Version 0.31

PROPOSAL 4 TO TOIP TSL TF

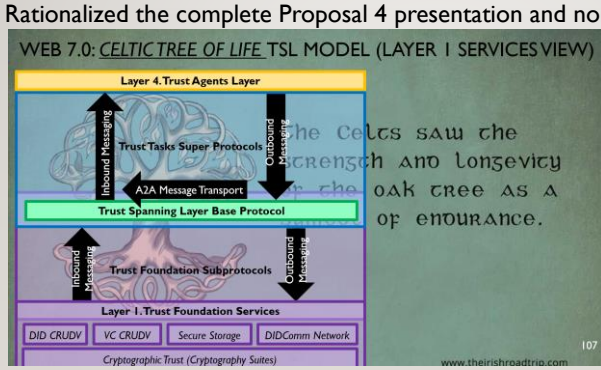
DID COMMUNICATIONS (DIDCOMM) PROTOCOL AS THE *BASIS* FOR A UNIFIED TRUST SPANNING LAYER BASE PROTOCOL

MICHAEL HERMAN
SELF-SOVEREIGN BLOCKCHAIN ARCHITECT, DEVELOPER, AND FUTURIST
TRUSTED DIGITAL WEB
HYPERONOMY DIGITAL IDENTITY LAB
PARALLELSPACE CORPORATION
BINDLOSS, ALBERTA, CANADA / CHELEM, MEXICO

1

CHANGE LOG VERSION 0.31 (FINAL 5)

1. Rationalized the complete Proposal 4 presentation and nomenclature around the model in Slide 107



2. Added Appendix D: Two-Layer Honey-Peanut Butter-Jelly Model for Trust Spanning Layer Frameworks. See Slide 118

2

2

CHANGE LOG
VERSION 0.30 (FINAL 4)

1. Appendix A: Added slide Web 7.0: Celtic Tree of Life TSL Model (Trust Foundation Services View). See slide 106
2. Appendix C added: Trust Protocol Profile-Trust Spanning Layer Framework: Trust Protocol Profile Example Scenarios. See slide 113
3. Appendix C: Added slide Trust Protocol Profile-Trust Spanning Layer Framework: Proposal 4 Assessment. See slide 114
4. Appendix C: Added slide Trust Protocol Profile-Trust Spanning Layer Framework: Assessment of Other Proposals. See slide 115

3

3

CHANGE LOG
VERSION 0.28 (FINAL 3)

1. Appendix B added: Data Replication (Subscribe/Publish) Scenario : Publisher-Notify/Subscriber-Pull Super Protocol. See slide 106.

4

4

CHANGE LOG
VERSION 0.27 (FINAL 2)

1. Appendix A added: Celtic Tree of Life Trust Spanning Layer Model (Implementation View). See slide 102. Thank you Joe Spencer for the feedback.
2. Clarification: While DIDComm Message Attachments are formally part of (in-scope for) Proposal 4, Verifiable Credentials, a specific category of attachment, only represent one type of DIDComm Message Attachment (that is used for illustration purposes). The content/payload of a DIDComm Message Attachment can be anything (e.g. mDLs, Microsoft Office documents, XML documents, images/photos, etc.). Thank you Wenjing Chu for asking for this clarification.
3. Attachments can be imbedded in a DIDComm Message or external to a DIDComm Message (attached "by reference"). See slide 69.
4. "Verifiable Credential Sender-Receiver Model" renamed to "Credential Sender-Receiver Pattern".
5. Slide 85 added: Side Bar: Web 7.0 DIDComm DID Registry Gateway: Automatic Agent Code Generation. A response to the question about Hyperledger vs W3C DID Resolution protocol support.

5

SINGULAR PURPOSE OF THE PROPOSAL 4 CONTRIBUTION AND TODAY'S PRESENTATION

1. To table the complete Proposal 4 story – end-to-end – supporting the following proposition:
   - *DID Communications (DIDComm) Protocol as the basis for a Unified Trust Spanning Layer Base Protocol*

Proposal 4 represents a Unified Trust Spanning Layer Base Protocol solution based on readily available, proven, comprehensive, understandable Internet technologies and specifications

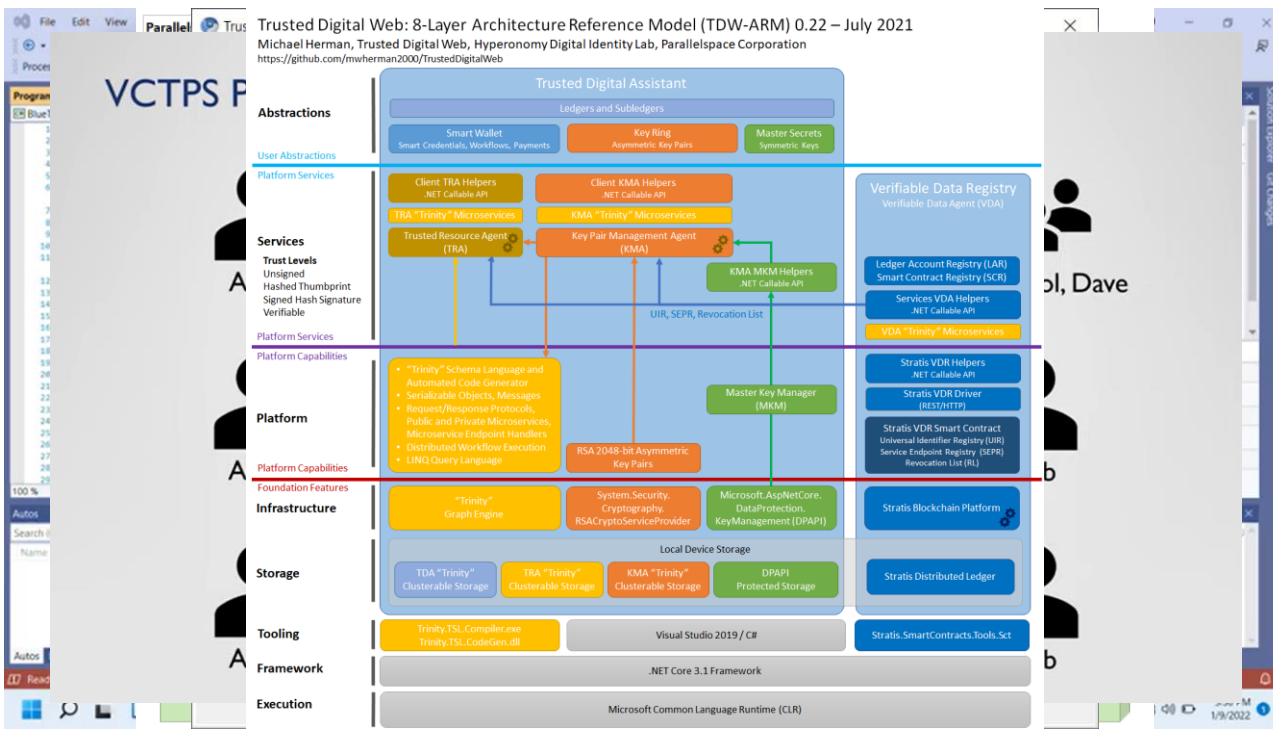
6

First Principles Thinking

> "Sometimes called "reasoning from first principles," the idea is to break down complicated problems into basic elements and then reassemble them from the ground up. It's one of the best ways to learn to think for yourself, unlock your creative potential, and move from linear to non-linear results."
>
> *First Principles: The Building Blocks of True Knowledge (https://fs.blog/2018/04/first-principles/)*

> "I think it is most important to reason from first principles rather than by analogy. One of the ways we conduct our lives is we reason by analogy. We do this because something was like something else that was done or it was like what other people were doing. It's mentally easier to reason by analogy rather than from first principles."
>
> *First Principles Method Explained by Elon Musk (https://www.youtube.com/watch?v=NV3sBlRgzTI)*

7



8

PROPOSAL 4 : TRUST SPANNING PROTOCOL TASK FORCE

- Mission
  - The mission of the TSWG is to draft the ToIP Trust Spanning Protocol V1.0 Specification to meet the requirements for ToIP Layer 2 as specified in the ToIP Technology Architecture V1.0 Specification.
- Deliverables
  - The deliverable of this Task Force is the ToIP Trust Spanning Protocol Specification that must meet the 18 requirements for the ToIP Layer 2 protocol as specified in the ToIP Technology Architecture V1.0 Specification.

9

ToIP Layer 2 Trusted Spanning Protocol Assessment Checklist

TAS Req #	Requirement	Section	Brian Richter's DIDComm V2 Comments	Daniel's DIDComm v2 Comments	Overall Assessment
L2.1	A ToIP Endpoint System MUST communicate with another ToIP Endpoint System using the ToIP Trust Spanning Protocol.	7.3	Yes. DIDComm only talks to DIDComm	yes	Meets requirement
L2.2	A ToIP identifier MUST be unique within the context in which it is used for identification.	8.2	DIDs are used so yes they have this property	yes	Meets requirement
L2.3	A ToIP identifier MUST be a verifiable identifier, i.e., verifiably bound to at least one set of cryptographic keys discoverable via an associated discovery protocol.	8.2	Any DID method with the ability to have a serviceEndpoint can talk didcomm	yes	Meets requirement
L2.4	A ToIP identifier SHOULD be a decentralized identifier, i.e., a verifiable identifier that does not require registration with a centralized authority.	8.2	YES requirement of didcomm	yes	Meets requirement
L2.5	A ToIP identifier SHOULD be an autonomous identifier, i.e., a decentralized identifier that is self-certifying and fully portable.	8.2	I don't think this is met by didcomm as many did methods that are acceptable do not meet this requirement	yes. DIDComm supports this but doesn't require it	Meets requirement
L2.6	A ToIP identifier SHOULD support rotation of the associated cryptographic keys for the lifetime of the identifier.	8.2	DID methods that include key rotation can be used.	yes	Meets requirement
L2.7	A ToIP identifier MAY also support rotation to an entirely different ToIP identifier that can be cryptographically verified to be a synonym of the original ToIP identifier.	8.2	You can move a thread to a new DID entirely using the 'from_prior' property https://identity.foundation/didcomm-messaging/spec/#did-rotation	yes. DIDComm supports this, and AFAIK is the only tech that does so.	Meets requirement
L2.8	A ToIP identifier SHOULD support the ability to: a) associate the identifier with the network address of one or more ToIP Systems that can deliver to one or more Endpoint Systems under the locus of control of the ToIP identifier controller, and, b) if desired by the controller, enable that association to be discoverable.	8.2	Yes, service endpoints in DID document	yes	Meets requirement
L2.9	The ToIP Trust Spanning Protocol specification MUST define how to construct and format messages that are cryptographically verifiable to have the following four properties: (1) Authenticity: the message was sent from a sender who has control over the ToIP identifier. (2) Integrity: the contents of the message transmitted by the sender are received by the recipient without modification. (3) Confidentiality: the contents of the message are only accessible by authorized parties. (4) Privacy: the contents of the message are bound to conditions of usage agreed to by the parties	8.3	Definitely meets authenticity, integrity and confidentiality using auth-crypt. Not much in place re: message usage	Yes on the first 3. DIDComm doesn't have a defined strategy for #4, but has all the plumbing to easily create it. Wrt to point 4, this is handled by a DIDComm Protocol (a co-protocol (aka super protocol) derived from the base protocol).	Meets requirement

DID Communications

Submitted to the Task Force Feb. 24. 2023

10

DID Communications

Submitted to the Task Force Feb. 24. 2023

ToIP Layer 2 Trusted Spanning Protocol Assessment Checklist

TAS Req #	Requirement	Section	Brian Richter's DIDComm V2 Comments	Daniel's DIDComm v2 Comments	Overall Assessment
L2.10	In a ToIP Endpoint System, an implementation of the ToIP Trust Spanning Protocol MUST support authenticity and integrity.	8.3	Yes, authcrypt	yes	Meets requirement
L2.11	In a ToIP Endpoint System, an implementation of the ToIP Trust Spanning Protocol MAY support confidentiality and privacy.	8.3	Yes, encryption for confidentiality but privacy could be improved (lacks message usage terms)	yes. This is not a requirement of DIDComm, but rather of the implementations. A full implementation of the DIDComm spec would require support for confidentiality, but the DIDComm spec doesn't actually say if lesser implementations are still considered conformant.	Meets requirement
L2.12	The ToIP Trust Spanning Protocol MUST enable the composition of higher-level Trust Task Protocols (such features as co-protocols).	8.3	Yes, didcomm protocols on top of didcomm are used for this	yes	Meets requirement
L2.13	The ToIP Trust Spanning Protocol MUST support extensible message schema.	8.3	Yes	yes	Meets requirement
L2.14	The ToIP Trust Spanning Protocol MUST support resolution of ToIP identifiers to: a) the network addresses of receiving Endpoint Systems, and b) any required cryptographic keys.	8.4	Yes, DID resolution with service blocks and verification methods	yes	Meets requirement
L2.15	The ToIP Trust Spanning Protocol MUST support transport of messages via ToIP Layer 1 interfaces.	8.4	Yes	yes	Meets requirement
L2.16	The ToIP Trust Spanning Protocol MUST support delivery of messages to the Layer 2 interface of the Endpoint System of the ultimate receiver of the message.	8.4	Yes	yes	Meets requirement
L2.17	The ToIP Trust Spanning Protocol MUST support delivery of messages via Intermediary Systems.	8.4	Yes, DIDComm routes through mediators when required	yes	Meets requirement
L2.18	The ToIP Trust Spanning Protocol MUST support confidentiality with regard to the metadata required for message routing.	8.4	Uses routing "layers" similar to an onion so only relevant parties can see	yes	Meets requirement
					DID Communications (DIDComm) MEETS OVERALL REQUIREMENTS

11

11

File Message Help

Share to Teams Find

ToIP Layer 2 Trusted Spanning Protocol Assessment Checklist: COMPLETED. Assessment: P...

