TSP is an Inter-Trust Domain Protocol (ITDP)

Wenjing Chu

Feb 21, 2023

Public Reference to this doc should be in its entirety and as:
{Wenjing Chu, "TSP is an Inter-Trust Domain Protocol (ITDP)", Feb 21, 2023. https://github.com/wenjing/Inter-Trust-Domain-Protocol}

A Quick Bio:

- I had participated and developed many Internet/network protocols in my career with several Startups and Cisco, e.g. TCP/IP stack, Internet routing protocols (BGP, OSPF, ISIS, RIP…), IP Multicast, IP Mobility, MPLS/ATM/FR, Wi-Fi/IEEE 802.11, and 4G/5G mobile networks...
- A Senior Product Manager for Nokia in security.
- A Distinguished Engineer in Dell/VMware and currently at Futurewei, where I am Sr. Director of Technology Strategy.
- Have been actively involved in many open source, standard and other communities: ToIP, OpenWallet (OWF), LF Edge, LF Network, C2PA, W3C, IETF, IEEE, ETSI ... over the years.
- With ToIP: a founding Steering Committee member, primary contributor of TechArch Spec, Co-chair of TSP task force, Co-chair of AI and metaverse task force, etc.

My proposal

1. A protocol should be understood under a Reference Architecture.
    a. I will re-present a short overview of my Reference Architecture that was first presented at IIW April 2022 and then contributed to the TechArch TF.
2. What is TSP, exactly?
3. Less is More - what the TSP should and shouldn't include.
4. What the Protocol Specification defines
5. How upper layer Trust Tasks can be implemented
6. How lower layer Support Functions may implement what TSP needs
7. Q&A

I won't have time to cover at this time, but can go over in a followup.

Wenjing Chu

(1) Proposed Reference Architecture

A protocol stack is to view the decomposition vertically in functionality, where each higher layer incrementally adds functionality above the layer(s) below it. It is suitable within an endpoint where dependencies are clearly ordered. But it is not suitable to capture relationships between different sub-systems. The Reference Architecture is a prerequisite to understand a protocol stack.
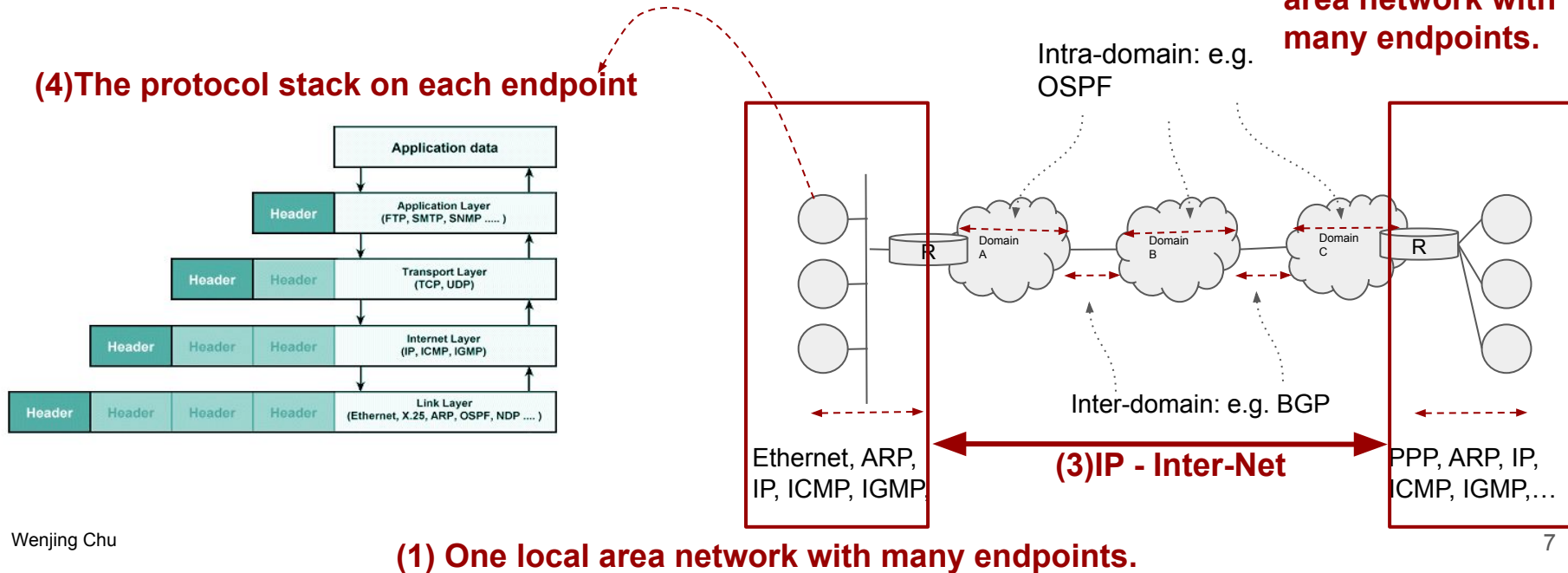
Layers of a Stack within an endpoint of a subsystem

Interactions between subsystems
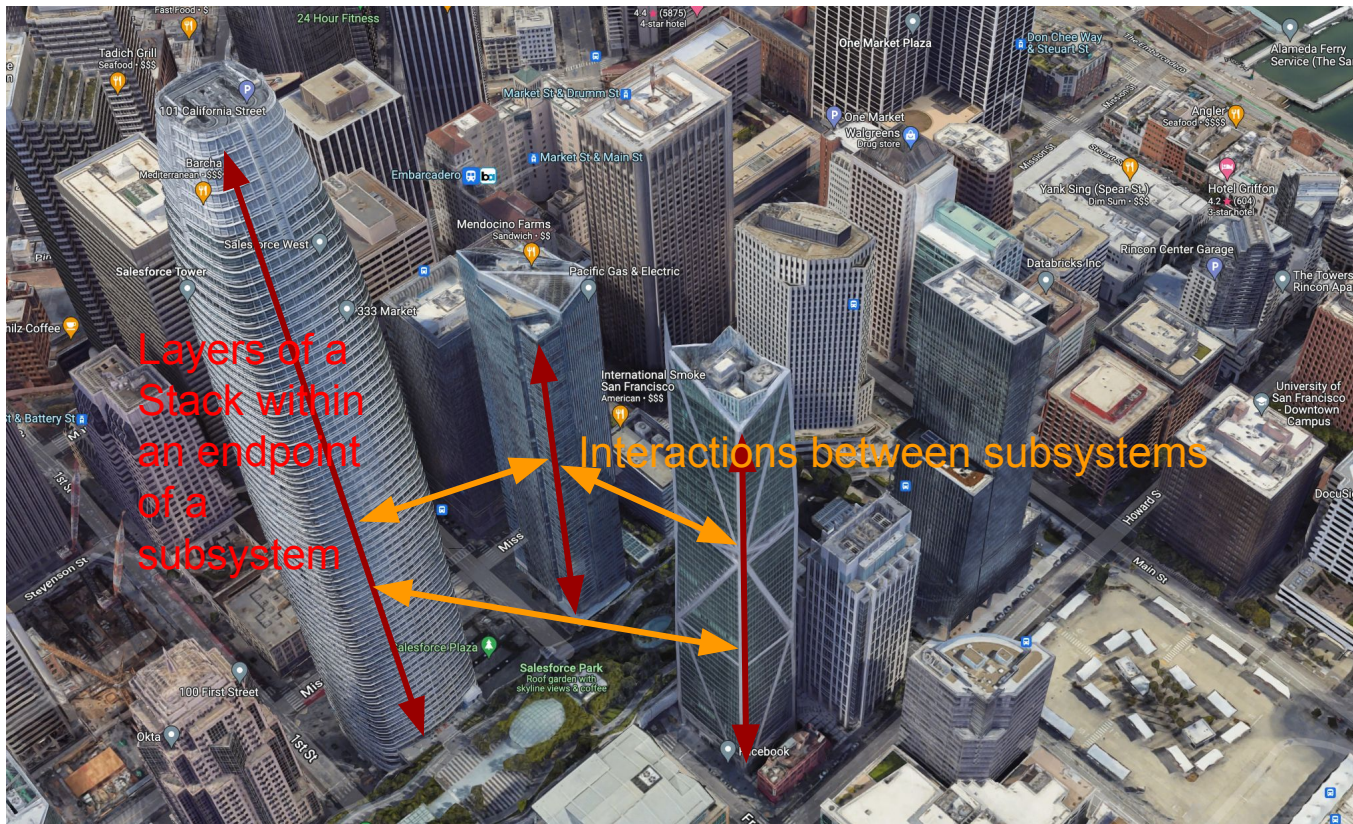
An analogy for a Reference Architecture

For Example: Internet Reference Architecture

The familiar Internet *stack view* is usually focused on *end systems*

The Internet reference architecture

(2)Another local area network with many endpoints.

Intra-domain: e.g. OSPF

(4)The protocol stack on each endpoint

(1) One local area network with many endpoints.

Inter-domain: e.g. BGP

(3)IP - Inter-Net

Ethernet, ARP, IP, ICMP, IGMP.

PPP, ARP, IP, ICMP, IGMP,…
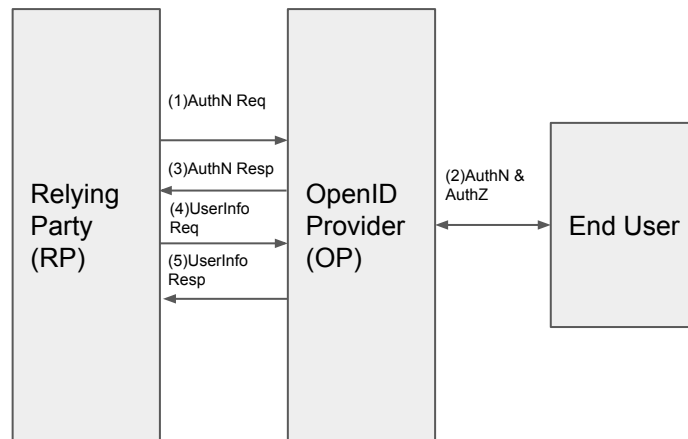
Another Example: OIDC Reference Architecture

The OpenID Connect protocol, in abstract, follows the following steps.

1. The RP (Client) sends a request to the OpenID Provider (OP).
2. The OP authenticates the End-User and obtains authorization.
3. The OP responds with an ID Token and usually an Access Token.
4. The RP can send a request with the Access Token to the UserInfo Endpoint.
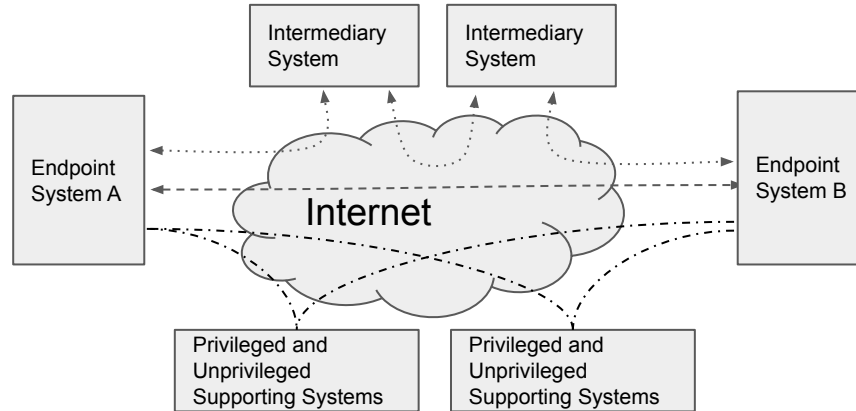5. The UserInfo Endpoint returns Claims about the End-User.

