에서 도입"

+

'legal validity'
(전자거래의) 법적 효력

United Nations Convention on the
Use of Electronic Communications
in International Contracts (2007)

6

국제표준화 현황

	proprietary	standard
Legal liability	De-Mail #Mail PReM EPCM • • •	
Open network	RosettaNet GTIN Peppol Bolero • • •	ebXML SOA XML/EDI web service
closed network	VAN VPN	EDI

Trusted communication legally liable

How can we go ?
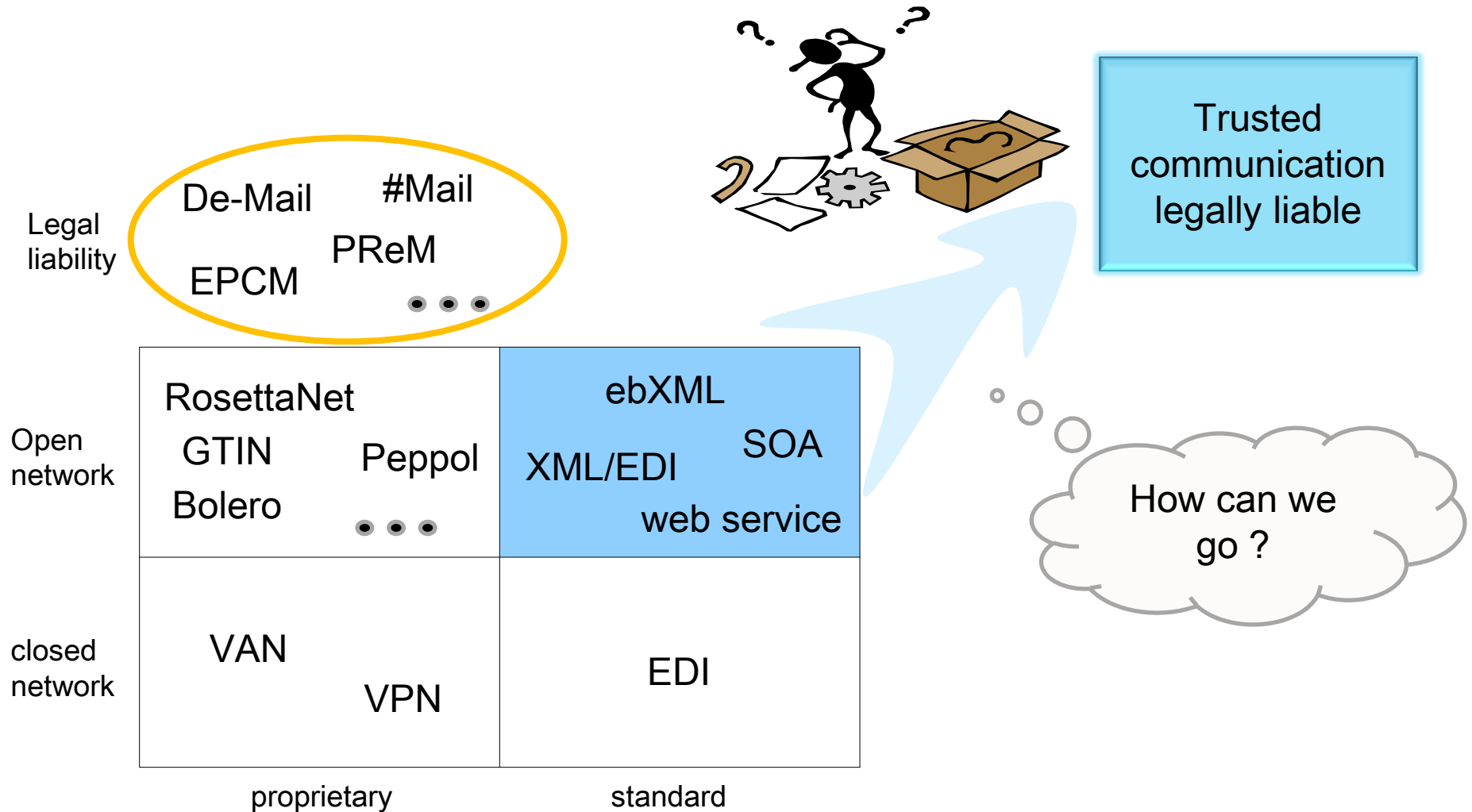
신뢰기반 전자문서유통 국제표준

- **ISO 19626-1, 2**

  Trusted Communication Platform for electronic documents
    - **Part 1 : Fundamentals**
    - **Part 2 : Extensions**