Reply Reply All Forward

Michael Herman (Trusted Digital Wel

To Drummond Reed (Gen) (drummond.reed@gendigital.com)

Cc Daniel Hardman (daniel.hardman@gmail.com); Brian Richter

Fri 2/24/2023 1:29 PM

Drummond, per our conversation from a couple of days ago, …

1. Daniel has provided his assessment of the DIDComm protocol relative to the 18 requirements
2. He added his comments to a copy of the Google spreadsheet you had sent me the link to. I ended up making a copy of yours because I was unable to edit it.
3. Brian had already added a full set of comments/feedback. I transposed Brian's comments into a companion set of comments in their own column alongside Daniels.
4. Danial and I reviewed the overall spreadsheet on a 1:1 call today.
5. The overall assessment is that DIDComm meets or exceeds all the 18 requirements for a Layer 2 Spanning Protocol.
6. I think this will become more clear after my Proposal 4 where I have a few slides that easily explain the essence of DIDComm (https://hyperonomy.com/2023/02/22/proposal-4-to-toip-tsl-tf-web-7-0trust-spanning-layerframework/).

Each of you has been emailed a link from Google Docs. Let me know if there are any issues.

Best regards,
Michael Herman
Web 7.0

If you want something done as quickly as possible, assign it to a busy person.

12

12

PROPOSAL 4 : TRUST SPANNING PROTOCOL TASK FORCE

- Mission
  - The mission of the TSWG is to draft the ToIP Trust Spanning Protocol V1.0 Specification to meet the requirements for ToIP Layer 2 as specified in the ToIP Technology Architecture V1.0 Specification.
- Deliverables
  - The deliverable of this Task Force is the ToIP Trust Spanning Protocol Specification that must meet the 18 requirements for the ToIP Layer 2 protocol as specified in the ToIP Technology Architecture V1.0 Specification.

- Proposal 4 represents a Unified Trust Spanning Layer Base Protocol solution based on readily available, proven, comprehensive, understandable Internet technologies and specifications

13

13

PROPOSAL 4

1. Proposal 4 Background
2. Proposal 4 Examples
3. Proposal 4 Summary: Recommendation for V1 Standardization
4. Proposal 4 Definitions and Drill-down
   i. Web 7.0 *Celtic Tree of Life* Trust Spanning Layer Model: Super Protocols, Base Protocols, and Subprotocols
   ii. Credential Sender-Receiver Pattern
   iii. Layer 1 Trust Foundation Services
   iv. Trust Tasks Super Protocols & Overlays
5. Conclusion: Recommendation for V1 Standardization

[1] *This presentation has lots of detail, but the goal is to present these concepts at an Awareness level.*

[2] *Web 7.0 tagline: Take what you need; leave the rest*

14

14

PROPOSAL 4 BACKGROUND

DIDCOMM ARCHITECTURE REFERENCE MODEL

WHAT IS WEB 7.0?

Web 7.0 is a unified software and hardware ecosystem for building resilient, trusted, decentralized systems using decentralized identifiers, DIDComm agents, and verifiable credentials.

Take what you need; leave the rest.

The Web 7.0 Architecture Whitepaper (#web7, @web7arch)

DIDComm Agent Architecture Reference Model (DIDComm-ARM)

A Design Guide for Software Architects and Developers

APPENDIX D – COPYRIGHT, TRADEMARKS, AND LICENSES

Copyright

This whitepaper is:

This whitepaper is an independent work product produced by the author; it is neither a W3C, DIF, Sovrin Foundation, nor ToIP publication.

18

PROPOSAL 4 BACKGROUND

DIDCOMM BASICS

21

21

PROPOSAL 4 : TRUST SPANNING PROTOCOL TASK FORCE

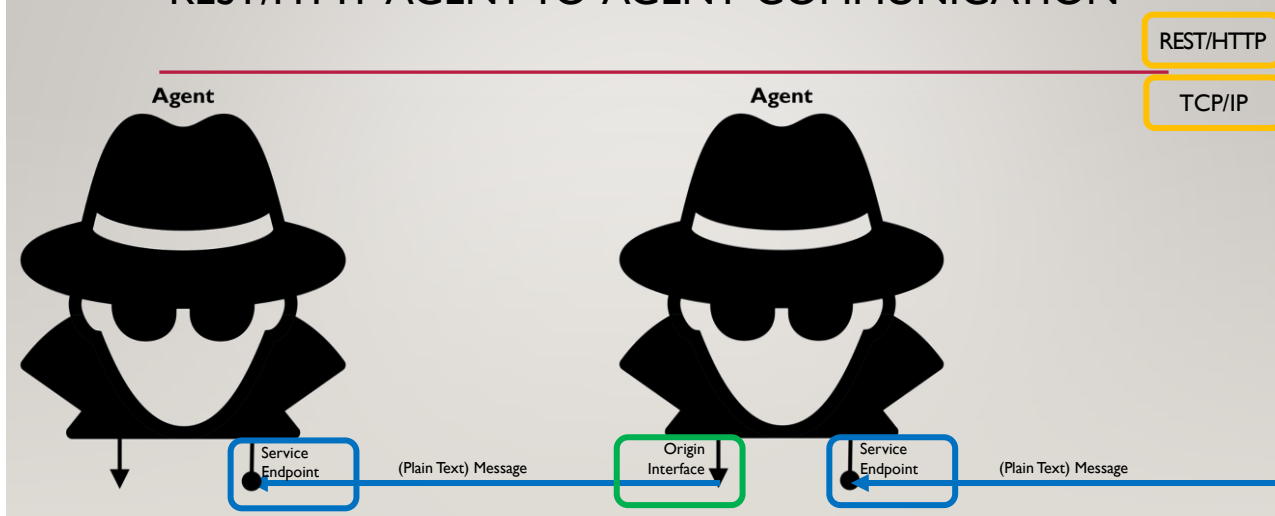
- Mission
  - The mission of the TSWG is to draft the ToIP Trust Spanning Protocol V1.0 Specification to meet the requirements for ToIP Layer 2 as specified in the ToIP Technology Architecture V1.0 Specification.
- Deliverables
  - The deliverable of this Task Force is the ToIP Trust Spanning Protocol Specification that must meet the 18 requirements for the ToIP Layer 2 protocol as specified in the ToIP Technology Architecture V1.0 Specification.

- Proposal 4 represents a Unified Trust Spanning Layer Base Protocol solution based on readily available, proven, comprehensive, understandable Internet technologies and specifications

22

22

REST/HTTP AGENT-TO-AGENT COMMUNICATION

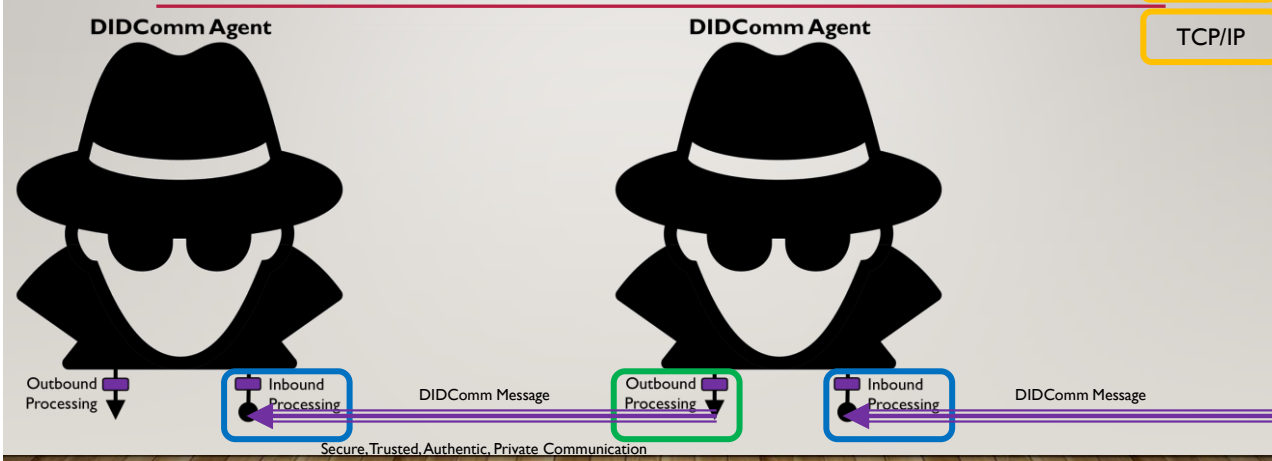


24

24

DIDCOMM AGENT-TO-AGENT COMMUNICATION

DIDComm Messaging
REST/HTTP
TCP/IP

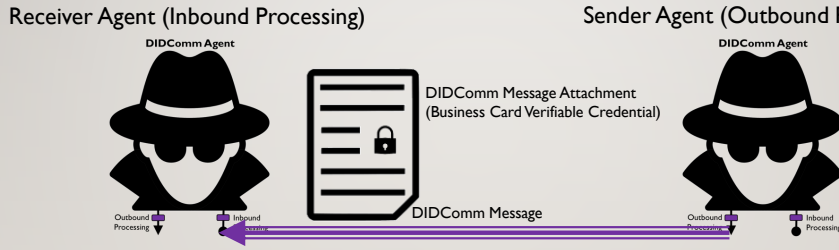


25

25

CREDENTIAL SENDER-RECEIVER PATTERN TRUST SPANNING LAYER BASE PROTOCOL

Attachments
DIDComm Messaging
REST/HTTP
TCP/IP

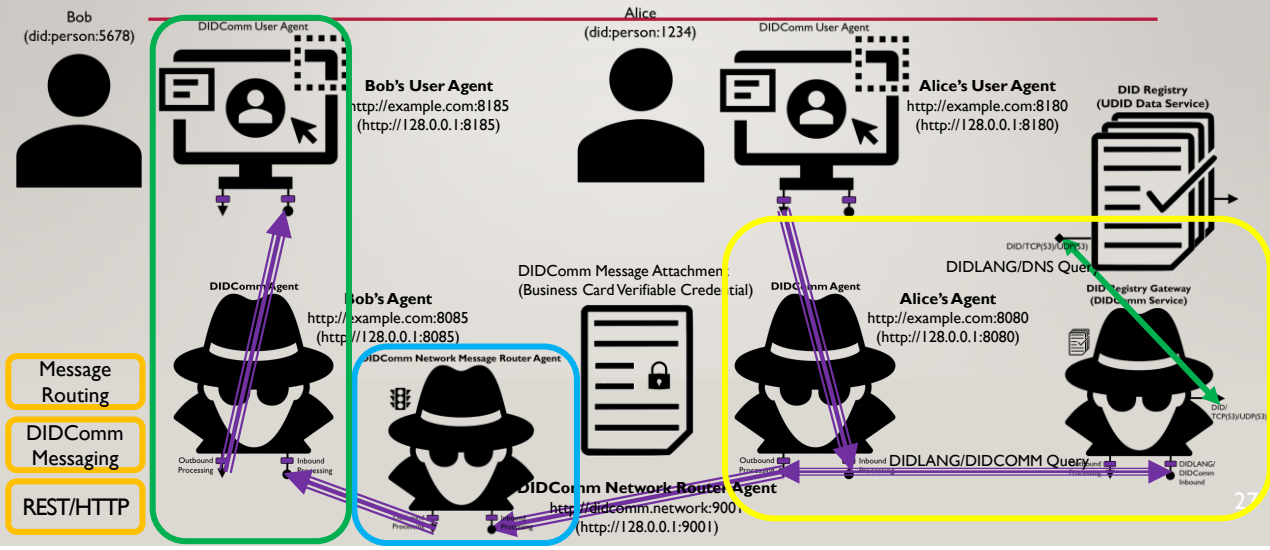


Verifiable Credentials are used for illustrative purposes only.