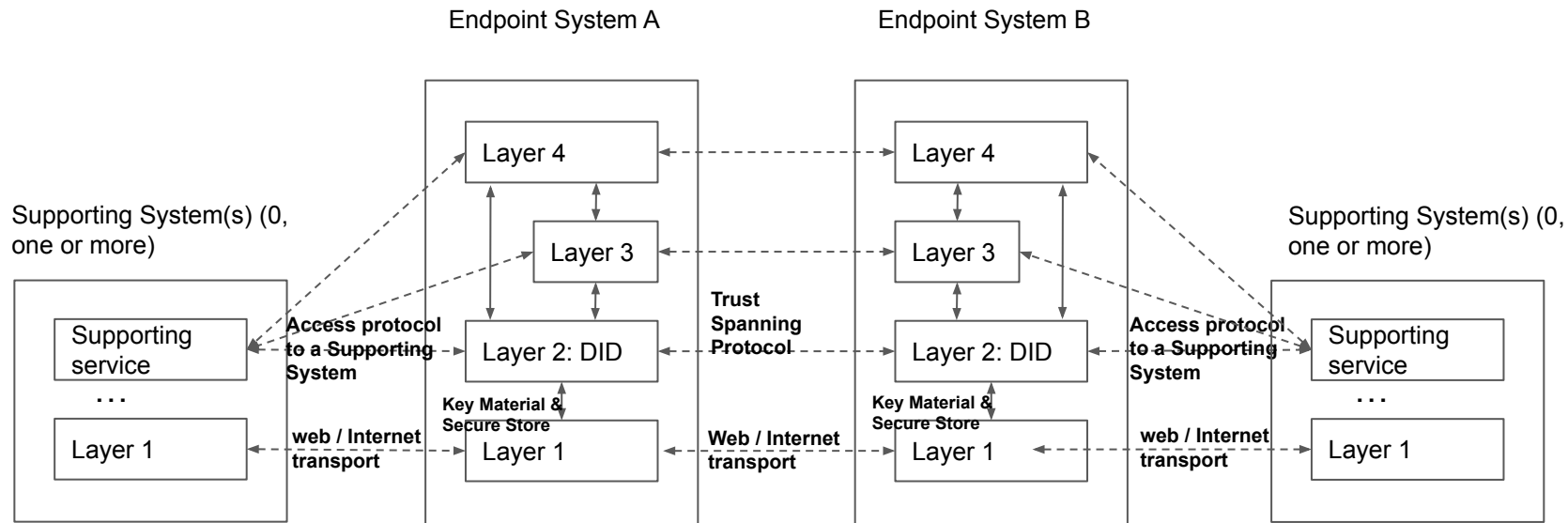These steps are illustrated in the following diagram:
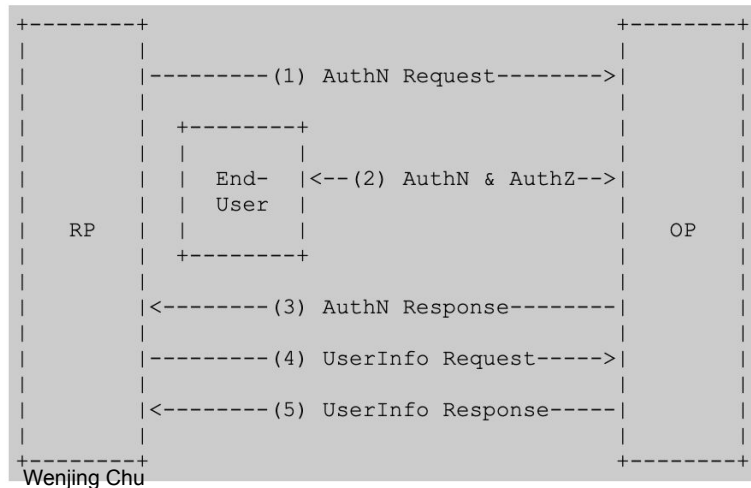
Same picture but unfolded.

```
+--------+                                  +--------+
|        |                                  |        |
|        |---------(1) AuthN Request------->|        |
|        |                                  |        |
|        |   +--------+                      |        |
|        |   |        |                      |        |
|        |   |  End-  |<--(2) AuthN & AuthZ-->|        |
|        |   |  User  |                      |        |
|   RP   |   |        |                      |   OP   |
|        |   +--------+                      |        |
|        |                                  |        |
|        |<--------(3) AuthN Response--------|        |
|        |                                  |        |
|        |---------(4) UserInfo Request----->|        |
|        |                                  |        |
|        |<--------(5) UserInfo Response-----|        |
|        |                                  |        |
+--------+                                  +--------+
```

Wenjing Chu
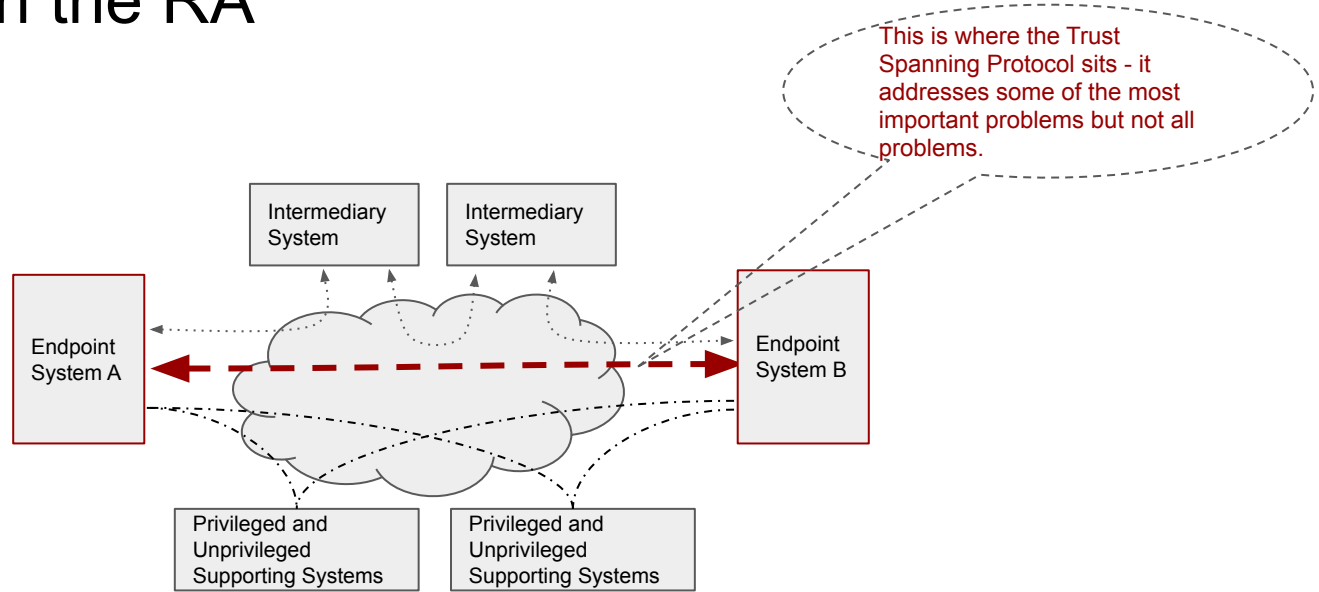
The proposed Reference Architecture (RA)

- Subsystems are delineated by **locus of control (domain)**
- They interact through **a set of protocols**, not just one.
- Each **type** of subsystems has a shared stack architecture*, but the stack architecture is not identical across different types of subsystems**.
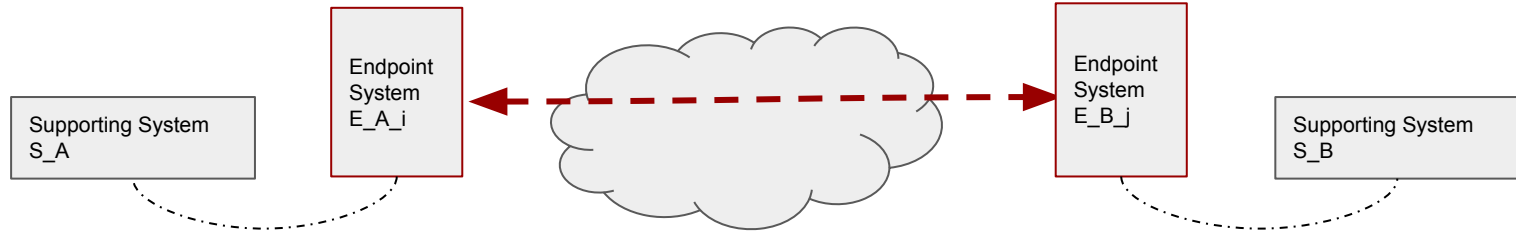
Endpoint System A

Endpoint System B

Supporting System(s) (0, one or more)

Supporting System(s) (0, one or more)

Layer 4

Layer 3

Trust Spanning Protocol

Access protocol to a Supporting System

Supporting service

. . .

Layer 2: DID

Key Material & Secure Store

Layer 1

web / Internet transport

Layer 1

Web / Internet transport

Access protocol to a Supporting System

Key Material & Secure Store

web / Internet transport

Supporting service

. . .

Layer 1

A Generalized Reference Architecture (with Intermediary Systems removed for clarity)

How TSP fits in the RA

This is where the Trust Spanning Protocol sits - it addresses some of the most important problems but not all problems.

Intermediary System

Intermediary System

Endpoint System A

Endpoint System B

Privileged and Unprivileged Supporting Systems

Privileged and Unprivileged Supporting Systems

How TSP fits in the RA

(2) What is TSP, exactly?

TSP is an Inter-Trust Domain Protocol (ITDP)

ITDP

Endpoint System E_A_i

Supporting System S_A

Endpoint System E_B_j

Supporting System S_B

Trust Domain T_A
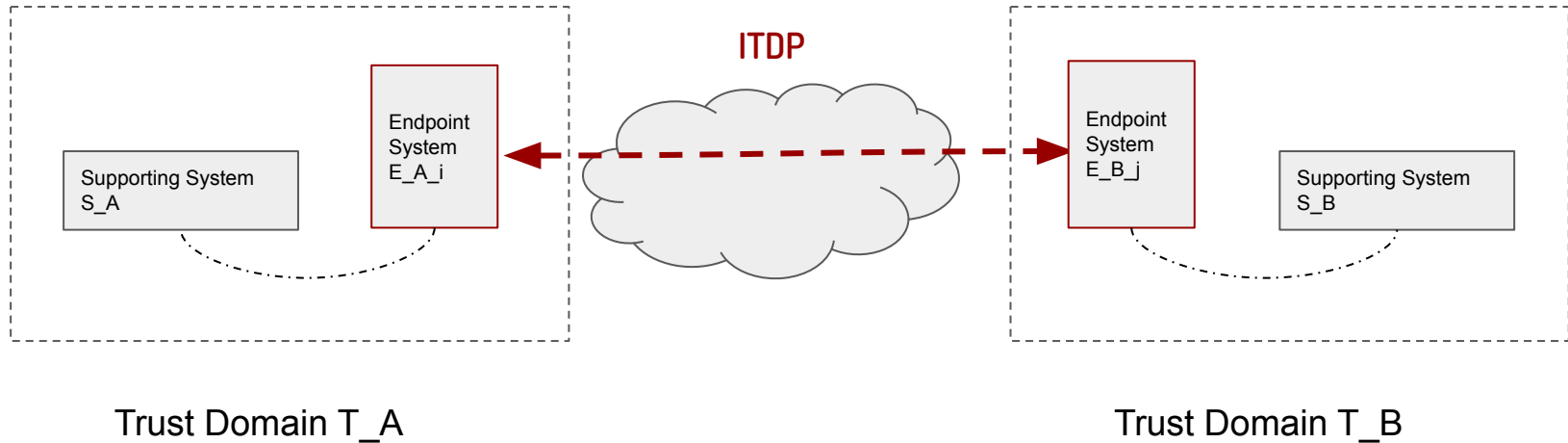
Trust Domain T_B

(0)How to bridge (or span) trust signals between Trust Domains is the problem that TSP needs to solve. Other problems are either the concerns of other layers of the same stack or other stacks entirely.

Wenjing Chu

TSP is an Inter-Trust Domain Protocol (ITDP)

(1)ITDP enables any Trust Domain x to any Trust Domain y interoperability and supports as many types of Trust Domains as possible.