◆ ISO 19626 추진경과 및 향후계획

- ('13.10)   New project proposal accepted (Berlin)

- ('14. 8)   19626-1 project draft ver.1.0

- ('14.10)   WG6 (Trusted e-communication) project (Incheon)

- ('15. 3)   19626-1 revision draft ver.2.0

- ('15. 6)   liaison between ISO TC 154 & TC46/SC11 (Beijing)

- ('15. 9)   TC154 WG 6 voting -- plan

◆ ISO TC1154 WG6 experts list

The list of experts for ISO/TC 154/WG 6

Name*	E-mail*	NSB or organization*	WG*	Role	Phone	Fax	
Jang, Jasmine	jasmine@nipa.kr	KATS (Korea, Republic of)	WG6	convener			
Peter Rybar	peter.rybar@nbusr.sk peterryb@gmail.com	SOSMT/National Security Authority	WG6	Committee member	+421903993708	+421268691701	
Pavol Futros	pavol.futros@nbusr.sk	SOSMT/National Security Authority	WG6	Committee member	+421268692136	+421268691701	
Sato, Masashi	masas-sato@secom.co.jp	JISC	WG6	committee member	+81-422-76-2111	+81-422-76-2120	
Kitagawa, Nobuhisa Mr	kokusai4@jsa.or.jp	JISC	WG6	observer			
Korte, Ulrike Dr.	ulrike.korte@bsi.bund.de	DIN	WG6	committee member	+49 228 999582-5842		
Bösler, Bernd	Bernd.Boesler@din.de	DIN	WG6	observer			
Choi, Keong Ju	kjchoi@kmu.ac.kr	KATS	WG6	committee member	+82-53-580-5641		

◆ ISO 19626 Benefits

- **Business value**
  - **Cost saving** : paperless & dematerialization etc
  - **Business innovation** : speed & liability etc

- **Application area**
  - **Single window portal** : e-Logistics, e-Trade, e-Government.. etc
  - **Trusted (cloud) service :** e-Payment, e-health, e-finance... etc
  - **Global export :** eGovernment services, paperless projects... etc

- **Future vision**
  - **TCP in cloud, IoT, Mobile**
    - * ISO 20415, TMEF(Trusted Mobile Electronic Framework)
  - **Supply Chain Integrity**

ISO 19626-1

Trusted Communication Platform for Electronic Documents
Part 1 : Fundamentals

Revision ver. 2
주요내용

◆ 정의(기본개념)

- **Communication** (by UNCITRAL)

Any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract

- **Electronic communication** (by UNCITRAL)

Any communication that the parties make by means of electronic documents

- **Trusted communication**

A **qualified** electronic communication including secure and reliable transfer of electronic documents and its provable custody for the purpose of **dematerialization**

- **TCP(Trusted communication Platform)**

A service platform enabling trusted communications of exchanging electronic documents on legal liability by open architecture on open network

◆ 신뢰유통을 위한 법적 고려사항

1. **Certainty of communication (커뮤니케이션/확실성)**
   1) certainty about communication parties (신원확인)
   2) certainty about communication context (커뮤니케이션맥락)
   3) certainty about communication contents (커뮤니케이션내용)

2. **Completeness of communication delivery (대행/온전성)**
   1) completeness from electronic transaction to contract (완결성)
   2) completeness of communication delivery with evidential admissibility (증거력)

3. **Confidentiality of communication delivery (대행/기밀성)**
   - confidentiality ← Information privacy(프라이버시보호)