26

26

DIDCOMM NETWORK LAYER 4 DEMO
CHAT/DIDCOMM/HTTP/NETWORK + VC ATTACHMENTS



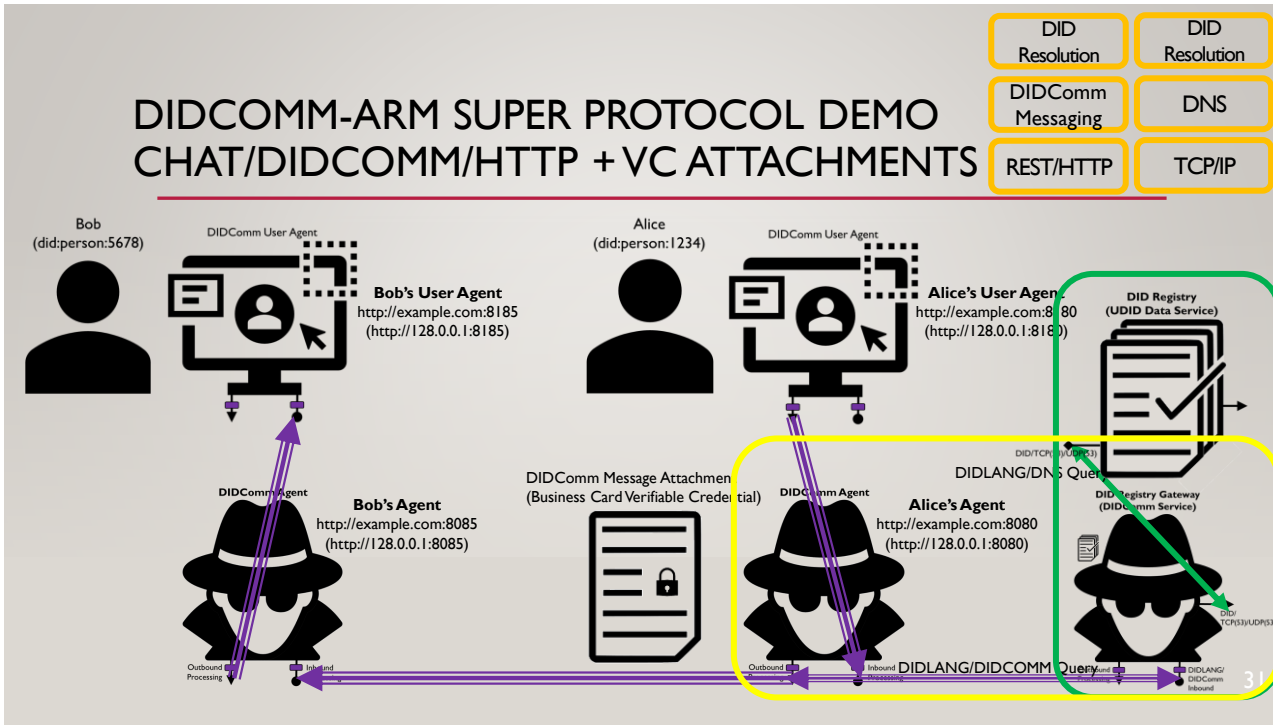
27

PROPOSAL 4 EXAMPLES

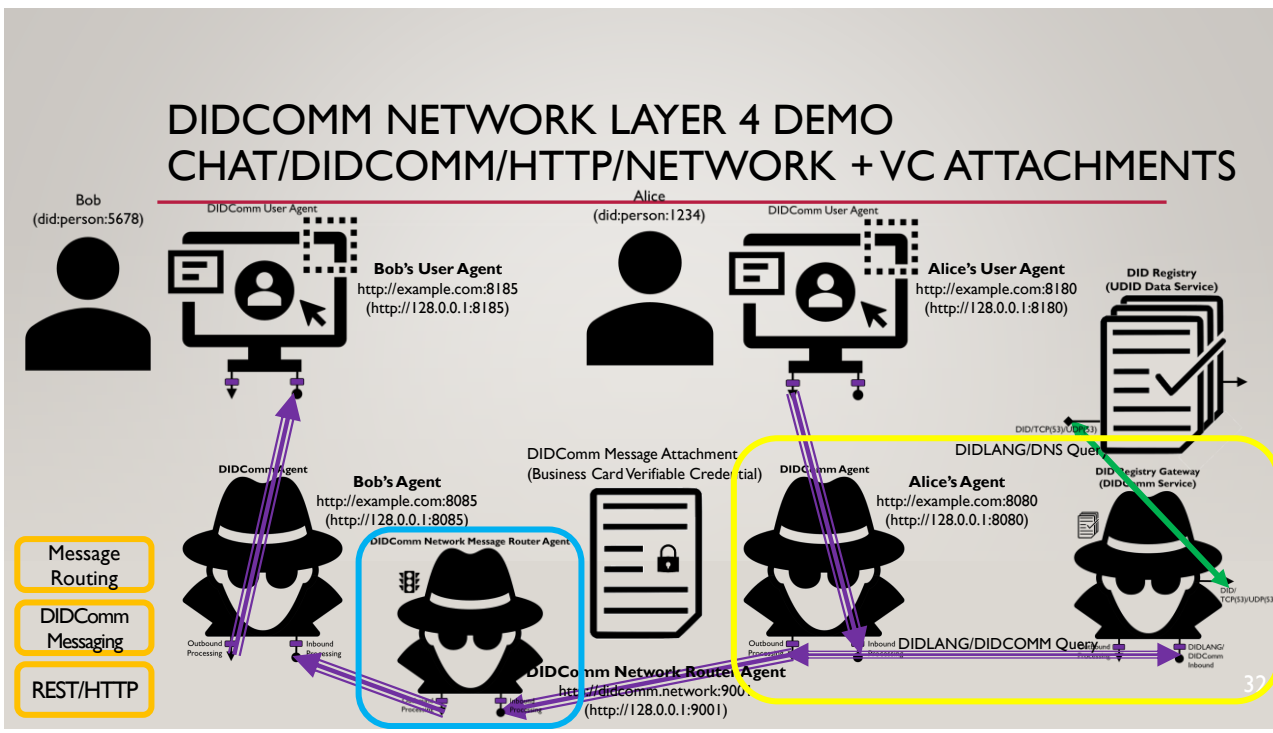
IIW36 DEMOS:
WEB 7.0 DIDCOMM-ARM AND CREDENTIAL SENDER-RECEIVER PATTERN

29

29


DID Resolution
DID Resolution
DIDComm Messaging
DNS
REST/HTTP
TCP/IP
DIDCOMM-ARM SUPER PROTOCOL DEMO
CHAT/DIDCOMM/HTTP + VC ATTACHMENTS
Bob
(did:person:5678)
DIDComm User Agent
Bob's User Agent
http://example.com:8185
(http://128.0.0.1:8185)
Alice
(did:person:1234)
DIDComm User Agent
Alice's User Agent
http://example.com:8180
(http://128.0.0.1:8180)
DID Registry
(UDID Data Service)
DIDLANG/DNS Query
DIDComm Agent
Bob's Agent
http://example.com:8085
(http://128.0.0.1:8085)
DIDComm Message Attachment
(Business Card Verifiable Credential)
DIDComm Agent
Alice's Agent
http://example.com:8080
(http://128.0.0.1:8080)
DID Registry Gateway
(DIDComm Service)
Outbound Processing
Inbound Processing
DIDLANG/DIDCOMM Query
DIDLANG/ DIDComm Inbound
31

31

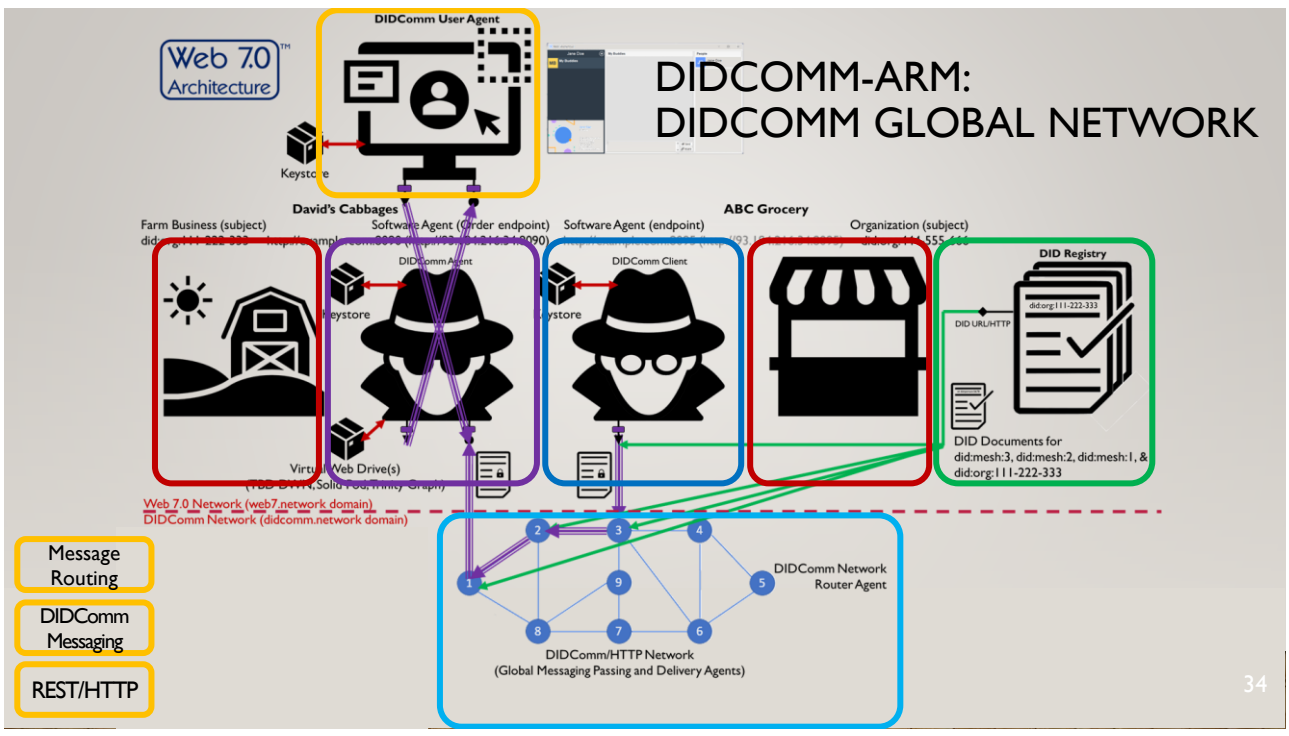

DIDCOMM NETWORK LAYER 4 DEMO
CHAT/DIDCOMM/HTTP/NETWORK + VC ATTACHMENTS
Bob
(did:person:5678)
DIDComm User Agent
Bob's User Agent
http://example.com:8185
(http://128.0.0.1:8185)
Alice
(did:person:1234)
DIDComm User Agent
Alice's User Agent
http://example.com:8180
(http://128.0.0.1:8180)
DID Registry
(UDID Data Service)
DIDLANG/DNS Query
DIDComm Agent
Bob's Agent
http://example.com:8085
(http://128.0.0.1:8085)
DIDComm Message Attachment
(Business Card Verifiable Credential)
DIDComm Agent
Alice's Agent
http://example.com:8080
(http://128.0.0.1:8080)
DID Registry Gateway
(DIDComm Service)
DIDComm Network Message Router Agent
Message Routing
DIDComm Messaging
REST/HTTP
DIDLANG/DIDCOMM Query
DIDComm Network Router Agent
(http://128.0.0.1:9001)
32