ITDP

Endpoint System E_A_i

Supporting System S_A

Endpoint System E_B_j

Supporting System S_B
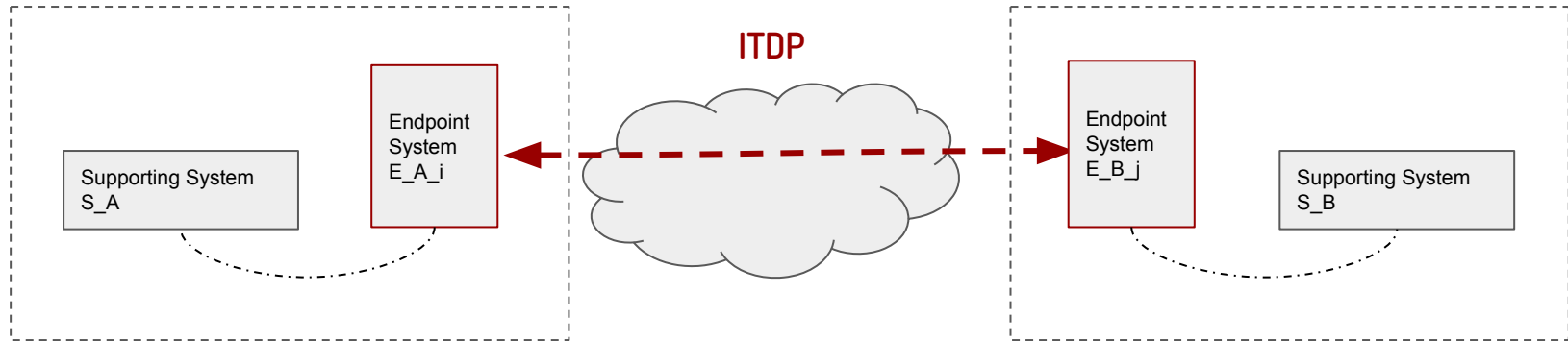
Trust Domain T_A

Trust Domain T_B

T_x examples… non-exhaustive at all	S_x	E_x
DID Method x	DID Method x impl. (eg blockchains)	Any except…
AID/KERI	KERI impl. (eg Witness pool)	Any except…
Centr. VID	Enterprise VID (eg IAM)	Enterprise issued accts
Fed. VID	OpenID VID (eg OIDC)	Any except…

TSP is an Inter-Trust Domain Protocol (ITDP)
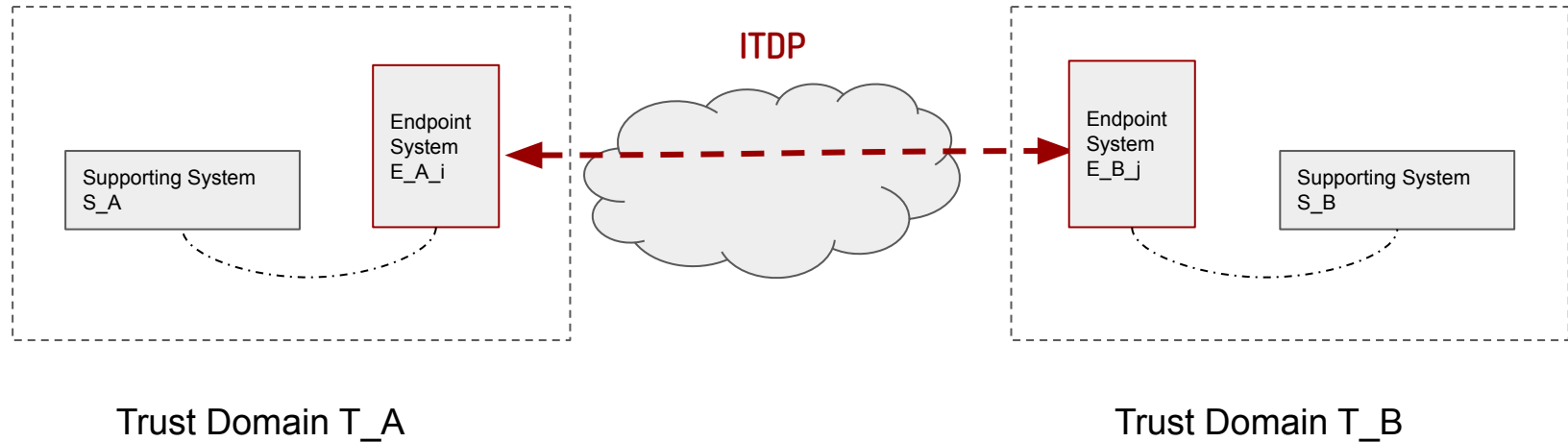
(2)The ITDP only bridges trust signal that EXISTS in trust domain A to trust domain B. It does not create new signals.

TSP is an Inter-Trust Domain Protocol (ITDP)

Trust Domain T_A   Trust Domain T_B
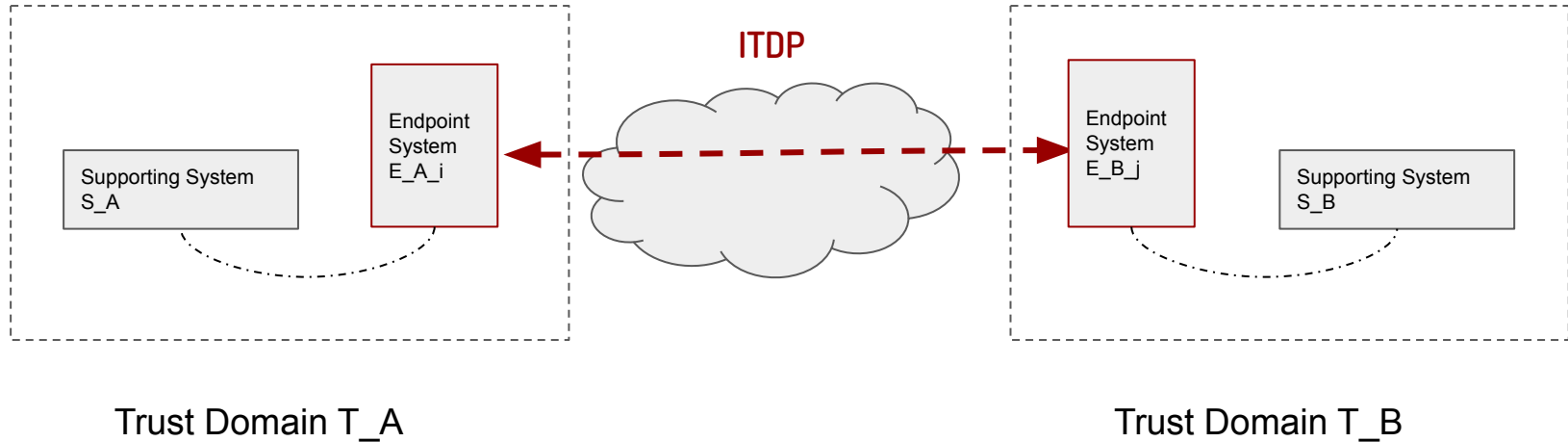
(3)The ITDP only enables the conveying of the trust signal. It is up to the endpoints to decide if those signals are indeed trustworthy or sufficient within the context that they know. (The End to End principle).

TSP is an Inter-Trust Domain Protocol (ITDP)

Trust Domain T_A
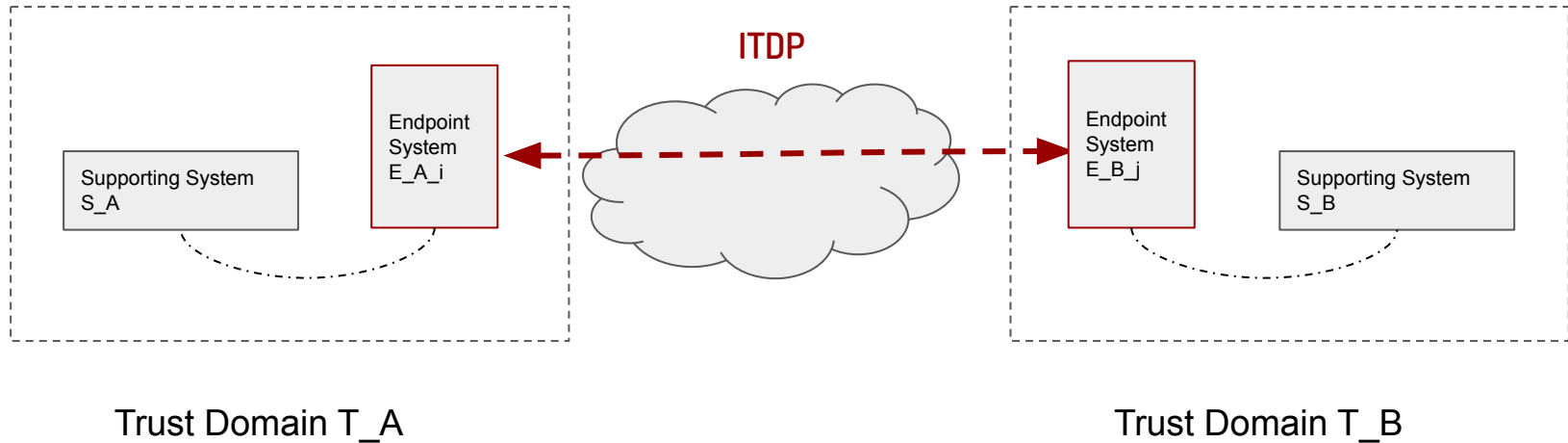
Trust Domain T_B

(4)ITDP only enables bootstrap of minimal level of trust between trust domains such that it's sufficient for they to continue to expand to more sophisticated levels of trust as they see fit.

TSP is an Inter-Trust Domain Protocol (ITDP)

Trust Domain T_A
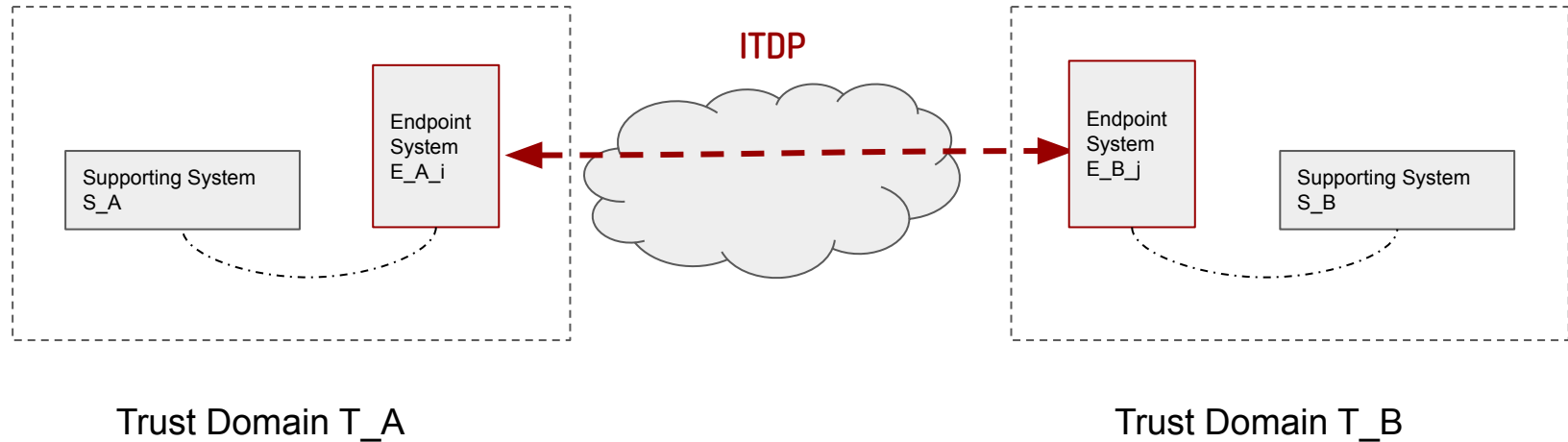
Trust Domain T_B

(5)After the bootstrap of minimally sufficient trust between trust domains, the ITDP is also the channel and language in which they can maintain & expand to more sophisticated trust levels as needed.

Wenjing Chu

TSP is an Inter-Trust Domain Protocol (ITDP)

Trust Domain T_A   Trust Domain T_B
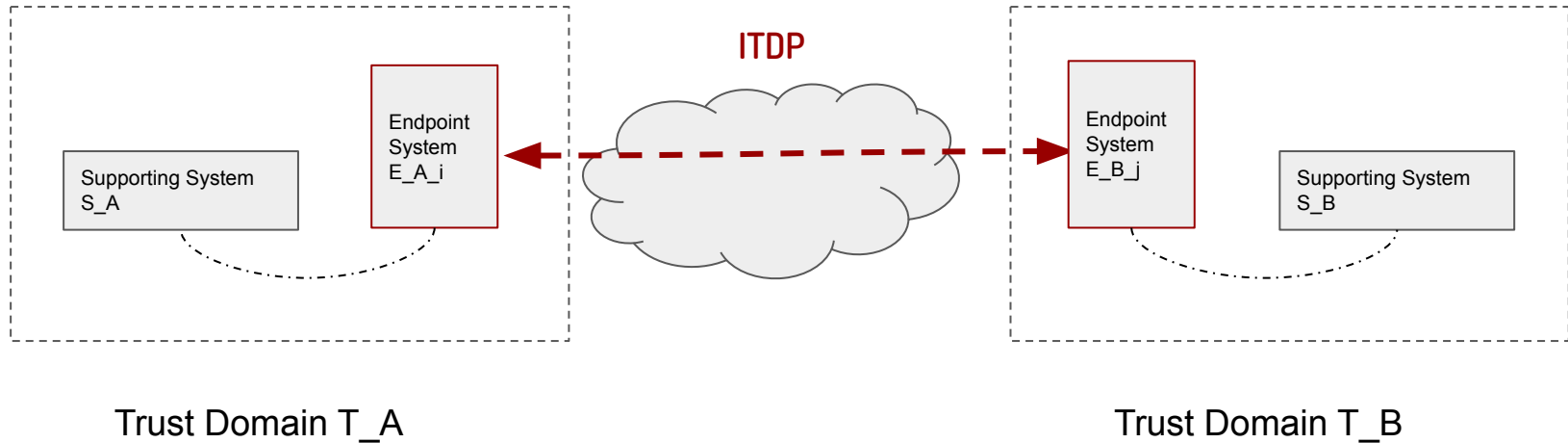
(6)Speakers of ITDP are any generic endpoints without much constraints – mobile, web, IoT, physical vs. virtual, human associated vs. objects, large vs. small vs. tiny, individualized vs. clusters vs. platforms vs. clouds, nor of their roles ... could be any of above, all of above, none of above or any mix we can't yet imagine.