◆ 신뢰유통 경영관리를 위한 고려사항…

- Trusted communication model (신뢰기반 전자문서유통 모델)
  - 주체별 역할과 책임 (신뢰의 가치사슬), 인증, 품질 및 리스크 관리, 협약 등 ....
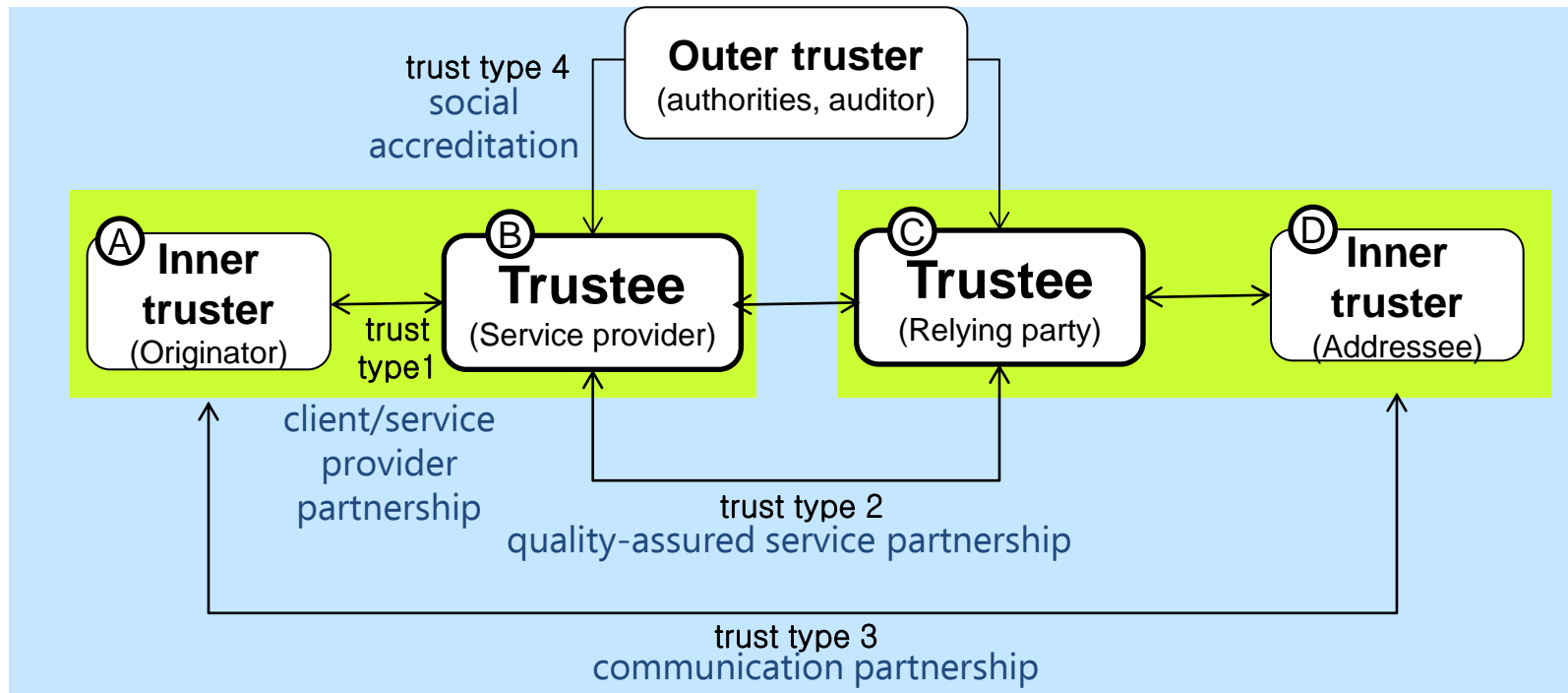
TCP(Trusted communication Platform)