32

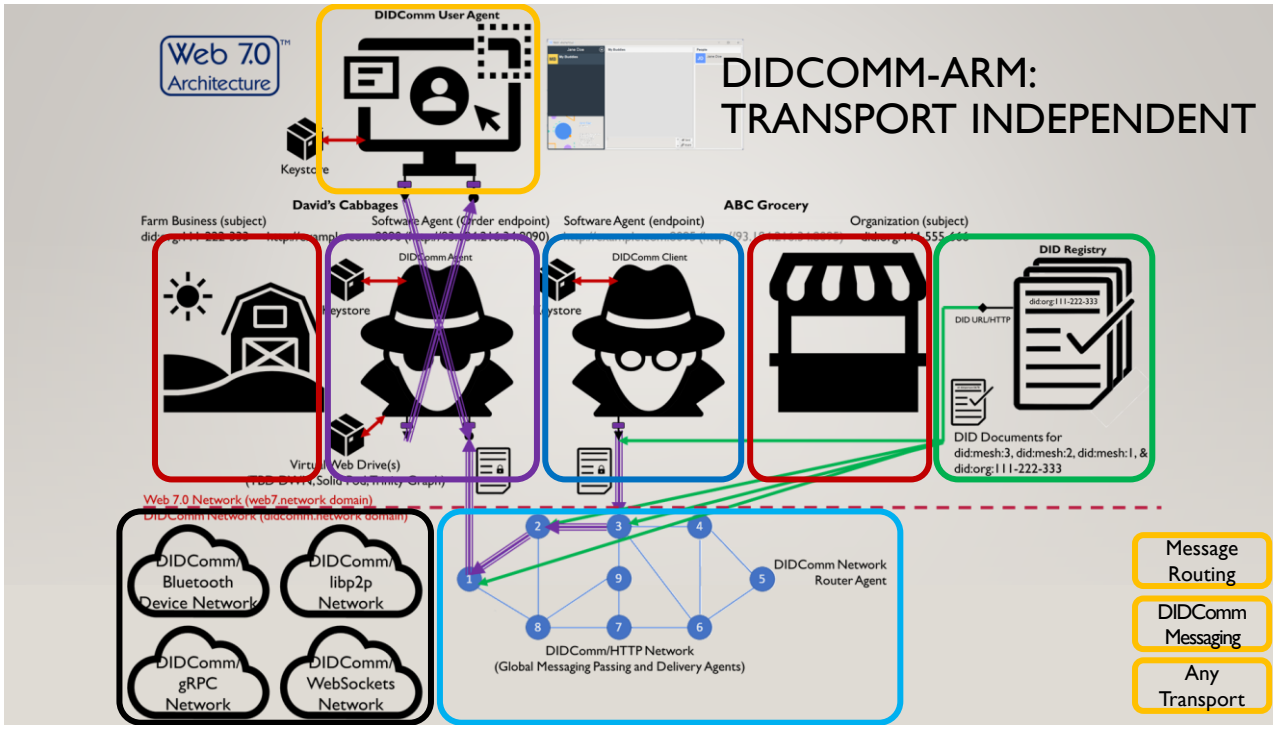
PROPOSAL 4 EXAMPLES

WEB 7.0 GLOBAL DIDCOMM NETWORK

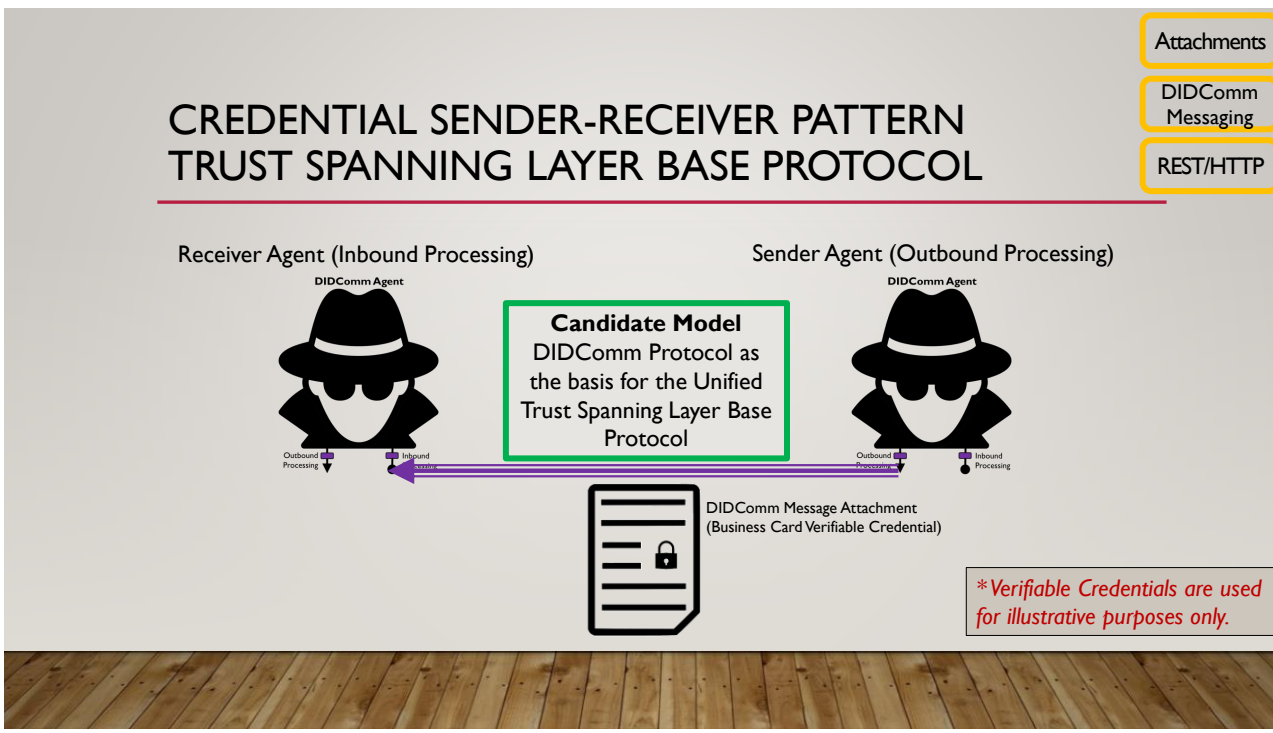
33



34


Web 7.0 Architecture
DIDComm User Agent
DIDCOMM-ARM:
TRANSPORT INDEPENDENT
Keystore
David's Cabbages
Farm Business (subject)
Software Agent (Order endpoint)
Software Agent (endpoint)
ABC Grocery
Organization (subject)
DIDComm Agent
DIDComm Client
Keystore
Keystore
DID Registry
DID URL/HTTP
did:org:111-222-333
DID Documents for
did:mesh:3, did:mesh:2, did:mesh:1, &
did:org:111-222-333
Virtual Web Drive(s)
Web 7.0 Network (web7.network domain)
DIDComm Network (didcomm.network domain)
DIDComm Bluetooth Device Network
DIDComm libp2p Network
DIDComm gRPC Network
DIDComm WebSockets Network
1
2
3
4
5
6
7
8
9
DIDComm Network Router Agent
DIDComm/HTTP Network
(Global Messaging Passing and Delivery Agents)
Message Routing
DIDComm Messaging
Any Transport

35


Attachments
DIDComm Messaging
REST/HTTP
CREDENTIAL SENDER-RECEIVER PATTERN
TRUST SPANNING LAYER BASE PROTOCOL
Receiver Agent (Inbound Processing)
Sender Agent (Outbound Processing)
DIDComm Agent
DIDComm Agent
Outbound Processing
Inbound Processing
Outbound Processing
Inbound Processing
Candidate Model
DIDComm Protocol as the basis for the Unified Trust Spanning Layer Base Protocol
DIDComm Message Attachment
(Business Card Verifiable Credential)
*Verifiable Credentials are used for illustrative purposes only.

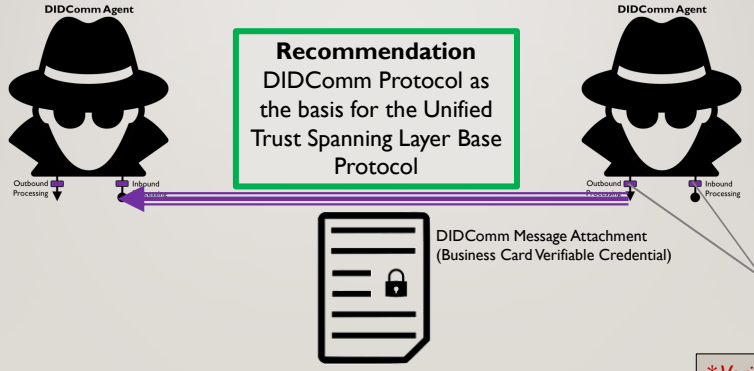
36

CREDENTIAL SENDER-RECEIVER PATTERN TRUST SPANNING LAYER BASE PROTOCOL

Attachments
DIDComm Messaging
REST/HTTP

Receiver Agent (Inbound Processing)

Sender Agent (Outbound Processing)



Recommendation
DIDComm Protocol as the basis for the Unified Trust Spanning Layer Base Protocol

DIDComm Message Attachment (Business Card Verifiable Credential)

4.iv. - Trust Tasks Super Protocols & Overlays: Drilldown and Examples

**Verifiable Credentials are used for illustrative purposes only.*

37

PROPOSAL 4 SUMMARY

Proposal 4 (as presented in this version of the Proposal 4 presentation) is a:

- Compelling story (with irrefutable evidence and examples) *supporting the selection of*
  - DID Communications (DIDComm) Protocol
  - Credential Sender-Receiver Pattern
- *as the basis for the Unified Trust Spanning Layer Base Protocol for any and all decentralized ecosystems*
  - Web 7.0 DIDComm Architecture Reference Model (DIDComm-ARM)
  - ToIP Technical Architecture Specification (ToIP TAS), Etc.
- Dan

Proposal #4 to ToIP TSP TF 0.8: Web 7.0 Trust Spanning Layer Framework++ (Summary Presentation) #27
mwherman2000 3 weeks ago · 7 comments · 9 replies

dhh1128 5 days ago Maintainer

I believe that DIDComm v2 ticks all the boxes, and I like Michael's proposal because I think it makes that clear. I can hardly say otherwise, since it's something I poured my heart and soul into. However, that does not mean I think it is optimal, which is why I didn't just recommend it in its current form.

…es that clear. I

…ent-5240938

38

38

PROPOSAL 4 DEFINITIONS AND DRILL-DOWN

- Web 7.0 Celtic Tree of Life Trust Spanning Layer Model: Super Protocols, Base Protocols, and Subprotocols
- Credential Sender-Receiver Pattern
- Layer 1 Trust Foundation Services
- Trust Foundation Services Subprotocols
- Trust Tasks Super Protocols & Overlays

40

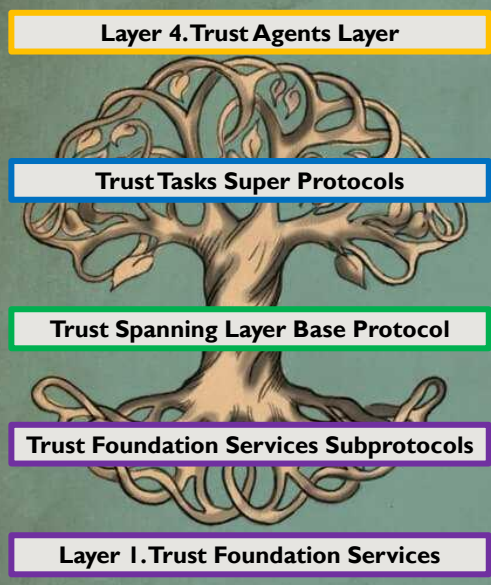
PROPOSAL 4 : TRUST SPANNING PROTOCOL TASK FORCE

- Mission
  - The mission of the TSWG is to draft the ToIP Trust Spanning Protocol V1.0 Specification to meet the requirements for ToIP Layer 2 as specified in the ToIP Technology Architecture V1.0 Specification.
- Deliverables
  - The deliverable of this Task Force is the ToIP Trust Spanning Protocol Specification that must meet the 18 requirements for the ToIP Layer 2 protocol as specified in the ToIP Technology Architecture V1.0 Specification.