(3)Less is More - What ITDP should and shouldn't do.

What ITDP shouldn't do…

It doesn't mean it shouldn't be done.

It doesn't mean it's unimportant.

It doesn't mean it's not related.

It just means better let others/protocols do it.

"Other layers of the same stack"

"Or other stacks entirely"

"Could be in a separate 'guide'"

"The principle of Separation of Concerns."

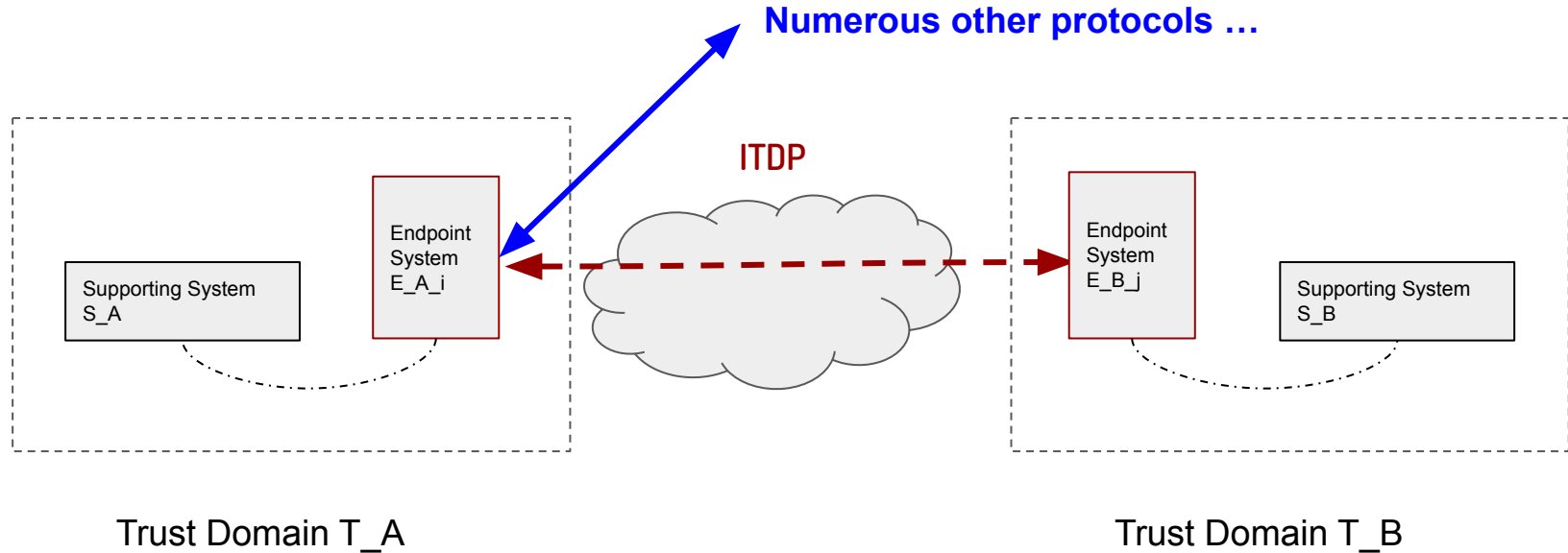**"The Hourglass principle"**

TSP is an Inter-Trust Domain Protocol (ITDP)

Trust Domain T_A
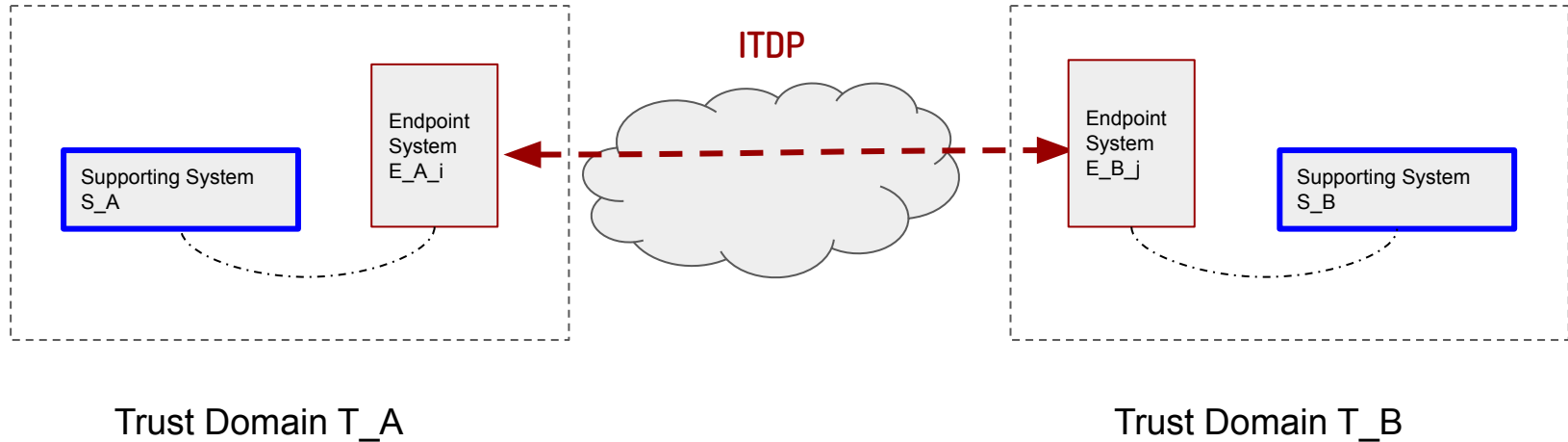
Trust Domain T_B

(7)Supporting systems themselves (e.g. blockchains, KERI witnesses, trust registries, reputation...) are out of scope, except the interface to them by the endpoints.

# TSP is an Inter-Trust Domain Protocol (ITDP)

Intermediary Systems perform Message Forwarding & other intermediating functions. They are beneficial in many aspects but not mandatory.

Intermediary System

Intermediary System

Endpoint System A

Internet

Endpoint System B

Privileged and Unprivileged Supporting Systems

Privileged and Unprivileged Supporting Systems
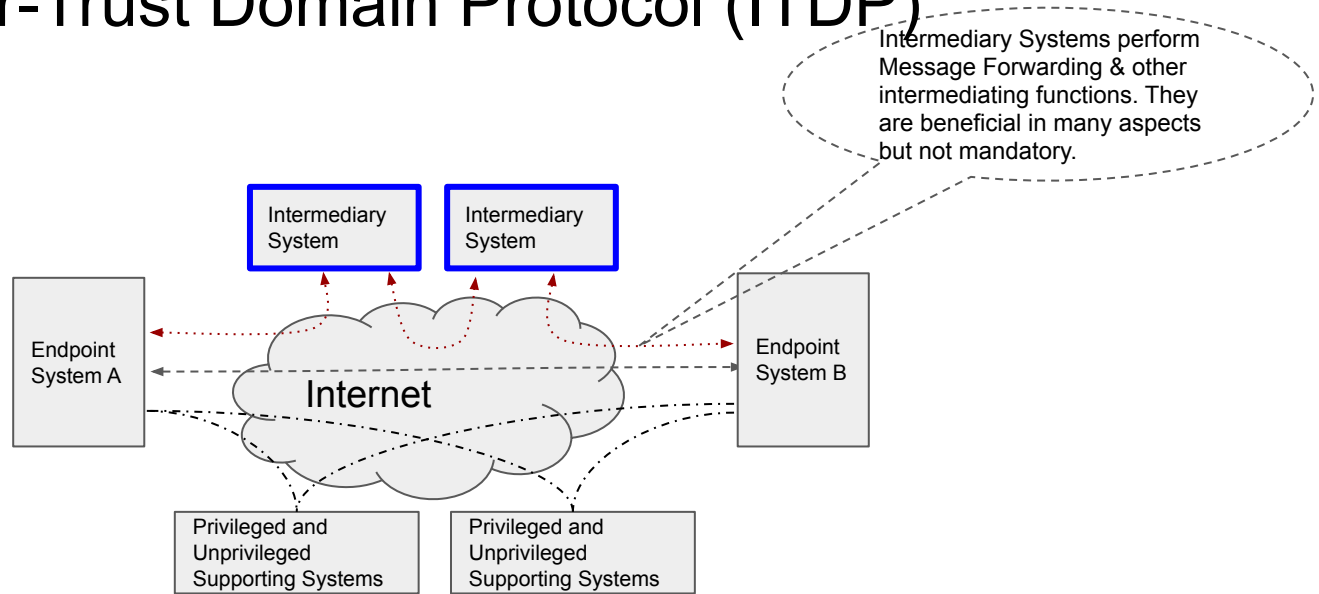
(8)Intermediary systems themselves (e.g. message routing, message storage, discovery...) are out of scope, except the interface to them by the endpoints.

TSP is an Inter-Trust Domain Protocol (ITDP)

Numerous other protocols …

ITDP

Endpoint System E_A_i

Supporting System S_A

Endpoint System E_B_j

Supporting System S_B

Trust Domain T_A

Trust Domain T_B

(9)The endpoints are likely to use numerous other protocols not directly concerned with bridging trust – they are all out of scope, and not depicted in my diagrams if not strictly necessary.
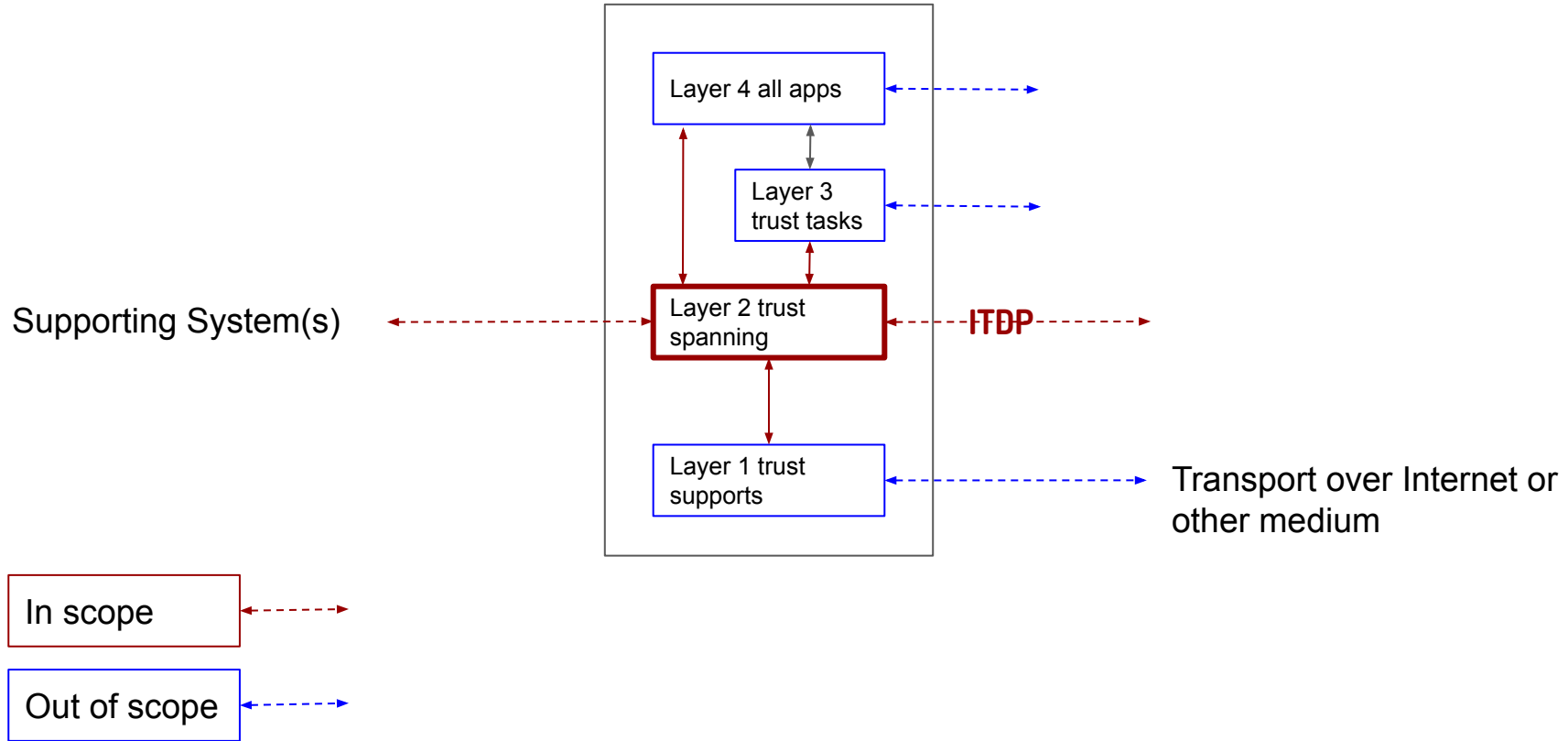
TSP is an Inter-Trust Domain Protocol (ITDP)