A service platform enabling trusted communications

of exchanging electronic documents

on legal liability

by open architecture on open network

◆ TCP 기술구현 아키텍처 …

```
                        ┌──────────────────────────┐
                   ┌───▶│   TCP identity directory  │◀───┐
                   │    └──────────────────────────┘    │
                   ▼                                      ▼
┌──────────────┐   ┌──────────────┐   ┌──────────────┐   ┌──────────────┐
│ Transmitting │◀─▶│ transmitting │◀─▶│  receiving   │◀─▶│  Receiving   │
│    Client    │   │   server     │   │   server     │   │   client     │
└──────────────┘   └──────────────┘   └──────────────┘   └──────────────┘
                   ▲                                      ▲
                   │    ┌──────────────────────────┐     │
                   └───▶│  TCP evidence repository  │◀────┘
                        └──────────────────────────┘
                                    ▲
                                    ▼
                        ┌──────────────────────────┐
                        │      certificate of       │
                        │  trusted communication    │
                        └──────────────────────────┘
```
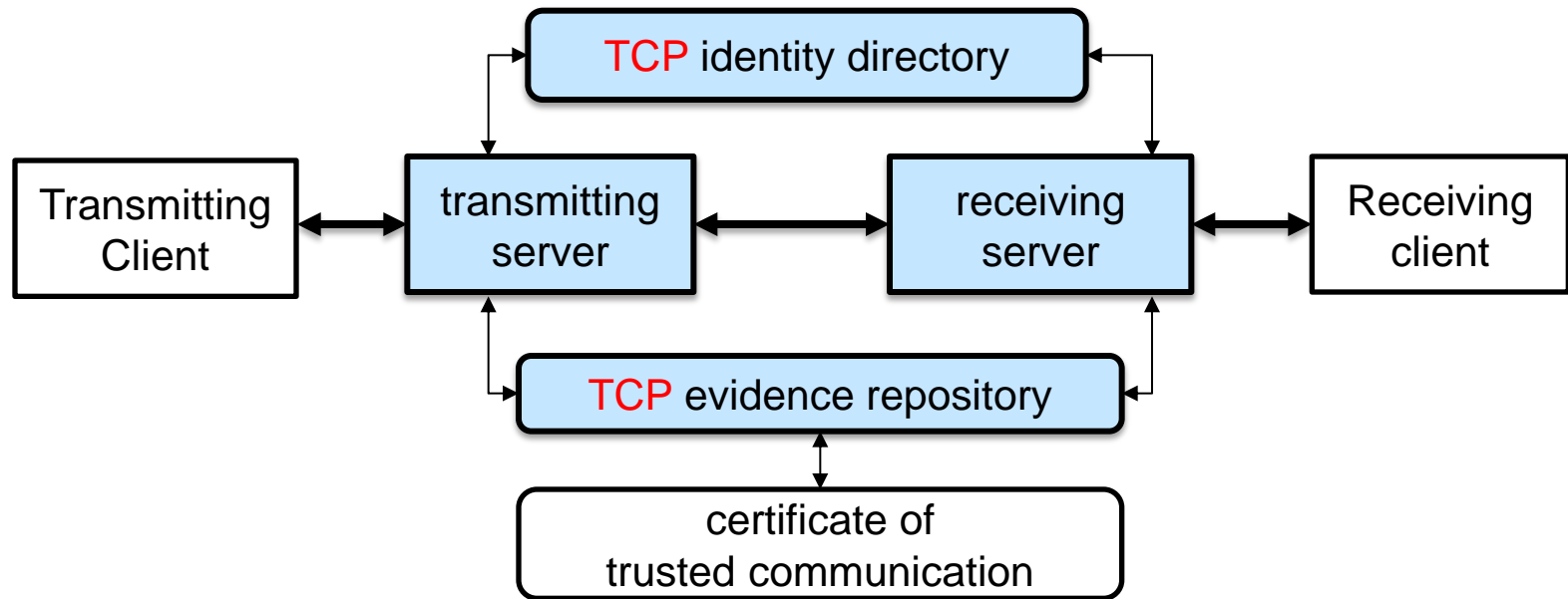
◆ TCP 기술구현 요건 : 5개 속성

1. Confidentiality (기밀성)

2. Authentication (인증)

3. Accountability (설명력)

4. Liability (책임성)

5. Portability (이식성)

• TCP requirements

1. Confidentiality
기밀성

(1) Confidentiality of electronic documents
(2) Secured transport channel (network)
(3) Security in each trust type sector (end-to-end)