- Proposal 4 represents a Unified Trust Spanning Layer Base Protocol solution based on readily available, proven, comprehensive, understandable Internet technologies and specifications

41

WEB 7.0 *CELTIC TREE OF LIFE* TRUST SPANNING LAYER MODEL



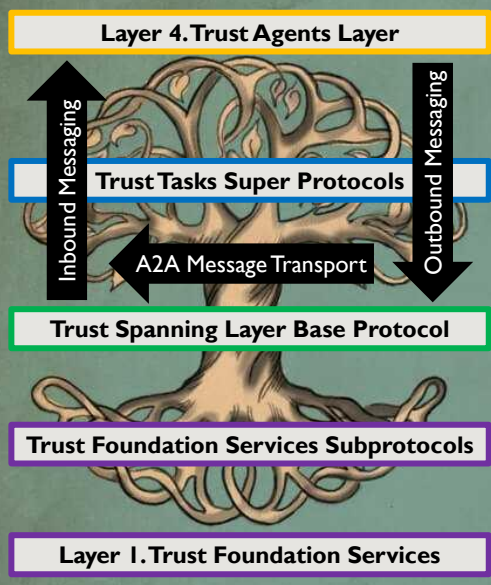
The Celts saw the strength and longevity of the oak tree as a symbol of endurance.

42

www.theirishroadtrip.com

42

TRUST TASKS SUPER PROTOCOLS: AGENT TO AGENT MESSAGING

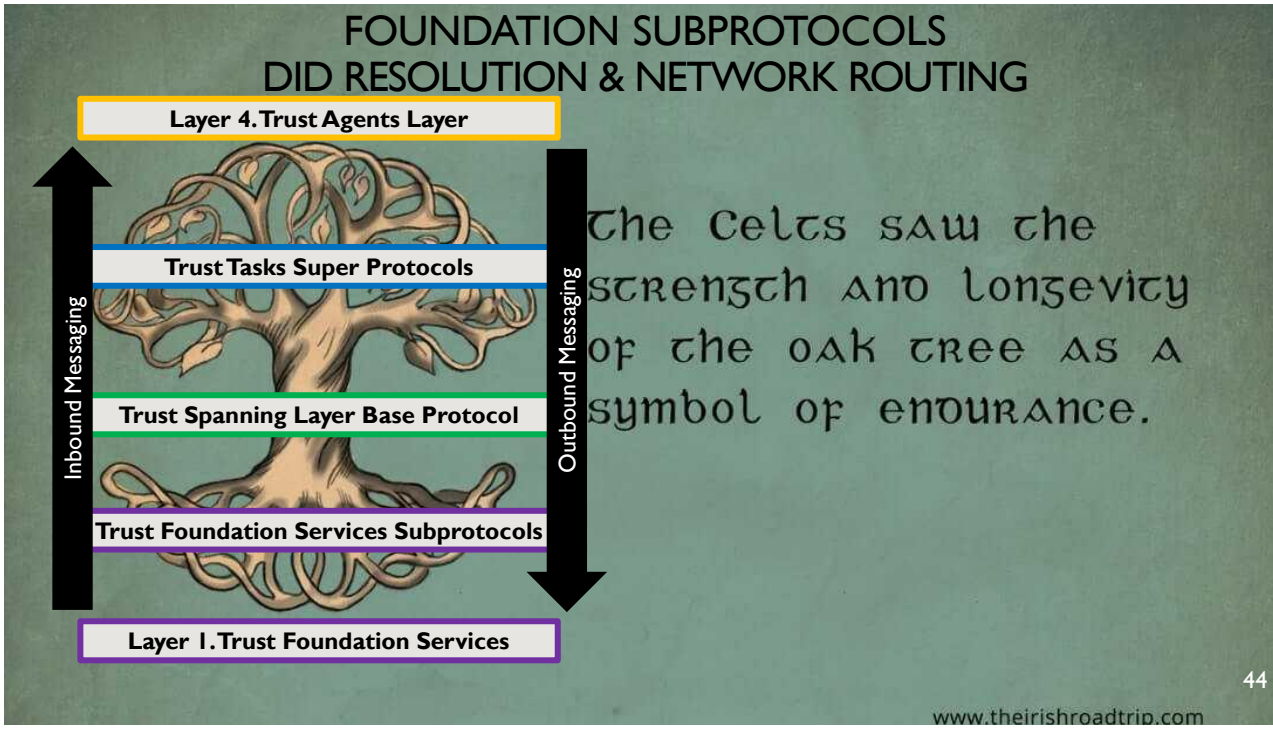


The Celts saw the strength and longevity of the oak tree as a symbol of endurance.

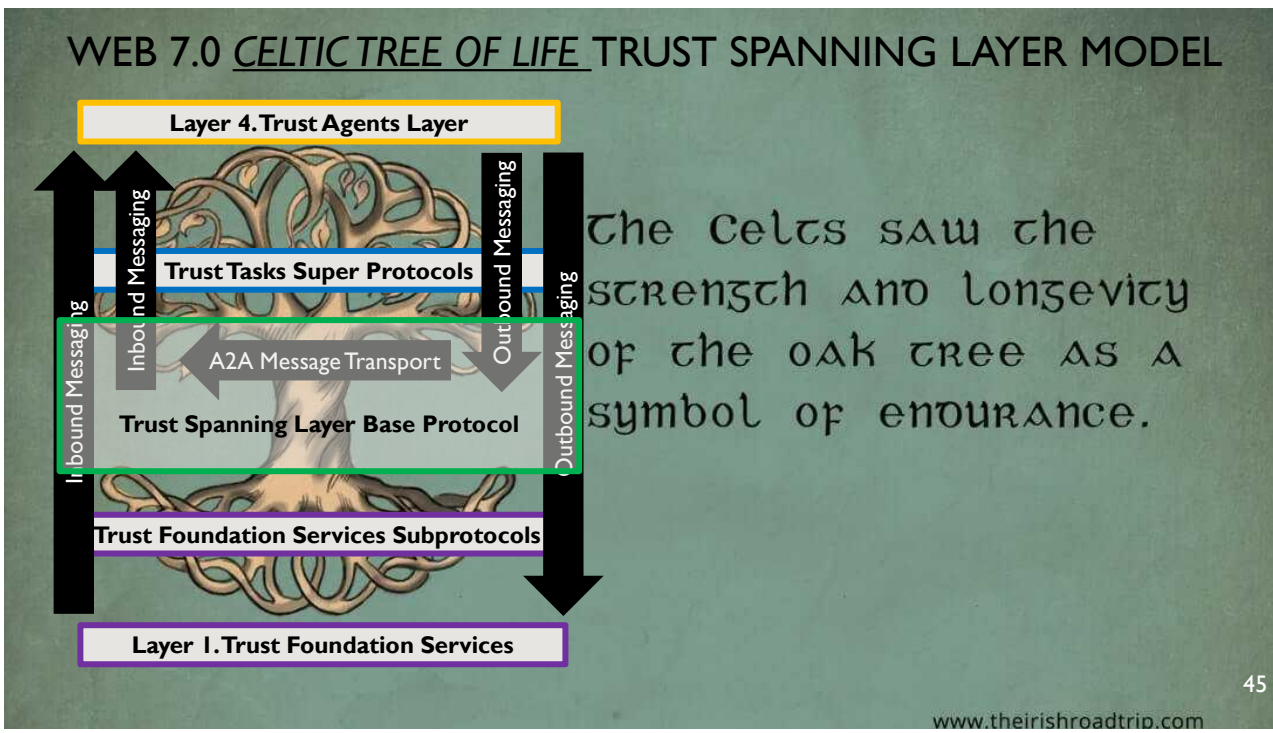
43

www.theirishroadtrip.com

43


FOUNDATION SUBPROTOCOLS
DID RESOLUTION & NETWORK ROUTING
Layer 4. Trust Agents Layer
Trust Tasks Super Protocols
Trust Spanning Layer Base Protocol
Trust Foundation Services Subprotocols
Layer 1. Trust Foundation Services
Inbound Messaging
Outbound Messaging
The Celts saw the strength and longevity of the oak tree as a symbol of endurance.
44
www.theirishroadtrip.com

44


WEB 7.0 CELTIC TREE OF LIFE TRUST SPANNING LAYER MODEL
Layer 4. Trust Agents Layer
Trust Tasks Super Protocols
A2A Message Transport
Trust Spanning Layer Base Protocol
Trust Foundation Services Subprotocols
Layer 1. Trust Foundation Services
Inbound Messaging
Outbound Messaging
The Celts saw the strength and longevity of the oak tree as a symbol of endurance.
45
www.theirishroadtrip.com

45

Proposal 3

SIDE BAR: TOIP TSP TASK FORCE SCOPE-OF-WORK

1. Need to adopt a systems, ecosystem-wide point-of-view/perspective
2. Scope of work cannot be limited to the specification of a Trust Spanning Layer Base Protocol
3. Post-proposals analysis and consolidation will require some perceived Trust Spanning Layer Base Protocol capabilities to be *relegated* or *delegated* to either:
   - Trust Tasks Super Protocols
   - Trust Foundation Services Subprotocols
   - This relegation/delegation activity needs to be in-scope. Detailed specification of the Trust Tasks Super Protocol and Trust Foundation Services Subprotocol framework and individual protocols to be deferred to a separate WG/TF activity

CREDENTIAL SENDER-RECEIVER PATTERN DRILL-DOWN

PROPOSAL 4 :TRUST SPANNING PROTOCOL TASK FORCE

- Mission
  - The mission of the TSWG is to draft the ToIP Trust Spanning Protocol V1.0 Specification to meet the requirements for ToIP Layer 2 as specified in the ToIP Technology Architecture V1.0 Specification.
- Deliverables
  - The deliverable of this Task Force is the ToIP Trust Spanning Protocol Specification that must meet the 18 requirements for the ToIP Layer 2 protocol as specified in the ToIP Technology Architecture V1.0 Specification.

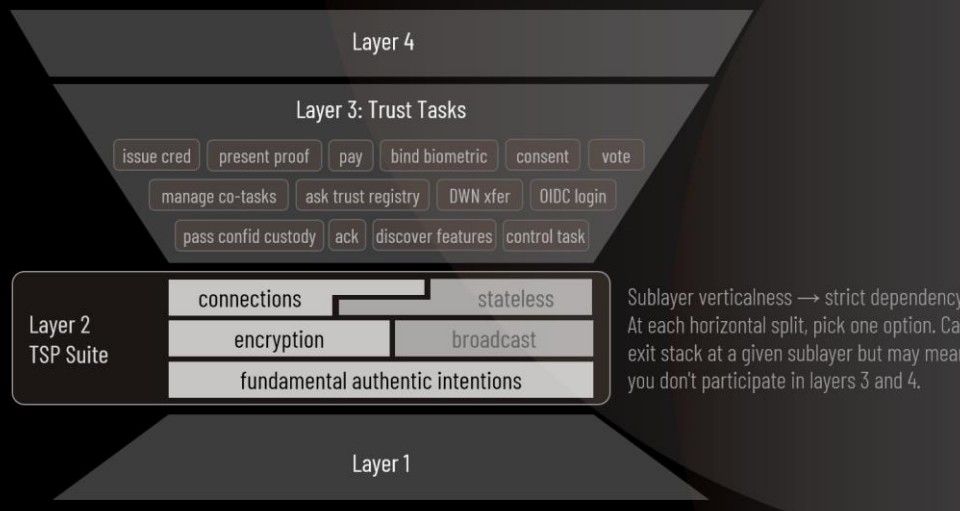
- Proposal 4 represents a Unified Trust Spanning Layer Base Protocol solution based on readily available, proven, comprehensive, understandable Internet technologies and specifications