Trust Domain T_A

Trust Domain T_B
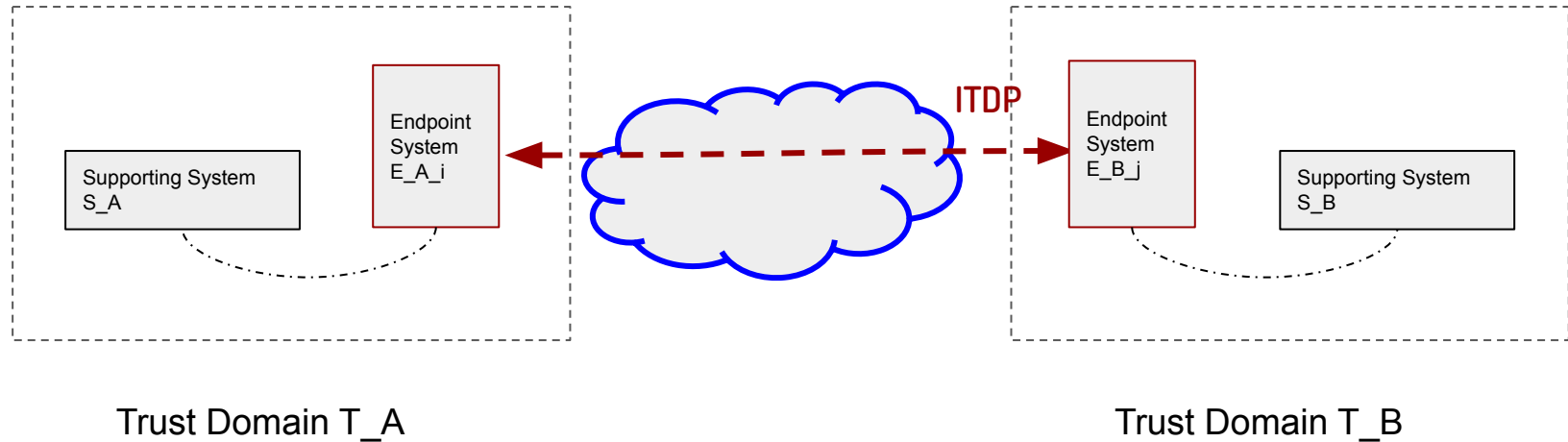
(10)The Internet (or other networking technologies) supports numerous communication or messaging functions – all of them are available for ITDP to use regardless of their layers within the Internet. ITDP uses them but they themselves are out of scope except the interface to use them.
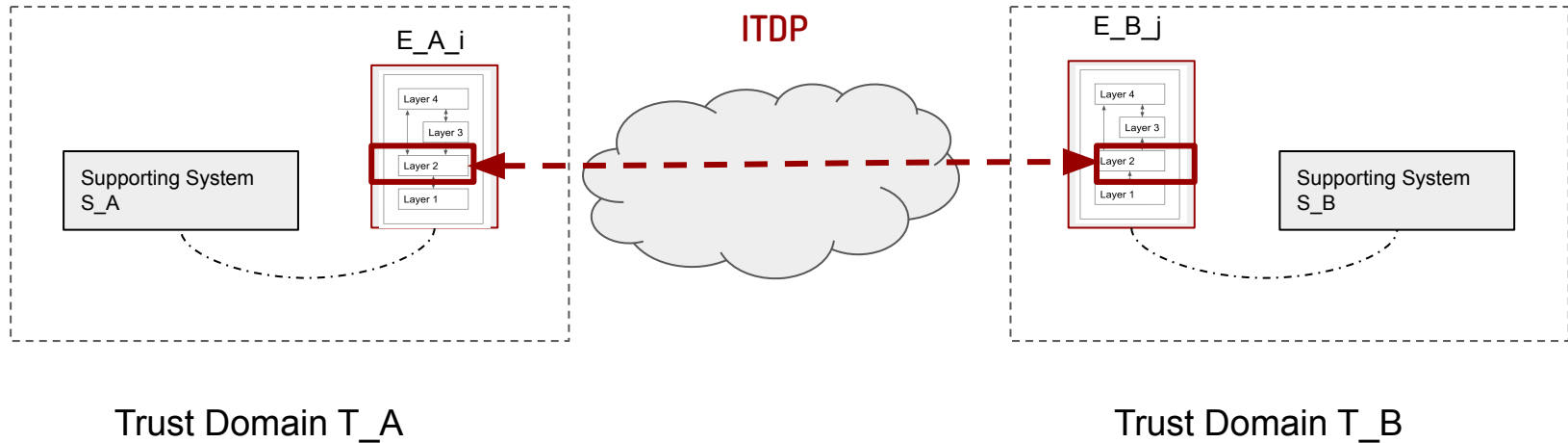
Wenjing Chu

TSP is an Inter-Trust Domain Protocol (ITDP)

Trust Domain T_A
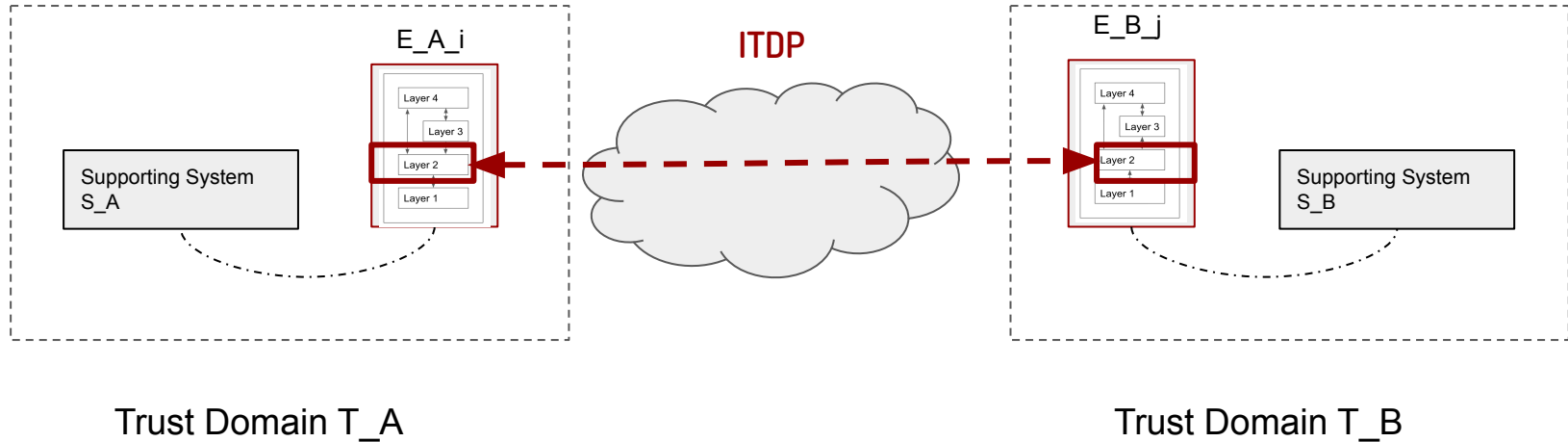
Trust Domain T_B

Then we can narrow down to what is in scope within the stack of an endpoint and specifically in the trust spanning layer (or layer 2).

An Endpoint's Trust Protocol Stack

Supporting System(s)

Layer 4 all apps

Layer 3 trust tasks

Layer 2 trust spanning

ITDP

Layer 1 trust supports

Transport over Internet or other medium

In scope

Out of scope

TSP is an Inter-Trust Domain Protocol (ITDP)

ITDP

E_A_i

E_B_j

Layer 4
Layer 3
Layer 2
Layer 1

Supporting System S_A

Supporting System S_B

Trust Domain T_A

Trust Domain T_B

(11)ITDP needs to support a *generic identification* that can be efficiently mapped to trust domain specific addresses AND can be verified for authenticity (*verifiable*). Both are required and should be efficient. The actual implementations of such generic verifiable identification are out of scope.

Wenjing Chu

TSP is an Inter-Trust Domain Protocol (ITDP)

(12)ITDP needs to have a *generic language* to express necessary trust signals and handshake protocols (i.e. primitives and messages) to bootstrap, maintain and enable further exchange for additional trust signals. The actual transport of messages and additional trust exchange protocols (e.g. VC issuance and presentation/proof) are out of scope.

TSP is an Inter-Trust Domain Protocol (ITDP)
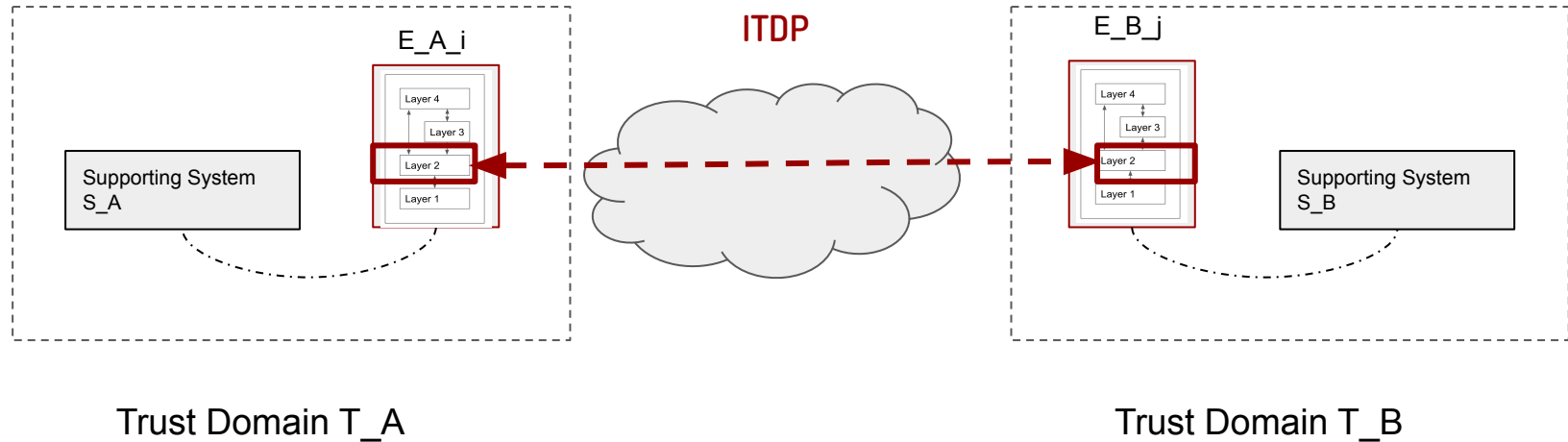
(13) ITDP establishes the minimum level of trust between endpoints, but it is not a tunneling protocol (unlike IP). The trust related information exchanged through ITDP can be used by the endpoints in any way they like, including creating tunnels or connections. Some can be, but Many such data exchanges are not tunneled through or encapsulated in ITDP. State it in another way, ITDP is a new tool that those data exchange protocols can use for trust.