2. Authentication
인증

(1) Authentication methods ,
(2) Chain of authentication and mutual recognition

• **TCP requirements**

3. Accountability
설명력

4. Liability
법적 책임성

(1) Proofs of trusted communication

(1) Chain of trust between intermediaries,
(2) Reliability form risk and quality
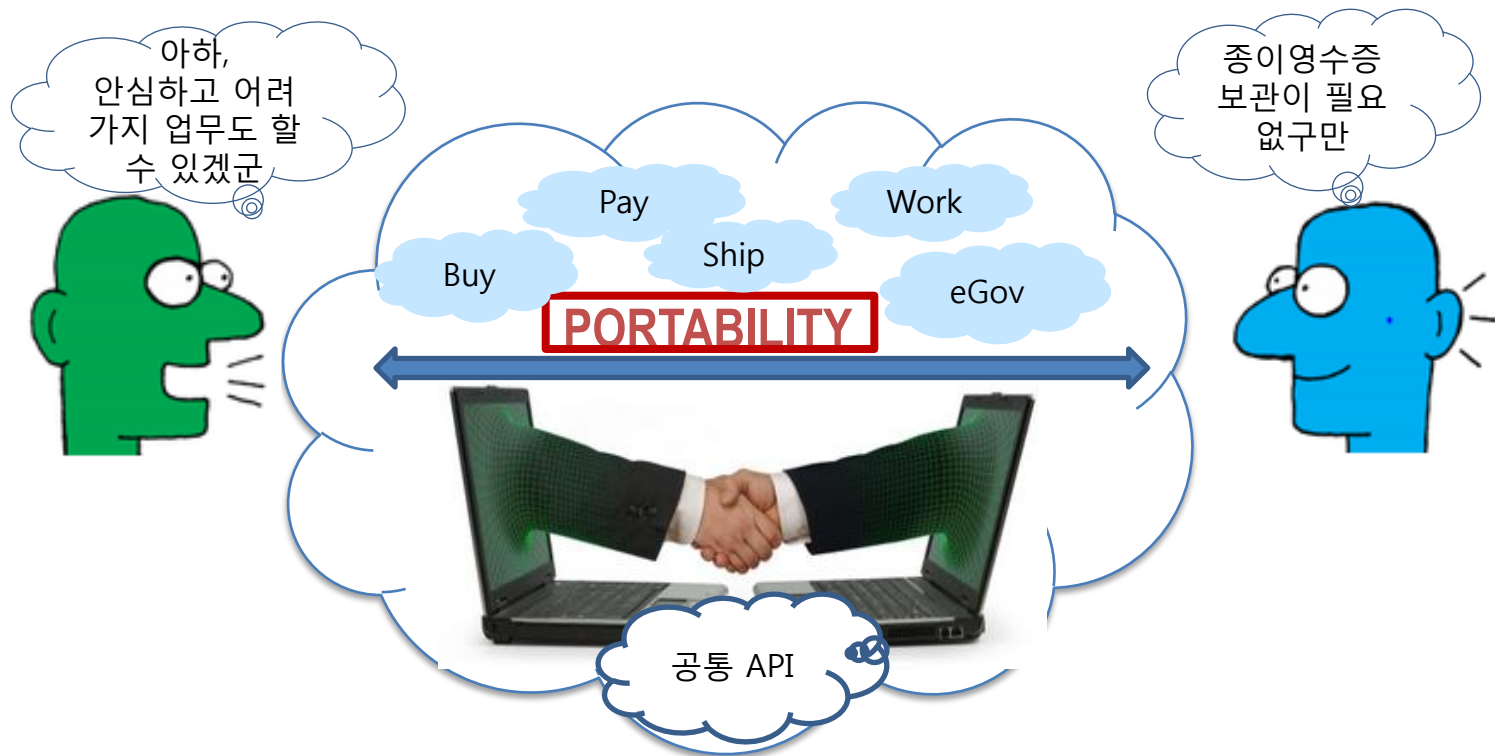(3) service agreement or contract between intermediaries and clients
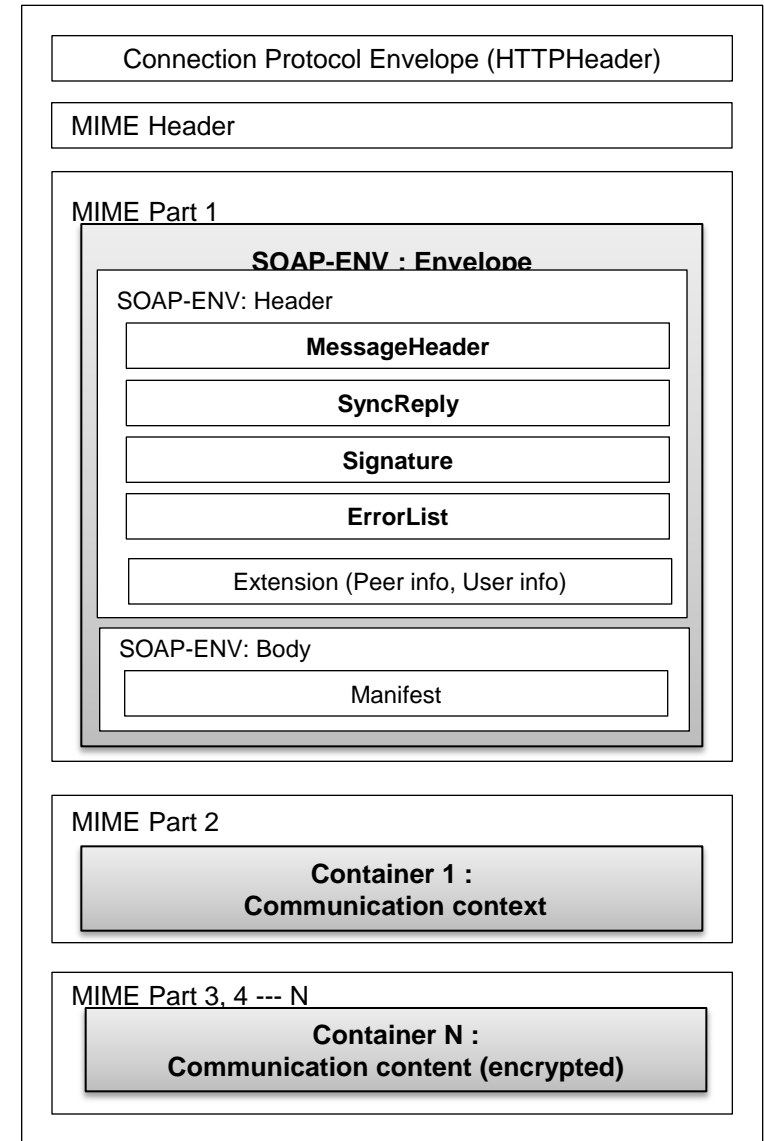
• **TCP requirements**