48

48

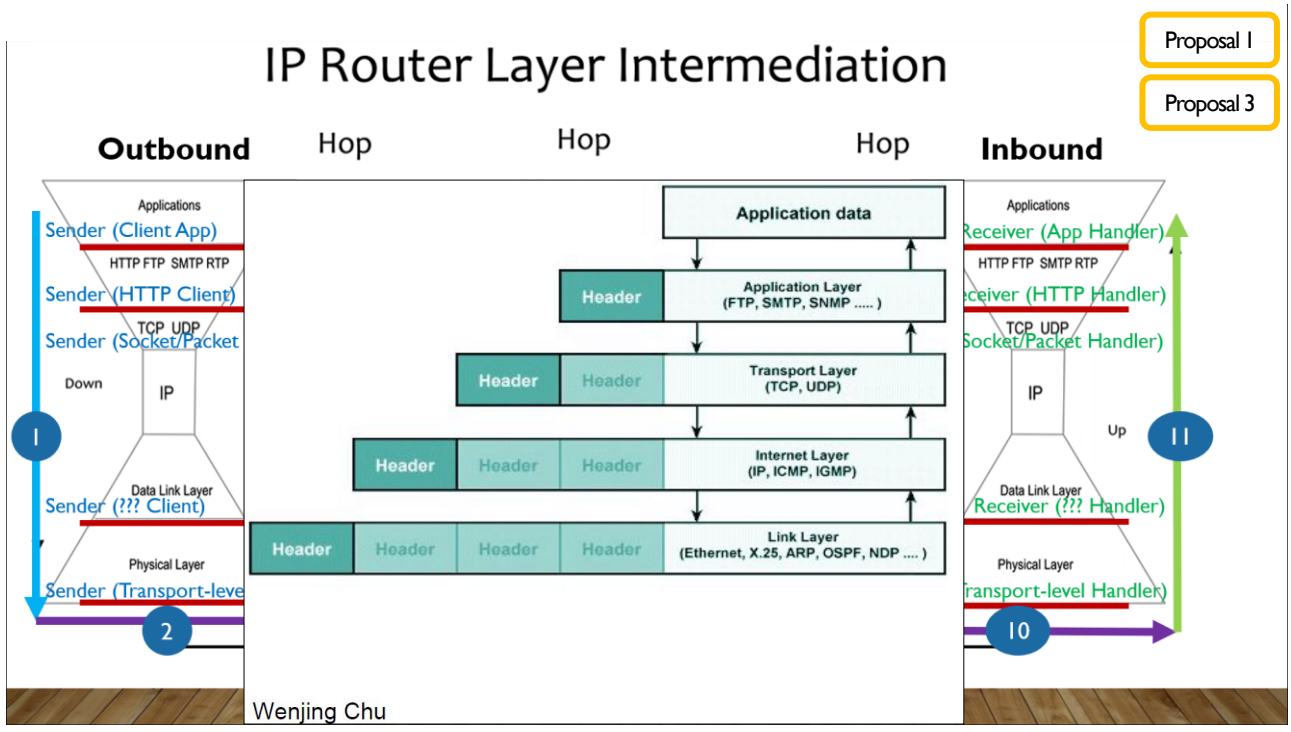
Proposal 2

Proposal as a picture

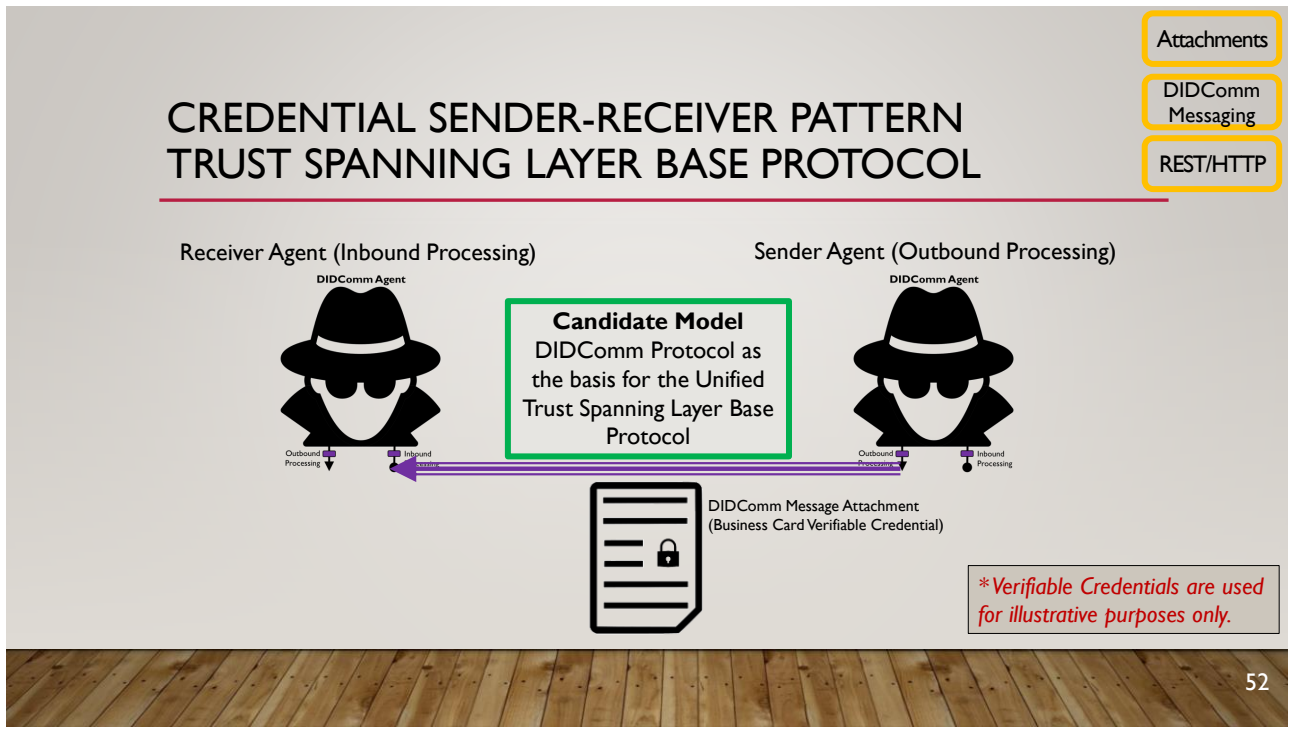


8

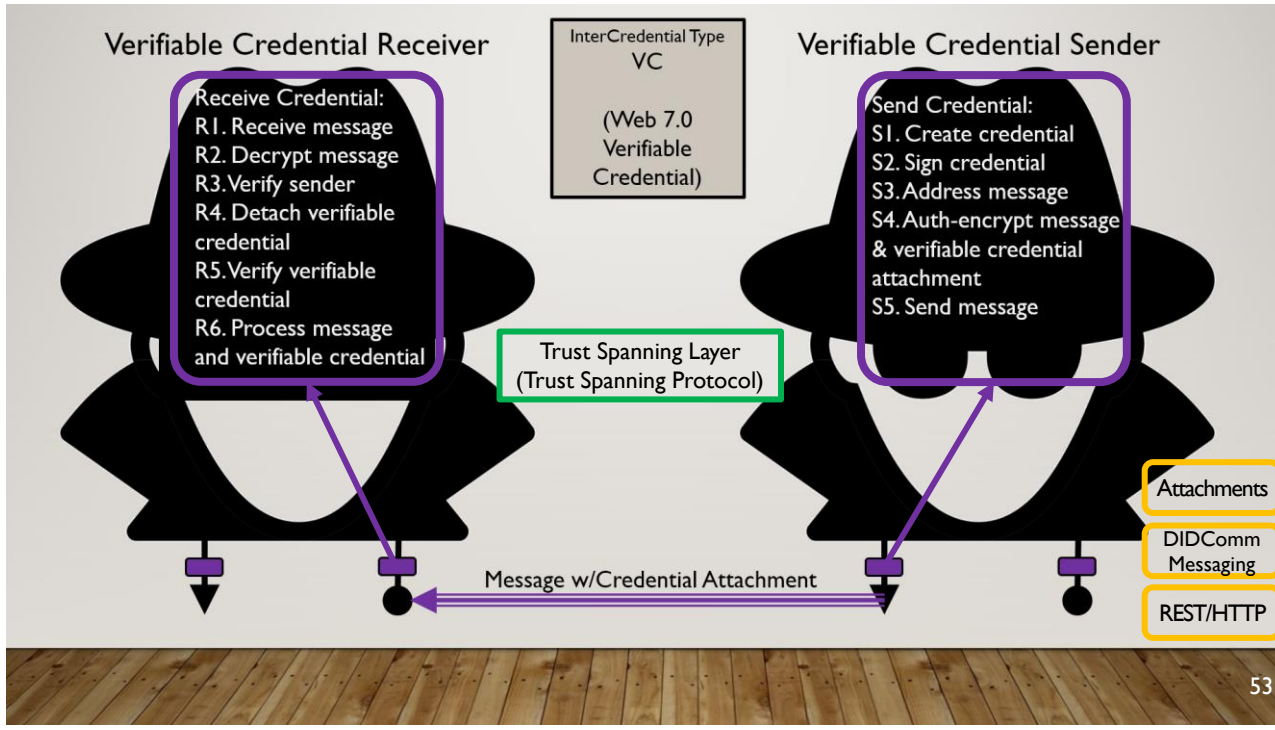
49


IP Router Layer Intermediation
Proposal 1
Proposal 3
Outbound
Hop
Hop
Hop
Inbound
Applications
Sender (Client App)
HTTP FTP SMTP RTP
Sender (HTTP Client)
TCP UDP
Sender (Socket/Packet
Down
IP
Data Link Layer
Sender (??? Client)
Physical Layer
Sender (Transport-leve
1
2
Application data
Header
Application Layer
(FTP, SMTP, SNMP .....)
Header
Header
Transport Layer
(TCP, UDP)
Header
Header
Header
Internet Layer
(IP, ICMP, IGMP)
Header
Header
Header
Header
Link Layer
(Ethernet, X.25, ARP, OSPF, NDP ....)
Applications
Receiver (App Handler)
HTTP FTP SMTP RTP
eiver (HTTP Handler)
TCP UDP
Socket/Packet Handler)
IP
Up
11
Data Link Layer
Receiver (??? Handler)
Physical Layer
ransport-level Handler)
10
Wenjing Chu

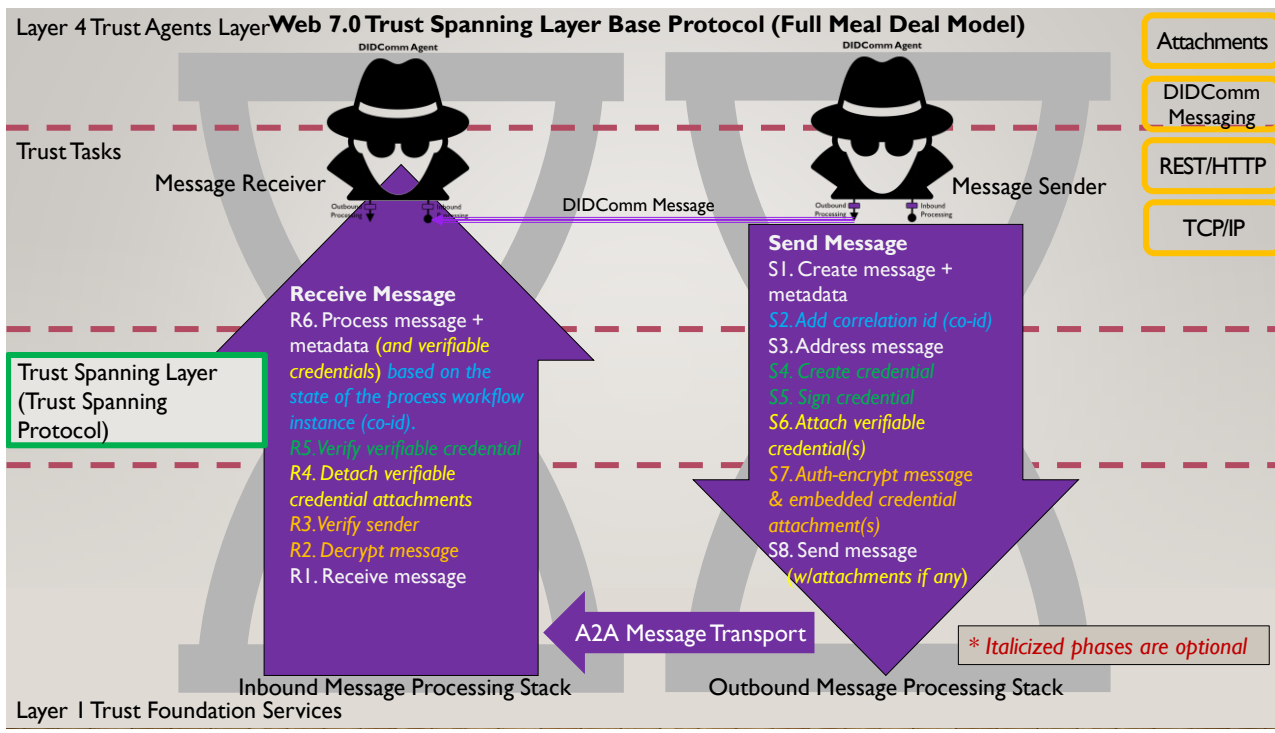
51


Attachments
DIDComm Messaging
REST/HTTP
CREDENTIAL SENDER-RECEIVER PATTERN
TRUST SPANNING LAYER BASE PROTOCOL
Receiver Agent (Inbound Processing)
Sender Agent (Outbound Processing)
DIDComm Agent
DIDComm Agent
Candidate Model
DIDComm Protocol as the basis for the Unified Trust Spanning Layer Base Protocol
Outbound Processing
Inbound Processing
Outbound Processing
Inbound Processing
DIDComm Message Attachment
(Business Card Verifiable Credential)
*Verifiable Credentials are used for illustrative purposes only.
52