TSP is an Inter-Trust Domain Protocol (ITDP)


Trust Domain T_A
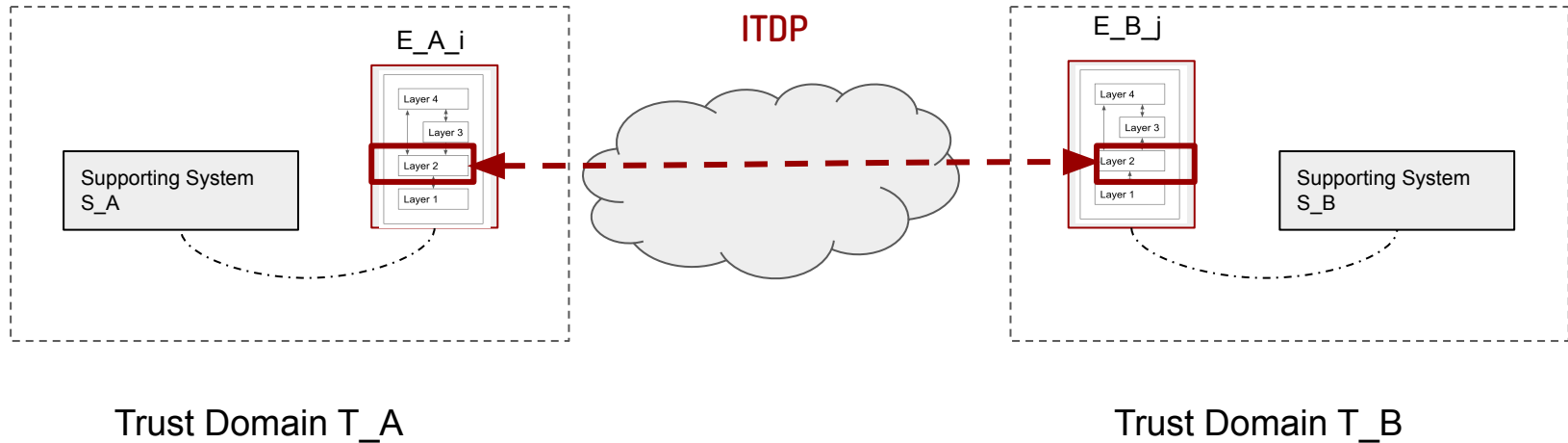
Trust Domain T_B

(14)ITDP supports multicast, anycast, broadcast in addition to unicast. An intermediary with an VID (i.e. destination) can perform these distribution functions.

Wenjing Chu

TSP is an Inter-Trust Domain Protocol (ITDP)
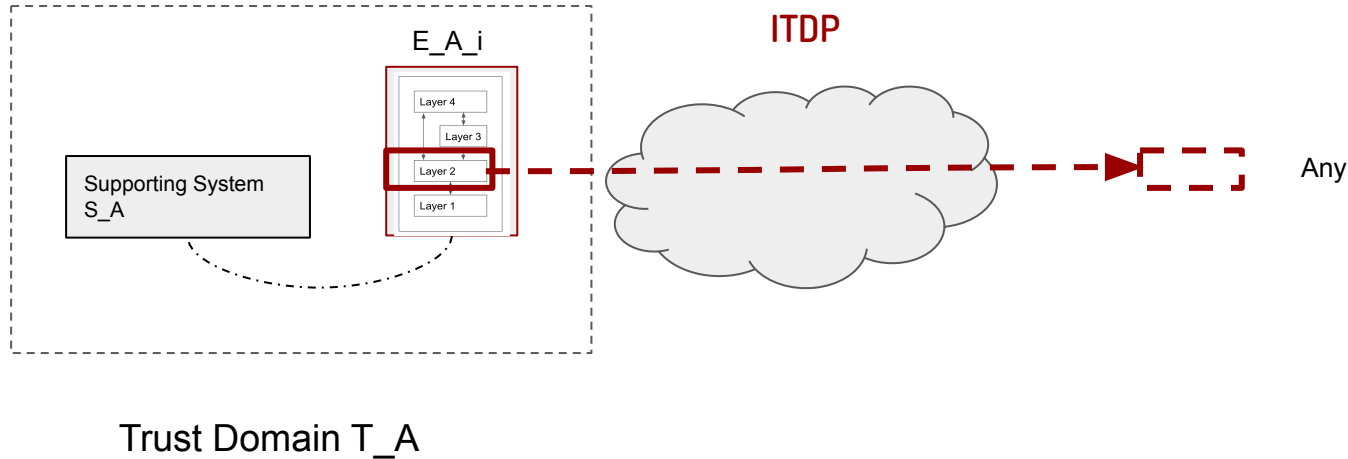
(15) ITDP may function without a destination VID. If used in this way, it should mean "To whom it may concern". And verification is one-direction only. It will be delivered to an intermediary (well known or pre-configured or known in other ways) whose interpretation of the message's handling is out of scope.
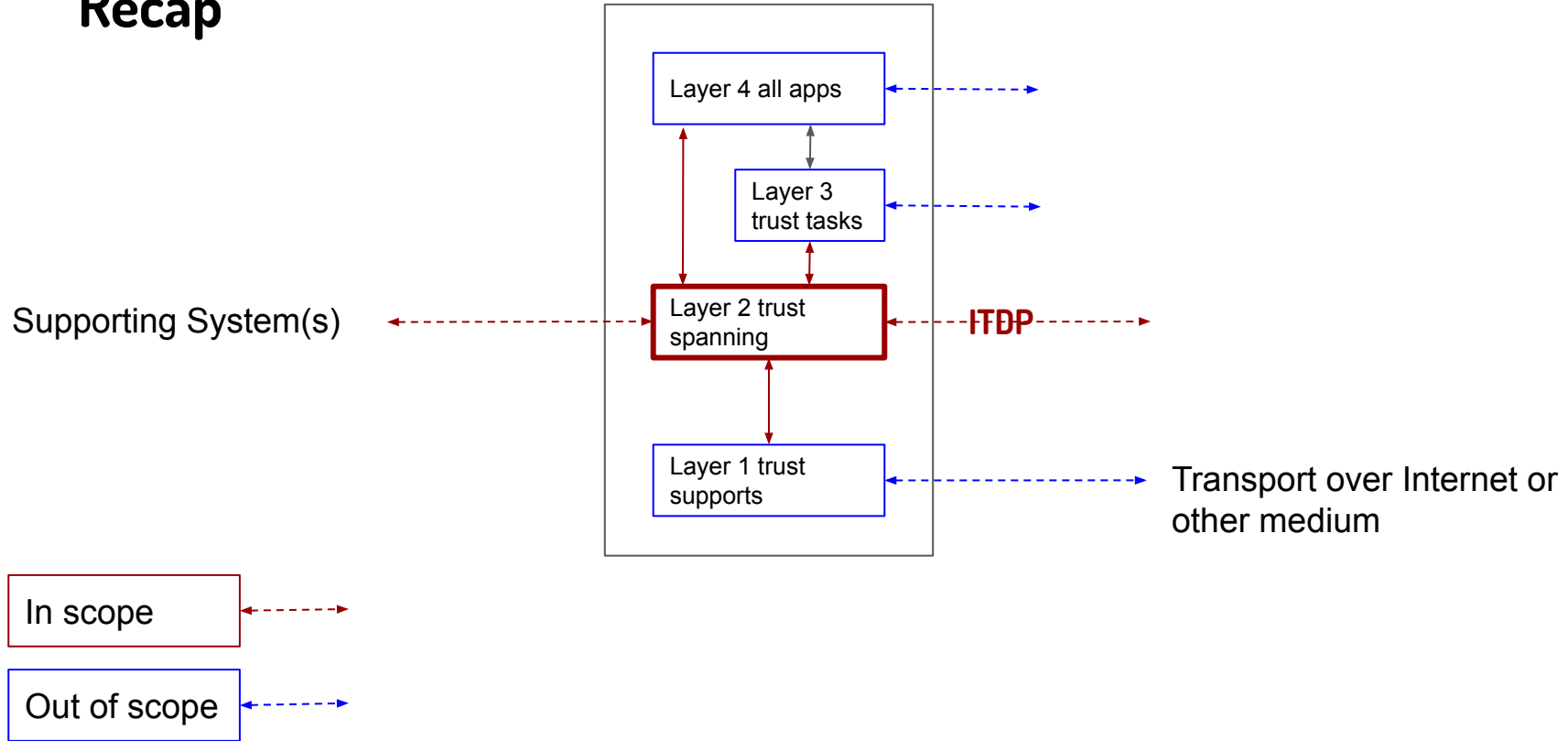
Wenjing Chu

TSP is an Inter-Trust Domain Protocol (ITDP)
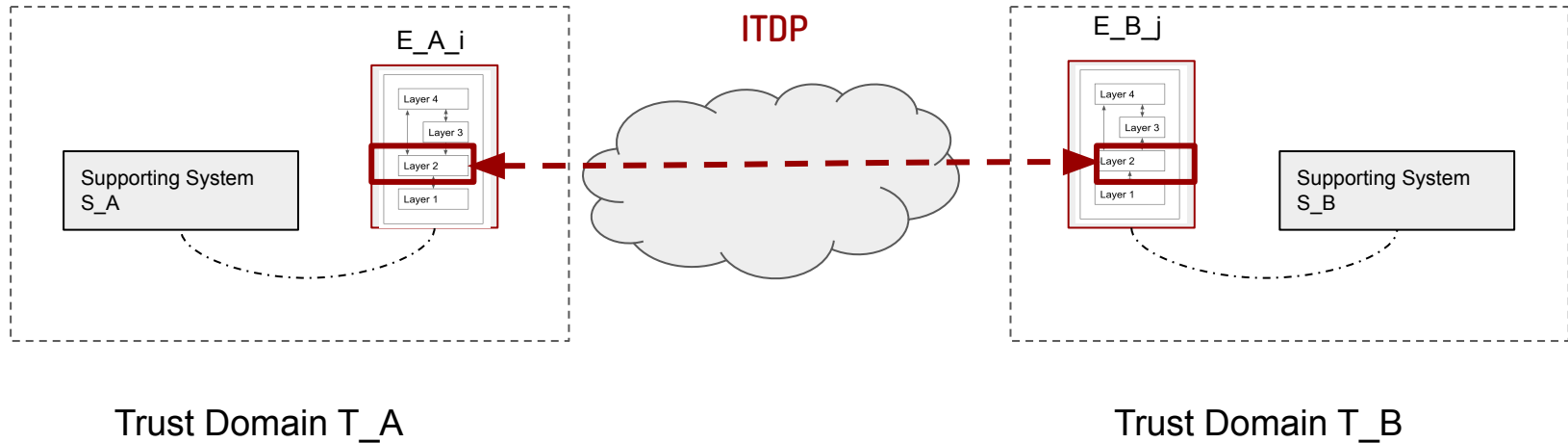
(16)ITDP can sit on top of any message delivery functions with wide/global reachability. Implementing those delivery functions are out of scope. There are numerous examples of such functions with global reachability.
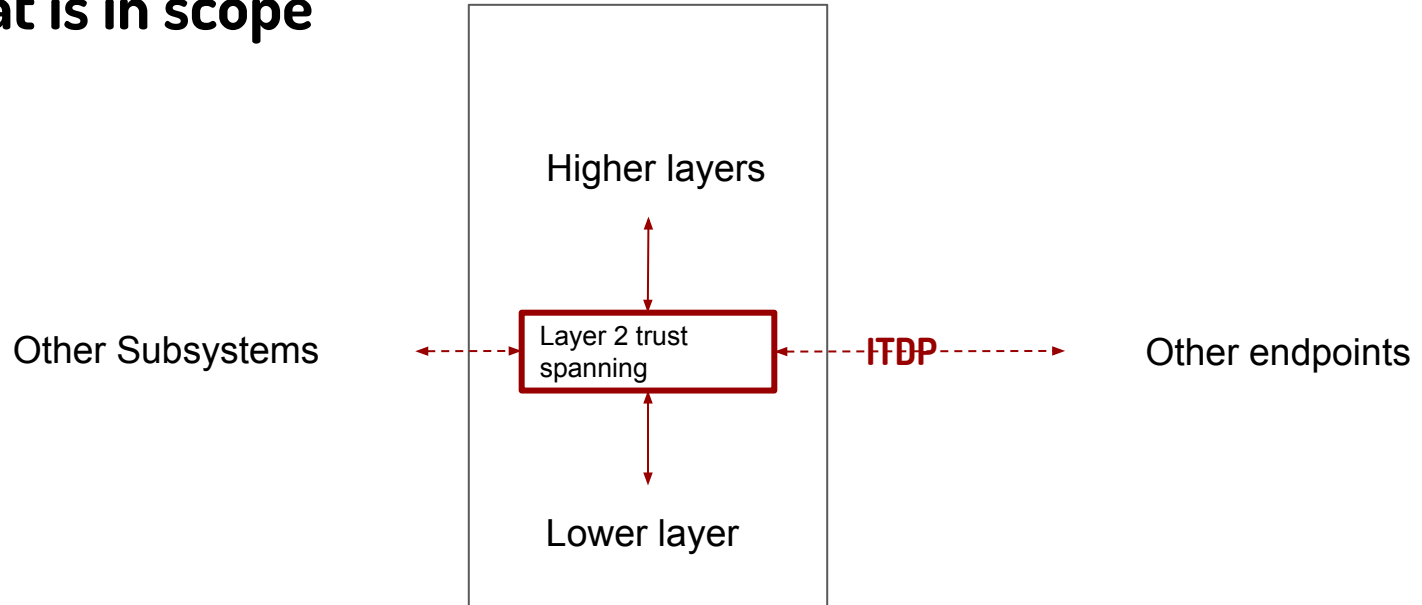
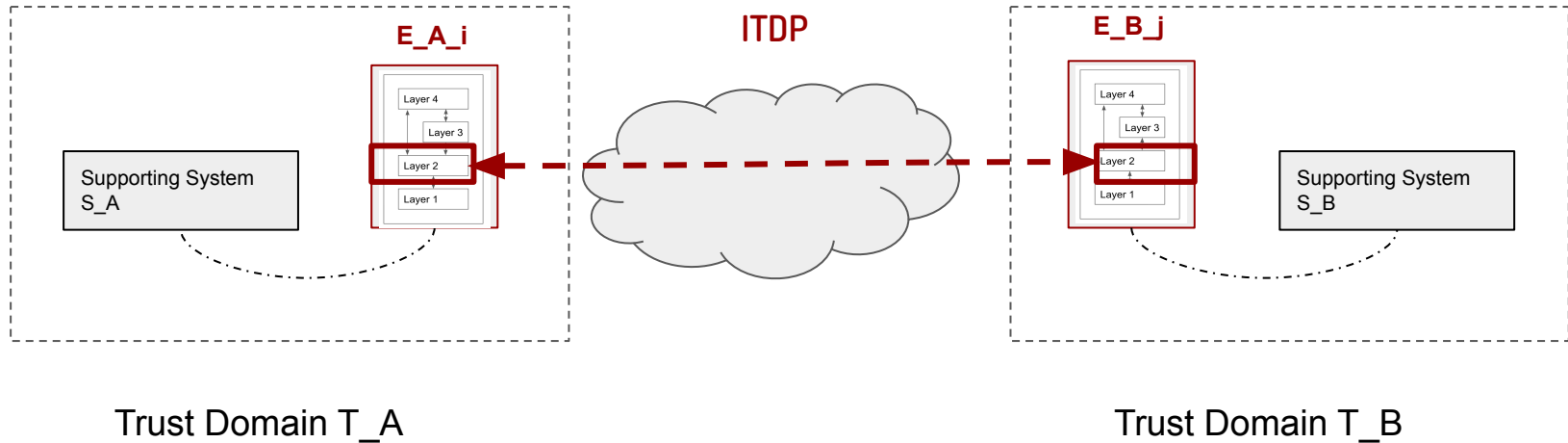# (4)What the ITDP specification defines.