5. Portability
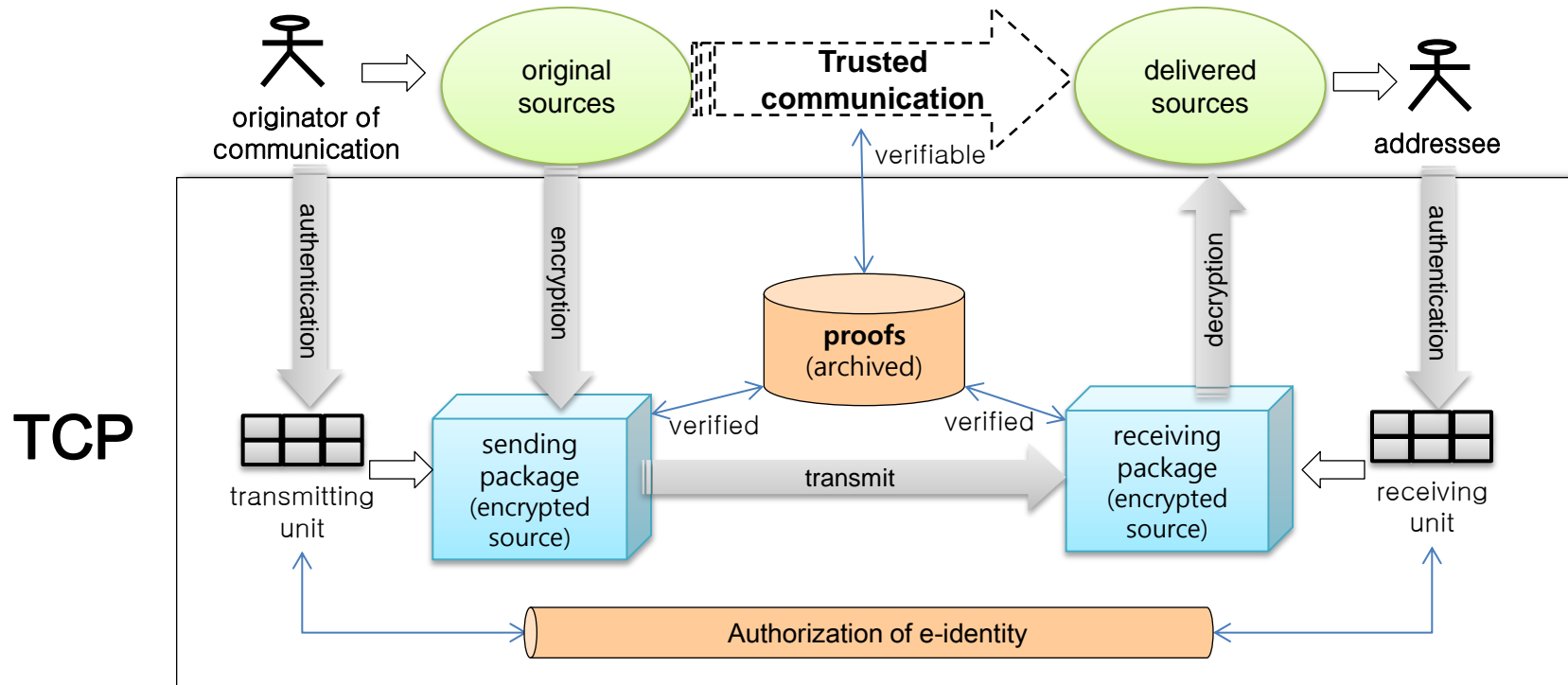이식성

(1) Service connectivity

◆ TCP 주요기능 ...

1. Secured communication
   (안전한 전자문서 유통)
2. Securely communicated documents
   (전자문서 내용기밀 유지)
3. TCP enveloping
   (TCP 전송봉투)
4. Dematerialization
   (증거력확보)

Connection Protocol Envelope (HTTPHeader)

MIME Header

MIME Part 1

SOAP-ENV : Envelope

SOAP-ENV: Header

MessageHeader
SyncReply
Signature
ErrorList
Extension (Peer info, User info)