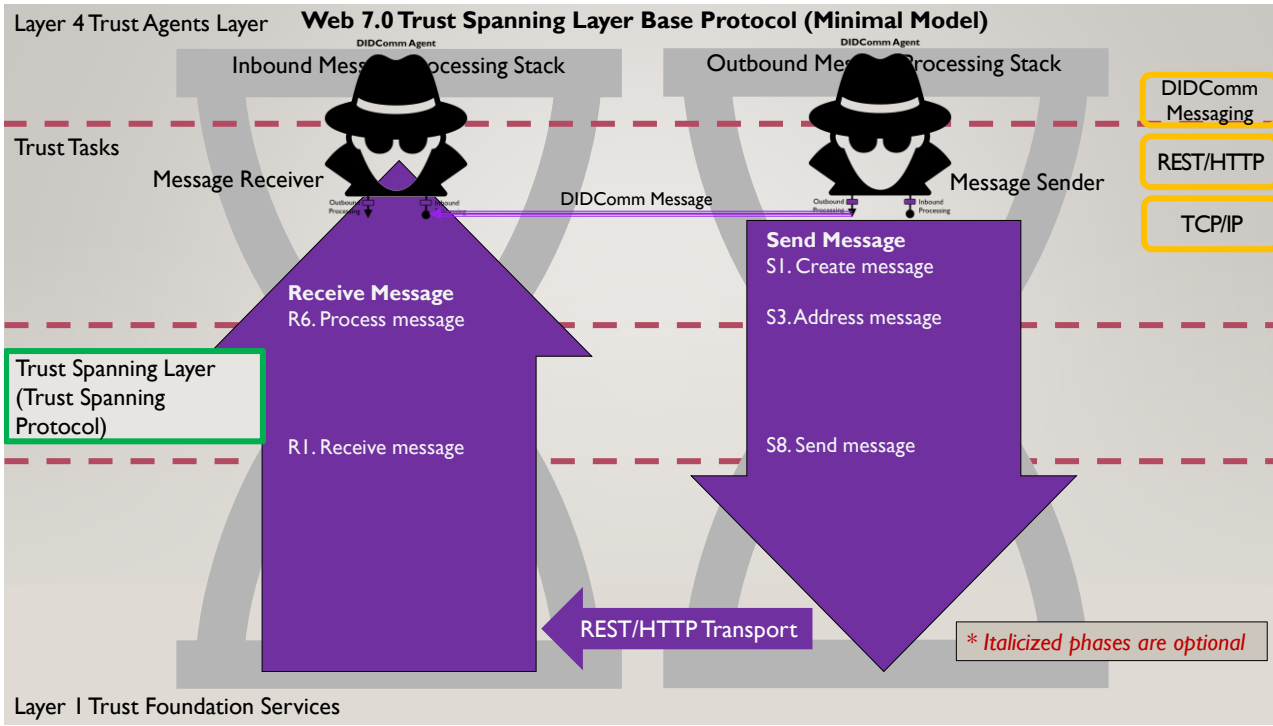
52


Verifiable Credential Receiver
InterCredential Type
VC
(Web 7.0
Verifiable
Credential)
Verifiable Credential Sender
Receive Credential:
R1. Receive message
R2. Decrypt message
R3. Verify sender
R4. Detach verifiable credential
R5. Verify verifiable credential
R6. Process message and verifiable credential
Send Credential:
S1. Create credential
S2. Sign credential
S3. Address message
S4. Auth-encrypt message & verifiable credential attachment
S5. Send message
Trust Spanning Layer
(Trust Spanning Protocol)
Message w/Credential Attachment
Attachments
DIDComm Messaging
REST/HTTP
53

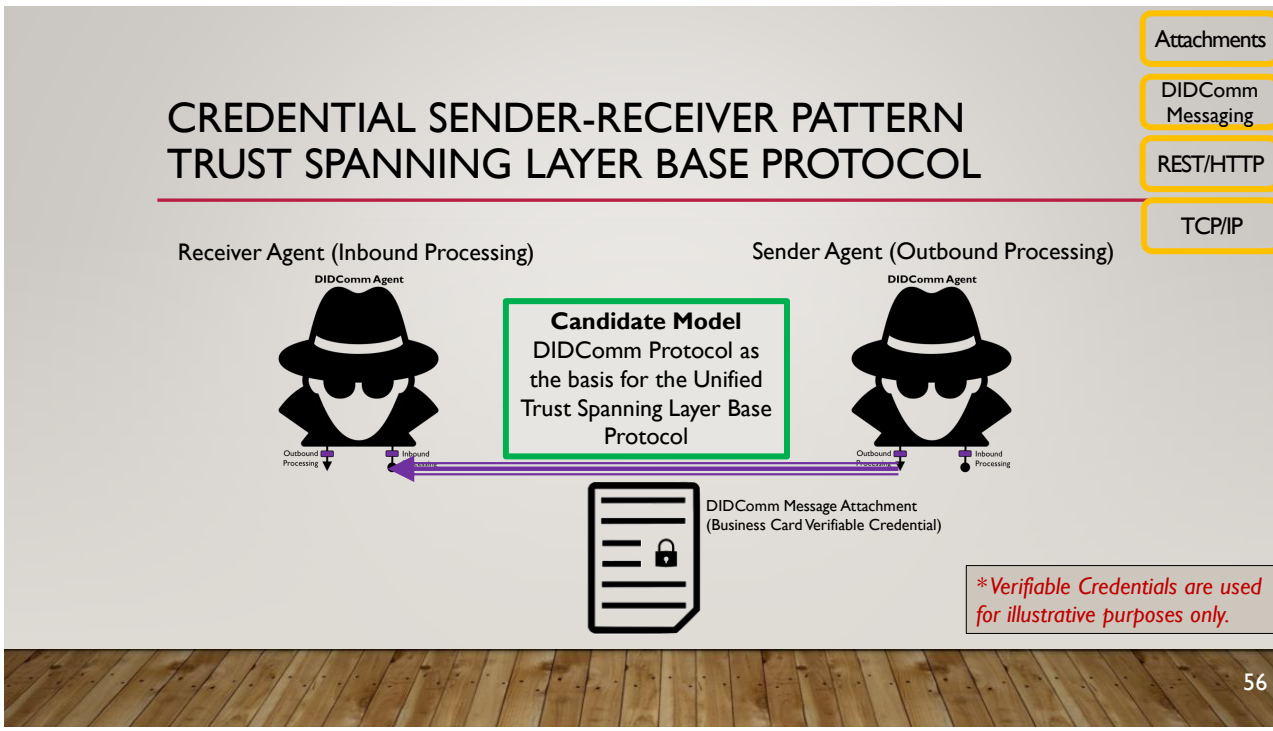
53


Layer 4 Trust Agents Layer
Web 7.0 Trust Spanning Layer Base Protocol (Full Meal Deal Model)
DIDComm Agent
DIDComm Agent
Attachments
DIDComm Messaging
REST/HTTP
TCP/IP
Trust Tasks
Message Receiver
DIDComm Message
Message Sender
Receive Message
R6. Process message + metadata (and verifiable credentials) based on the state of the process workflow instance (co-id).
R5. Verify verifiable credential
R4. Detach verifiable credential attachments
R3. Verify sender
R2. Decrypt message
R1. Receive message
Send Message
S1. Create message + metadata
S2. Add correlation id (co-id)
S3. Address message
S4. Create credential
S5. Sign credential
S6. Attach verifiable credential(s)
S7. Auth-encrypt message & embedded credential attachment(s)
S8. Send message (w/attachments if any)
Trust Spanning Layer
(Trust Spanning
Protocol)
A2A Message Transport
* Italicized phases are optional
Inbound Message Processing Stack
Outbound Message Processing Stack
Layer 1 Trust Foundation Services

54


Layer 4 Trust Agents Layer
Web 7.0 Trust Spanning Layer Base Protocol (Minimal Model)
DIDComm Agent
Inbound Mess ocessing Stack
DIDComm Agent
Outbound Me rocessing Stack
DIDComm Messaging
REST/HTTP
TCP/IP
Trust Tasks
Message Receiver
DIDComm Message
Message Sender
Send Message
S1. Create message
S3. Address message
S8. Send message
Receive Message
R6. Process message
R1. Receive message
Trust Spanning Layer (Trust Spanning Protocol)
REST/HTTP Transport
* Italicized phases are optional
Layer 1 Trust Foundation Services

55


Attachments
DIDComm Messaging
REST/HTTP
TCP/IP
CREDENTIAL SENDER-RECEIVER PATTERN
TRUST SPANNING LAYER BASE PROTOCOL
Receiver Agent (Inbound Processing)
Sender Agent (Outbound Processing)
DIDComm Agent
DIDComm Agent
Candidate Model
DIDComm Protocol as the basis for the Unified Trust Spanning Layer Base Protocol
DIDComm Message Attachment
(Business Card Verifiable Credential)
*Verifiable Credentials are used for illustrative purposes only.
56

56

PROPOSAL 4 TO TOIP TSP WG:

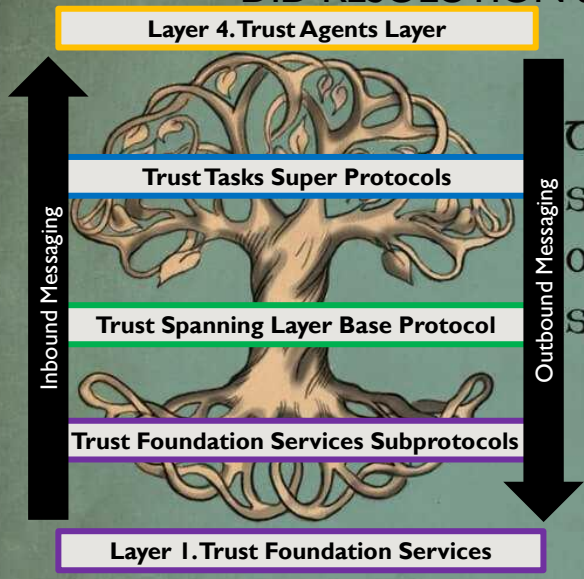
LAYER 1 TRUST FOUNDATION SERVICES TRUST FOUNDATION SERVICES SUBPROTOCOLS

- DID Resolution Gateway Agents
- DIDComm Intelligent Network Routing Agents

57

57

FOUNDATION SUBPROTOCOLS DID RESOLUTION & NETWORK ROUTING



The Celts saw the strength and longevity of the oak tree as a symbol of endurance.