Recap

An Endpoint's Trust Protocol Stack

Supporting System(s)

Layer 4 all apps

Layer 3 trust tasks

Layer 2 trust spanning — ITDP

Layer 1 trust supports

Transport over Internet or other medium

In scope

Out of scope

What is in scope

Higher layers

Other Subsystems

Layer 2 trust
spanning

ITDP

Other endpoints

Lower layer

TSP is an Inter-Trust Domain Protocol (ITDP)


Trust Domain T_A

Trust Domain T_B

(17)ITDP defines a generic, trust domain agnostic, adaptable, multi-format identification scheme. This scheme must satisfy most common schemes existed today and leave flexibility for future adaptation. (e.g. DID core...)

TSP is an Inter-Trust Domain Protocol (ITDP)
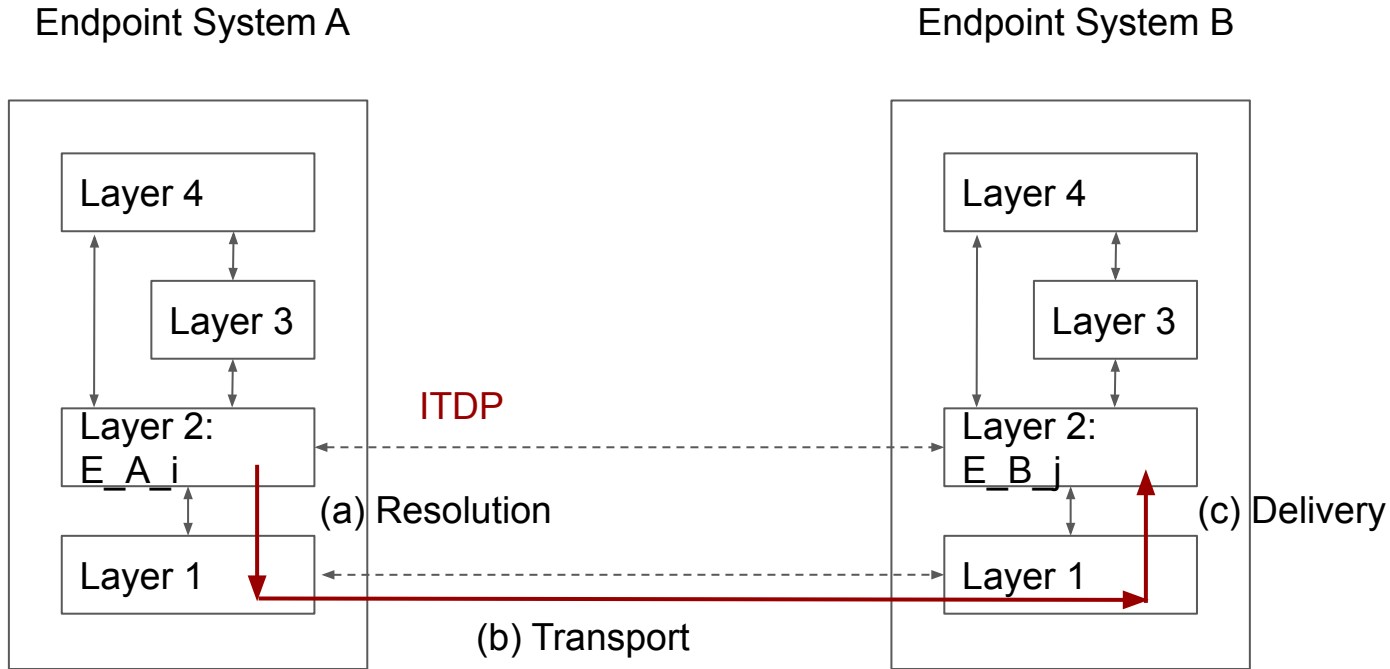

Trust Domain T_A

Trust Domain T_B
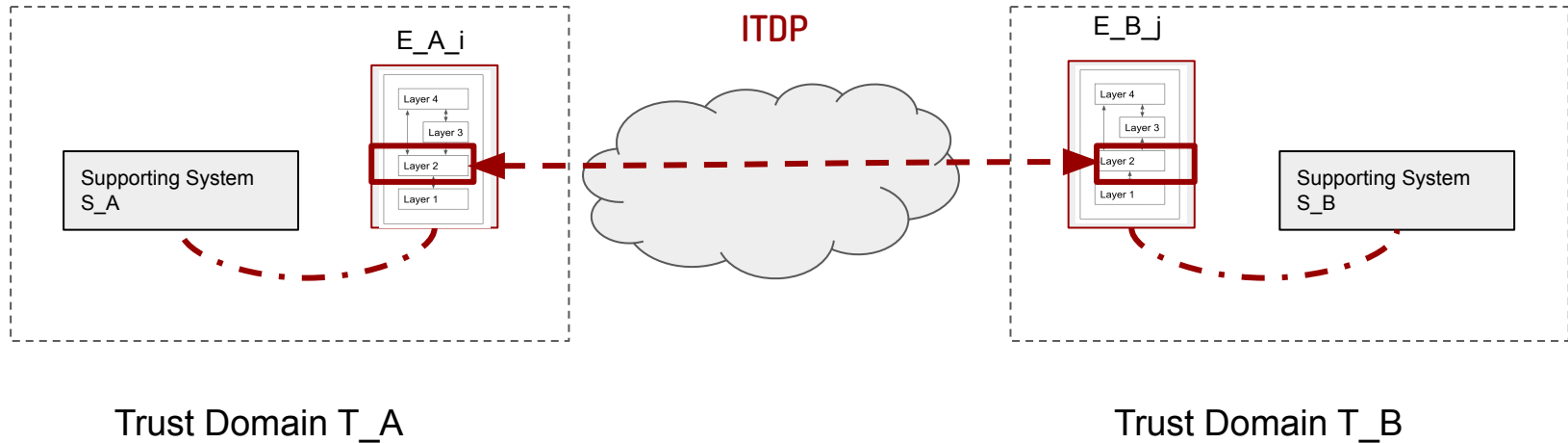
(18)ITDP defines a generic interface for management of identifications that supports all types of identifications. (e.g. major DID methods, AID/KERI, OpenID, other central/federated/distributed verifiable IDs.) This includes create, renewal/rotation, delete... operations.

Wenjing Chu

TSP is an Inter-Trust Domain Protocol (ITDP)
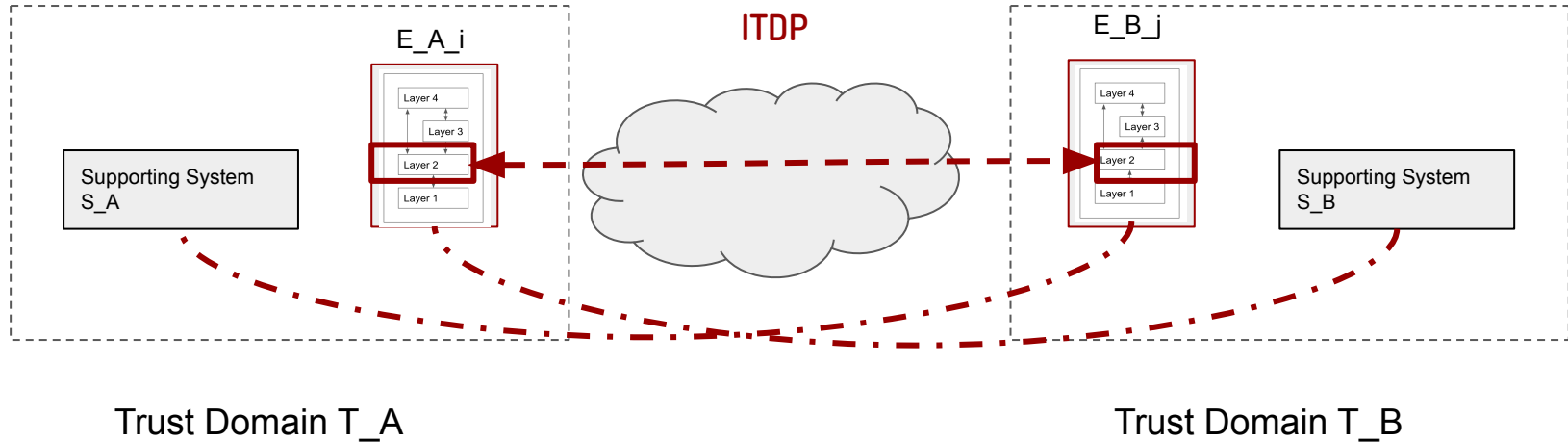
(19)ITDP defines a generic interface for verification of authenticity of all supported types of identifications.

Endpoint System A

Endpoint System B

Layer 4

Layer 3

Layer 2:
E_A_i

ITDP

(a) Resolution

Layer 1

Layer 4

Layer 3

Layer 2:
E_B_j

(c) Delivery

Layer 1

(b) Transport

(20)ITDP defines a generic identification resolution, transport and delivery (RTD) procedure that can be efficiently realized in existing implementation methods and flexible enough for future adaptation. Note: this generic procedure is able to accommodate numerous variations of how it can be satisfied. Please do not assume it is a simple process as depicted in the generic diagram above.