SOAP-ENV: Body

Manifest

MIME Part 2

**Container 1 :
Communication context**

MIME Part 3, 4 --- N

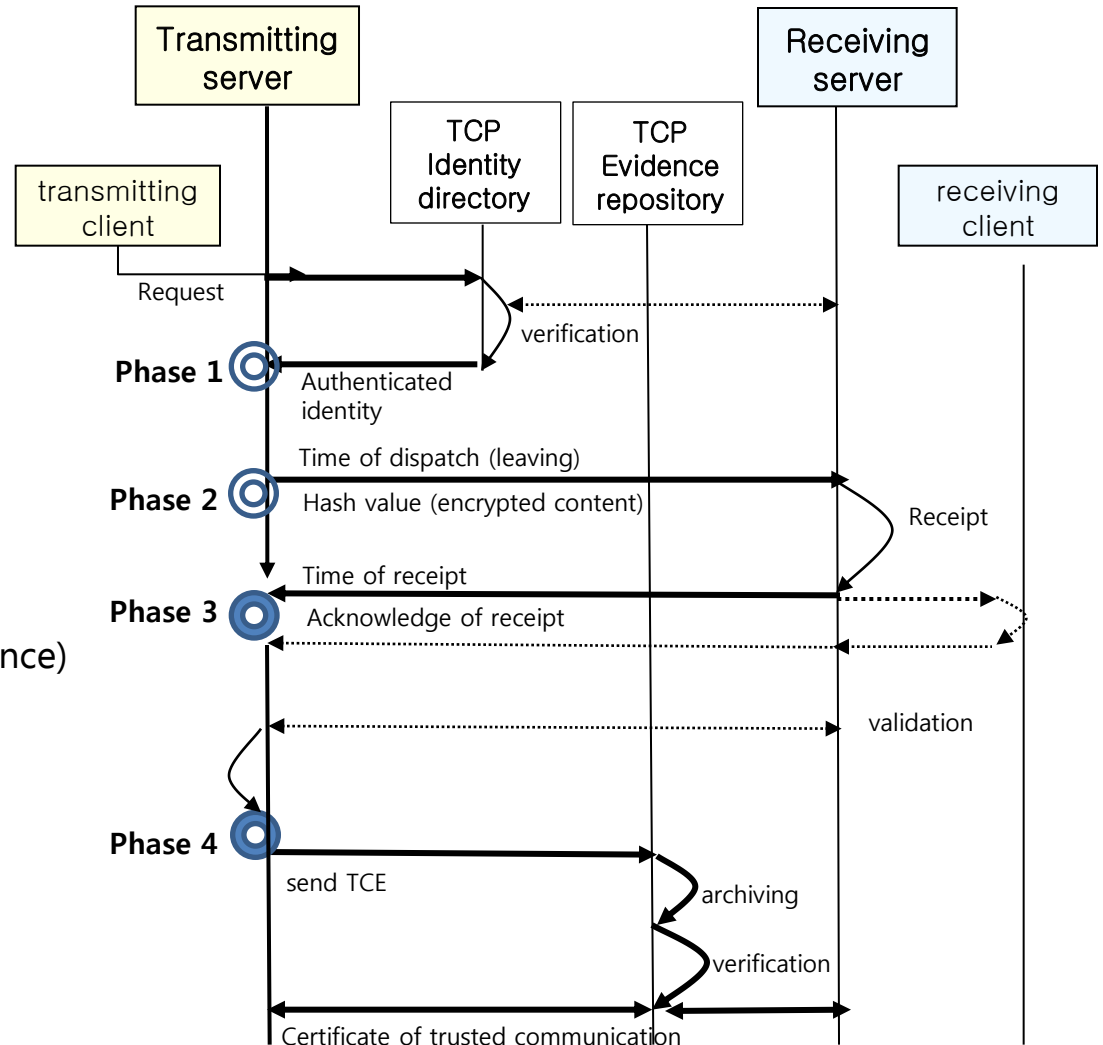**Container N :
Communication content (encrypted)**

◆ ISO 19626-1   TCP dematerialization mechanism

◆ ISO 19626-1 Proofs of trusted communication …

- 4 Phases
1. Capture : authorized e-identity
2. Capture : sending communication package
3. Capture : trusted delivery conformation
4. Custody : TCE(Trusted Communication Evidence)

Transmitting server

Receiving server

TCP Identity directory

TCP Evidence repository

transmitting client

receiving client

Request

verification

Phase 1
Authenticated identity

Time of dispatch (leaving)

Phase 2
Hash value (encrypted content)

Receipt

Time of receipt

Phase 3
Acknowledge of receipt

validation

Phase 4
send TCE

archiving

verification

Certificate of trusted communication

◆ ISO 19626-1 Proofs of trusted communication

A sample : Certificate of trusted communication

Certificate of trusted communication		
Communication	eigenvalue	1234-5678-89-1234
	type	transmission/ receiving/ perusal
Originator of communication	ID(address)	gildong.hongl#nipa.pe.kr
	extension	organization : nipa, org ID : 123-45-45678
Addressee	ID(address)	yori.ko#kisa.or.kr
	extension	organization : kisa, org ID : 987-65-43210
Communication date/time	transmitting time	2015.03.10 09:13
	receiving time	2015.03.10 09:16
	perusal time	2015.03.10 10:05
Communication contents	content title	Hello
	Hash value (content)	nOczepEXEhtZGtpJXvRUiMnFutw
	attached file name	TCP overview.ppt
	Hash value (attached file)	MnvWxtuiPhtoQRvTuROMSoptwP
Issue date		2015.05.05
Issuer of certificate		Trusted communication certificate committee

감사합니다.

장재경
(jasmine@nipa.kr)
정보통신산업진흥원