Endpoint System A

Layer 4

Layer 3

Layer 2:
E_A_i

ITDP

(a) Resolution

(c) Delivery

Layer 1

Layer 1

(b) Transport
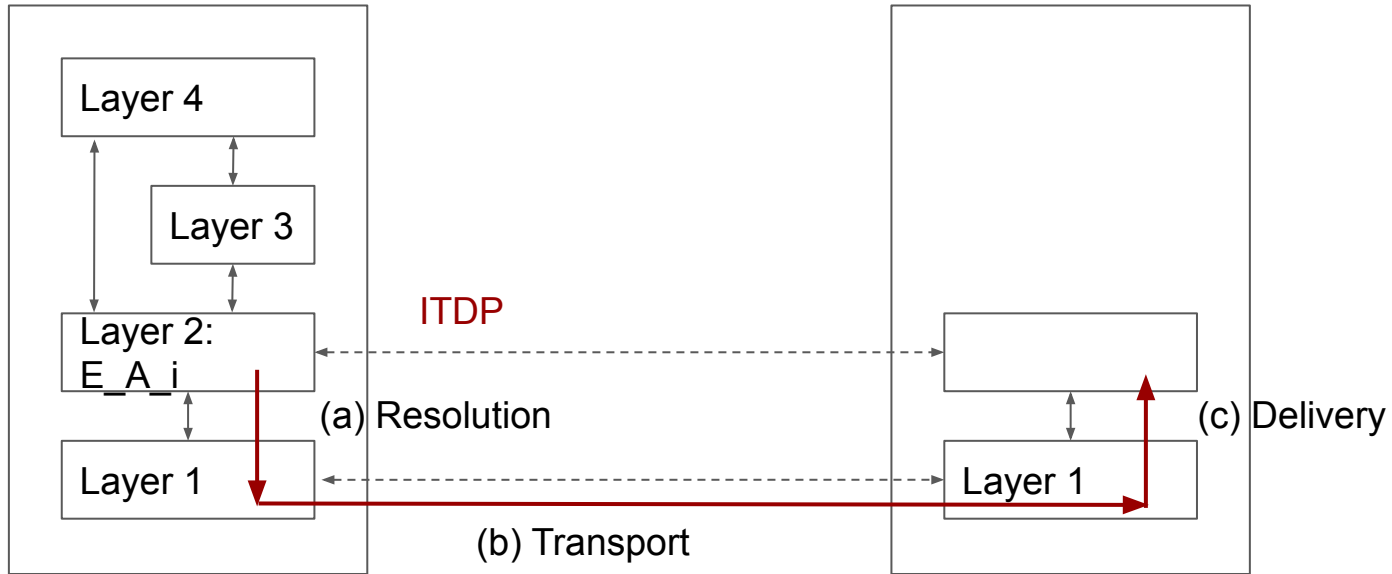
(21)As a special case, this RTD procedure can also support implicit destinations (e.g. without destination ID), including the default Internet without trust enhancement, or intermediaries. Note: if the destination does have a ID with special meaning, then it's the same procedure – may include additional handling.

TSP is an Inter-Trust Domain Protocol (ITDP)
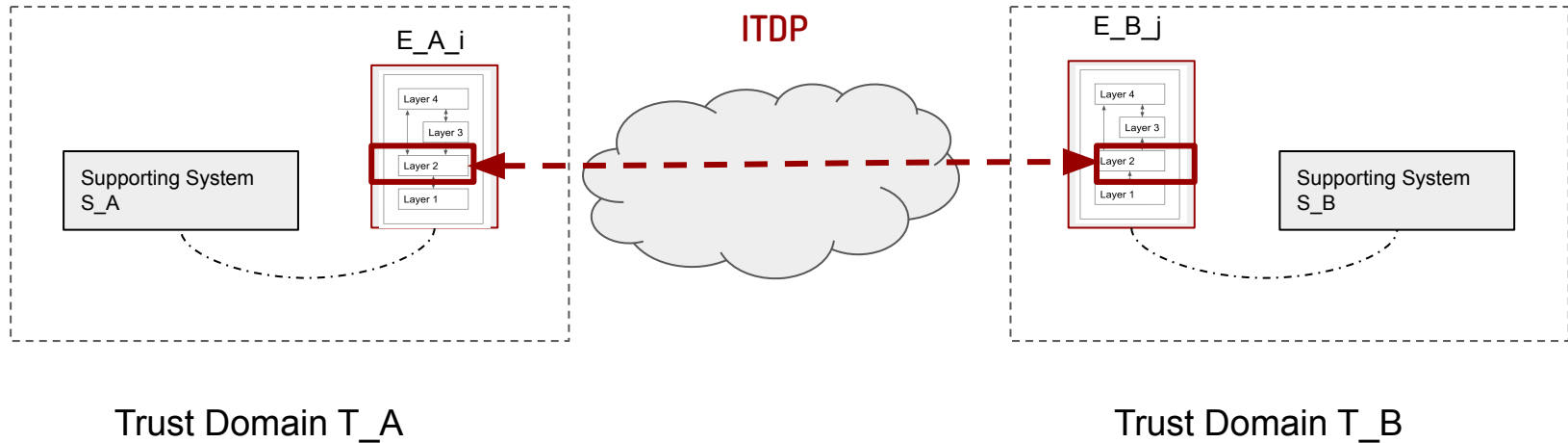

Trust Domain T_A

Trust Domain T_B
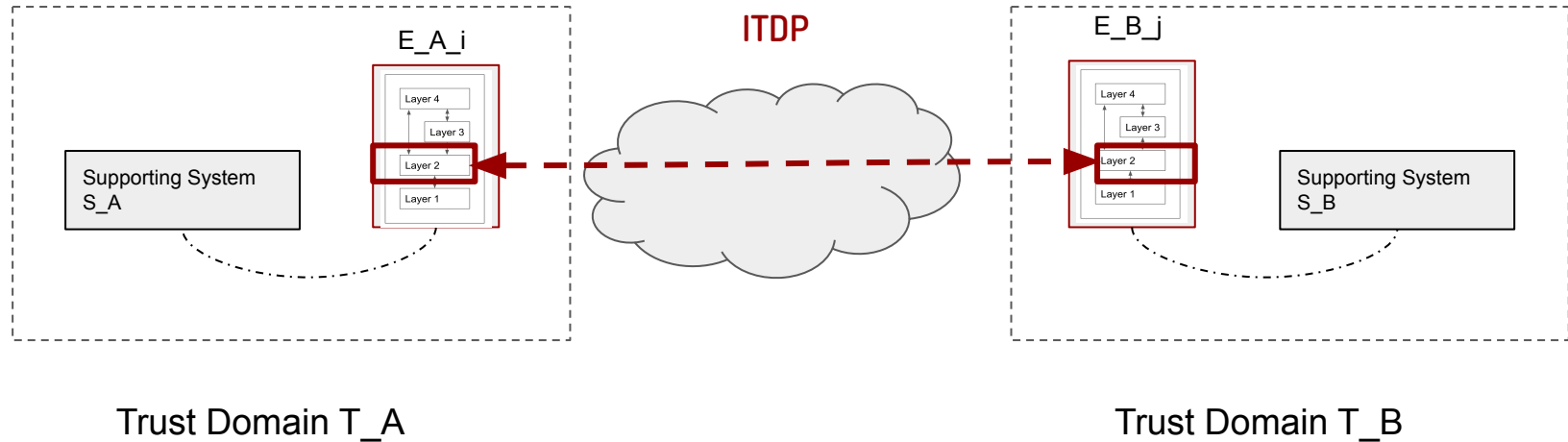
(22)ITDP defines a set of message types, format and how to use them in a dialogue (i.e. the language). This set is extendable. The minimum set is required which enables (a) the initial bootstrap (or introduction), (b) to initiate additional steps if needed, (c) to renew/update, delete, debug, or the equivalent/similar operations existed in various methods. This minimum set must be defined in ITDP.
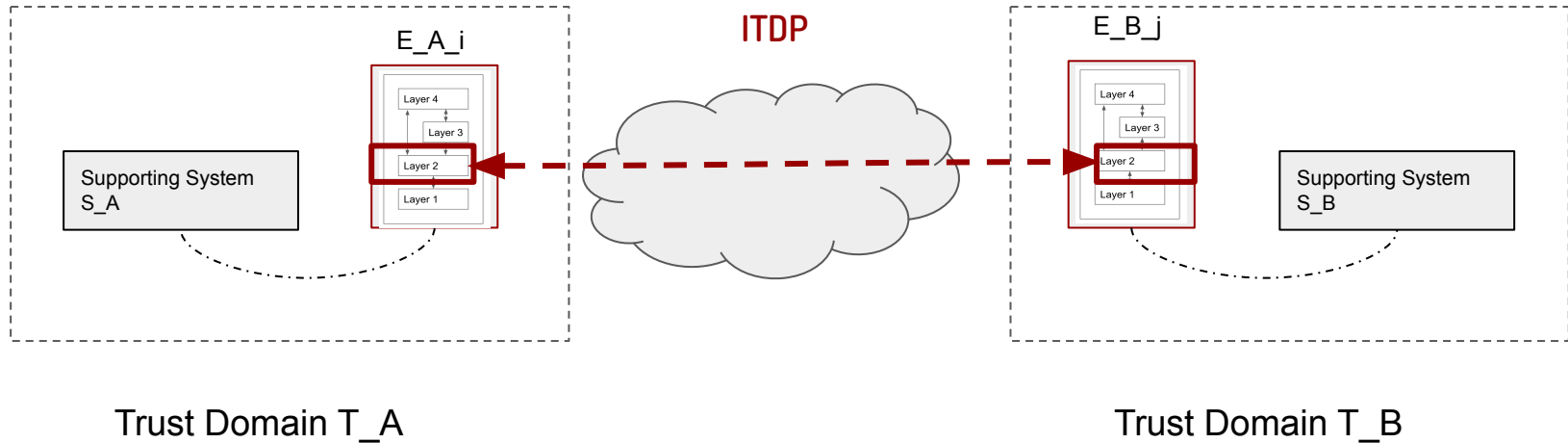
TSP is an Inter-Trust Domain Protocol (ITDP)
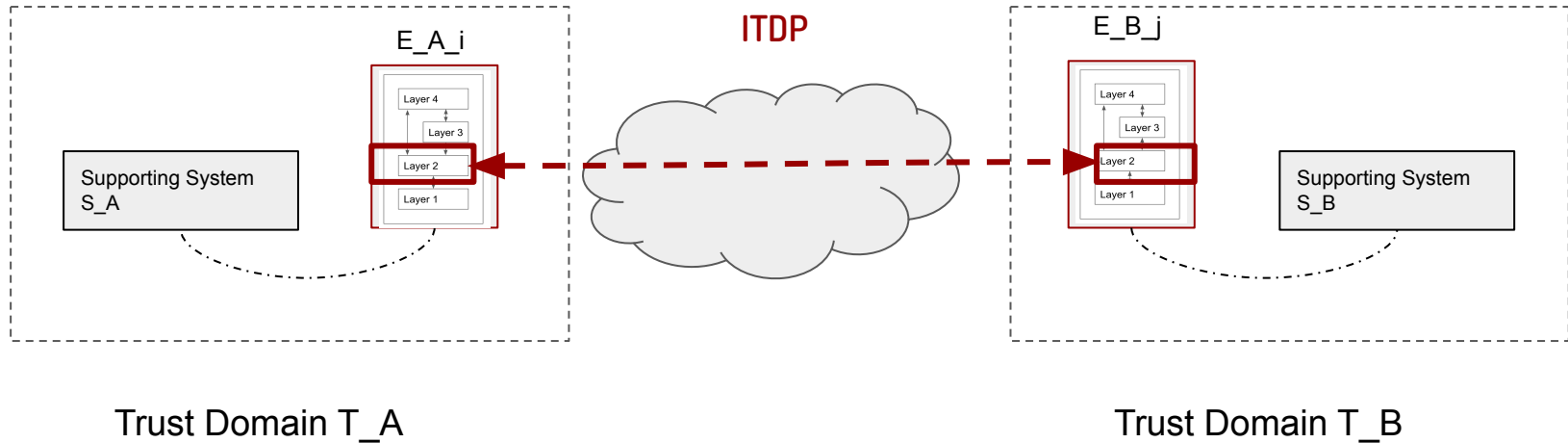
(23)ITDP can use any transport/messaging mechanism – including encoding schemes – existed today or newly created in future – in any of layers on Internet or any other means. The messaging mechanism may have any types of semantics as long as it can support the minimum unidirectional best effort delivery (similar to IP or UDP's assumptions in this regard). These transport mechanisms themselves are out of scope.

TSP is an Inter-Trust Domain Protocol (ITDP)

(24)ITDP messages incorporate primitives to protect their own content for message integrity, confidentiality and privacy. Some aspects of these may be left out optionally in some context. Note: again ITDP is not a tunneling protocol.

Wenjing Chu

TSP is an Inter-Trust Domain Protocol (ITDP)

Trust Domain T_A

Trust Domain T_B

(25)In summary, ITDP is a decentralized, distributed, peer-wise protocol designed for establishing and managing public key based trust of authenticity across different trust domains, including trust domains that utilize different trust frameworks such as centralized, federated, decentralized or future evolutions of them.

Wenjing Chu

(5)How various trust tasks can be built on top of ITDP (TSP)? How does ITDP relate to other protocols (forerunners)?

Wenjing Chu

Slides skip until next presentation

(6)How lower layer support functions may implement what ITDP needs?

Slides skip until next presentation

(7) Q&A

- Public Reference to this doc should be in its entirety and as: {Wenjing Chu, "TSP is an Inter-Trust Domain Protocol (ITDP)", Feb 21, 2023. https://github.com/wenjing/Inter-Trust-Domain-Protocol}.
- Presentation on the Reference Architecture at IIW-34:
  - https://youtu.be/QZssxxZ9f88
  - https://github.com/windley/IIW_homepage/blob/gh-pages/assets/proceedings/IIW_34_Book_of_Proceedings.pdf
- ToIP TechArch specification: https://github.com/trustoverip/TechArch