www.theirishroadtrip.com

58

58

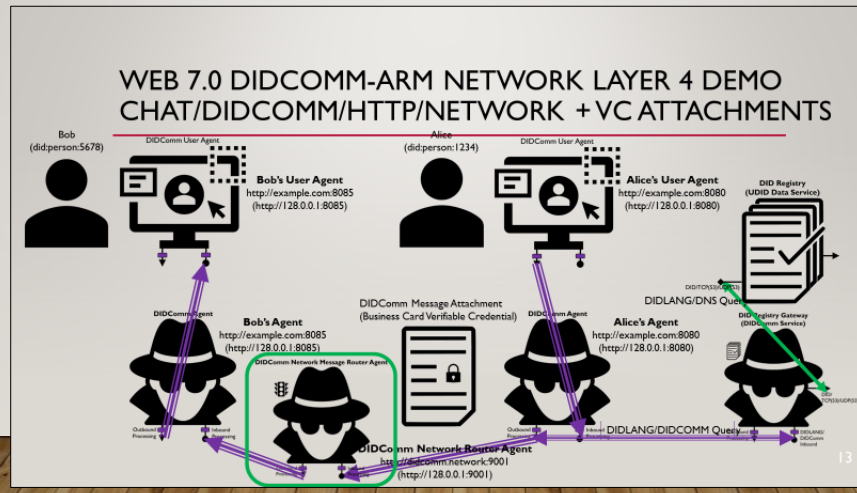
DIDCOMM NETWORK MESSAGE ROUTER AGENT

Foundation Subprotocol

Attachments

DIDComm Messaging

REST/HTTP



59

59

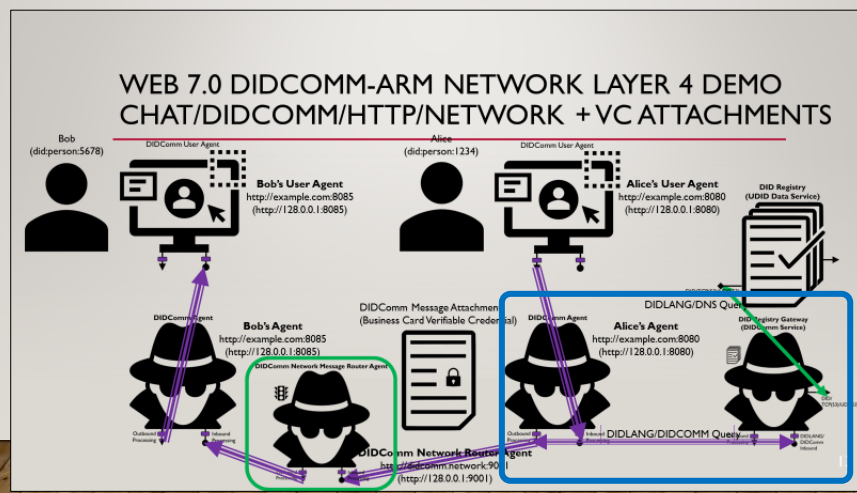
DID REGISTRY GATEWAY AGENT

Foundation Subprotocol

Attachments

DIDComm Messaging

REST/HTTP



61

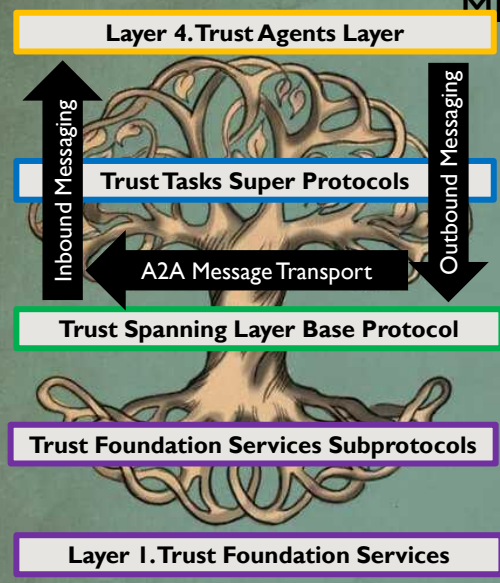
PROPOSAL 4 TO TOIP TSP WG:

TRUST TASKS SUPER PROTOCOLS & OVERLAYS

63

63

TRUST TASKS SUPER PROTOCOLS (AGENT TO AGENT MESSAGING)



The Celts saw the strength and longevity of the oak tree as a symbol of endurance.

www.theirishroadtrip.com

64

64

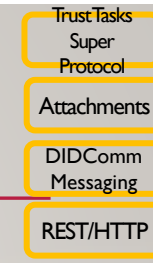
DANIEL HARDMAN'S DIDCOMM PROTOCOL EXAMPLES

- IssueCredential
- ProveWithCredential
- Connect, Introduce, SayGoodbye
- Pay, ListForSale
- TakeTest
- ApplyForLoan, ApplyForJob
- ScheduleEvent
- Vote
- Recommend
- FlipCoin
- CheckBiometric
- HailTaxi
- BookHotel
- PlanVacation
- RichChat
- NegotiatePriceAndPaymentMethod
- ReportCrime
- RequestSupport
- FileInsuranceClaim
- PutItemInEscrow
- AskAlexa
- PostTweet

65

65

ADDITIONAL USE CASES



Trust Tasks Super Protocol Use Cases

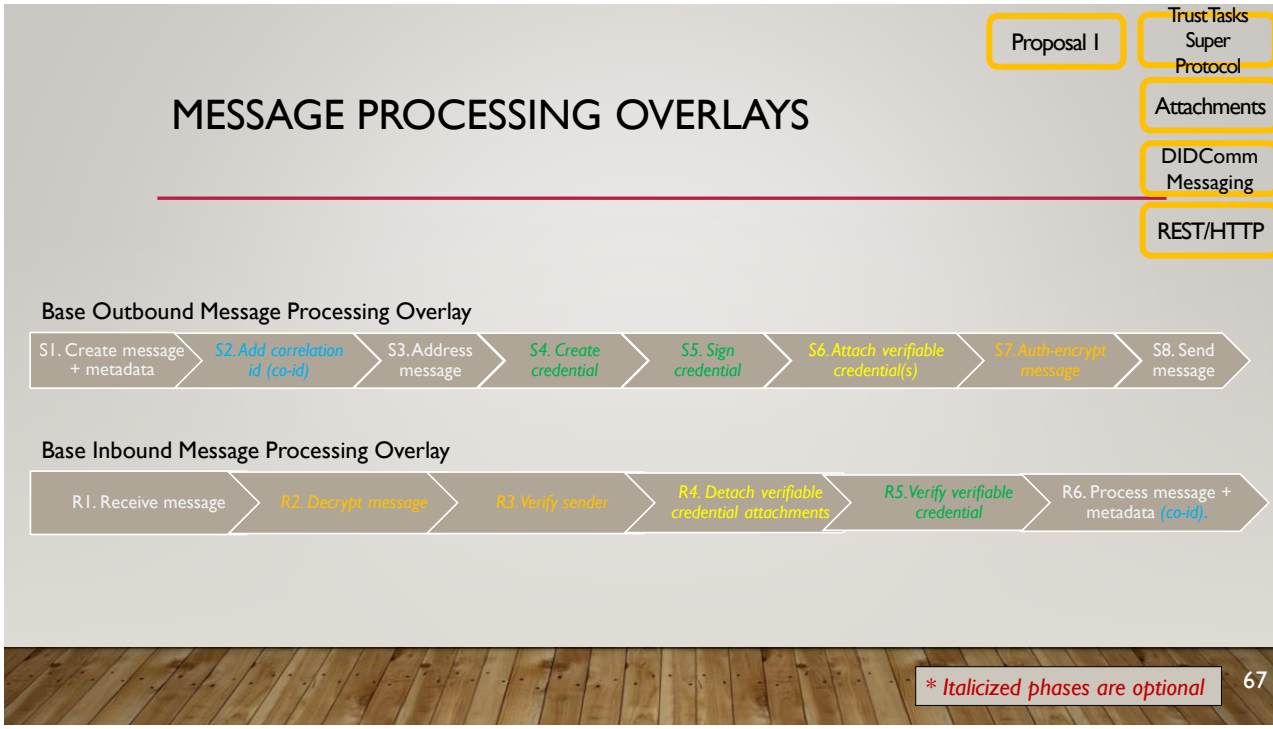
1. Secure, private, asynchronous agent to agent communication (one-way and full duplex)
2. A sample/simple procurement business process workflow (RFQ, PO, Waybill, Shipping Notifications, Delivery Confirmation, Invoice, Payment Confirmation, ...)
3. Issuer-Holder-Verifier Model
4. Issue Purchase Order
5. Issue Vaccination Record
6. Message, Credential Attachment, A2A Message Transport, and Trust System Interop (4-Corner Model)

Trust Foundation Services Subprotocol Use Cases

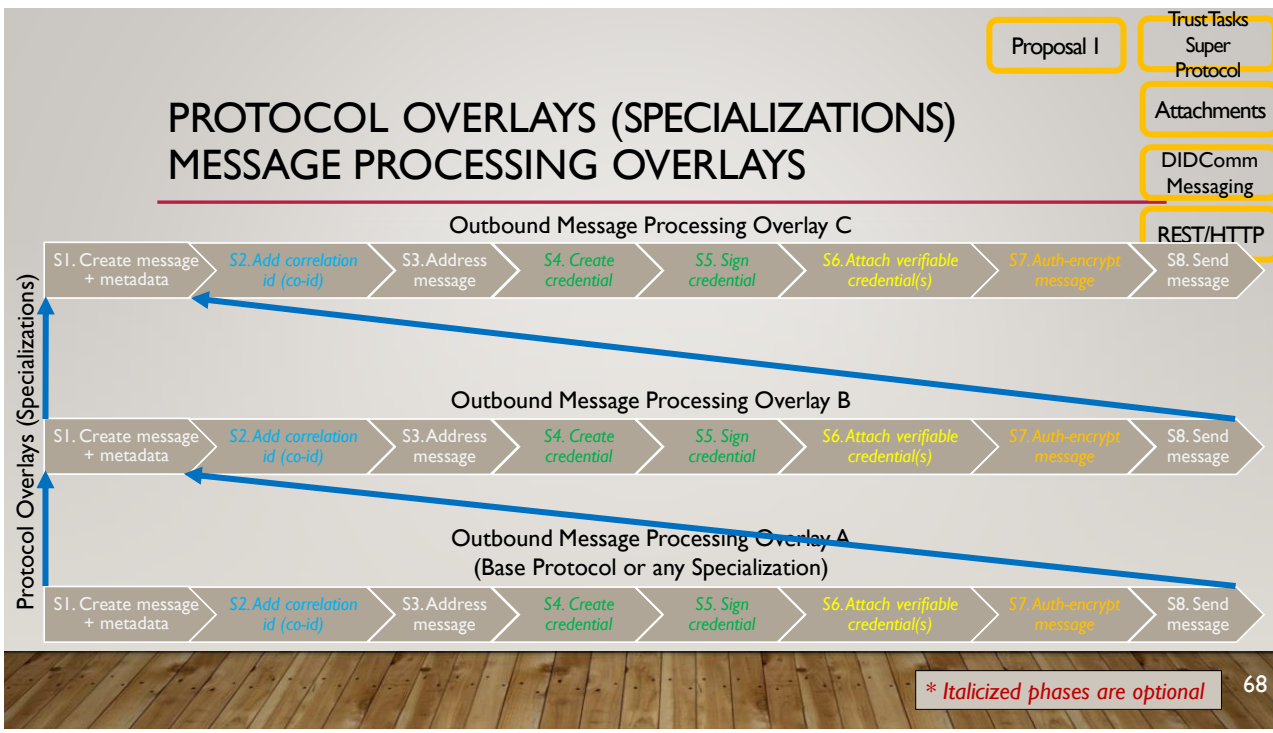
7. DID Resolution via L2 TSP (4 standard DID Resolution methods running over L2 TSP)
8. Intelligent Message Routing through an arbitrary, multiple Agent-based Network

66

66


Proposal I
Trust Tasks
Super Protocol
Attachments
DIDComm Messaging
REST/HTTP
MESSAGE PROCESSING OVERLAYS
Base Outbound Message Processing Overlay
S1. Create message + metadata
S2. Add correlation id (co-id)
S3. Address message
S4. Create credential
S5. Sign credential
S6. Attach verifiable credential(s)
S7. Auth-encrypt message
S8. Send message
Base Inbound Message Processing Overlay
R1. Receive message
R2. Decrypt message
R3. Verify sender
R4. Detach verifiable credential attachments
R5. Verify verifiable credential
R6. Process message + metadata (co-id).
* Italicized phases are optional
67

67


Proposal I
Trust Tasks
Super Protocol
Attachments
DIDComm Messaging
REST/HTTP
PROTOCOL OVERLAYS (SPECIALIZATIONS)
MESSAGE PROCESSING OVERLAYS
Protocol Overlays (Specializations)
Outbound Message Processing Overlay C
Outbound Message Processing Overlay B
Outbound Message Processing Overlay A
(Base Protocol or any Specialization)
S1. Create message + metadata
S2. Add correlation id (co-id)
S3. Address message
S4. Create credential
S5. Sign credential
S6. Attach verifiable credential(s)
S7. Auth-encrypt message
S8. Send message
* Italicized phases are optional
68

68

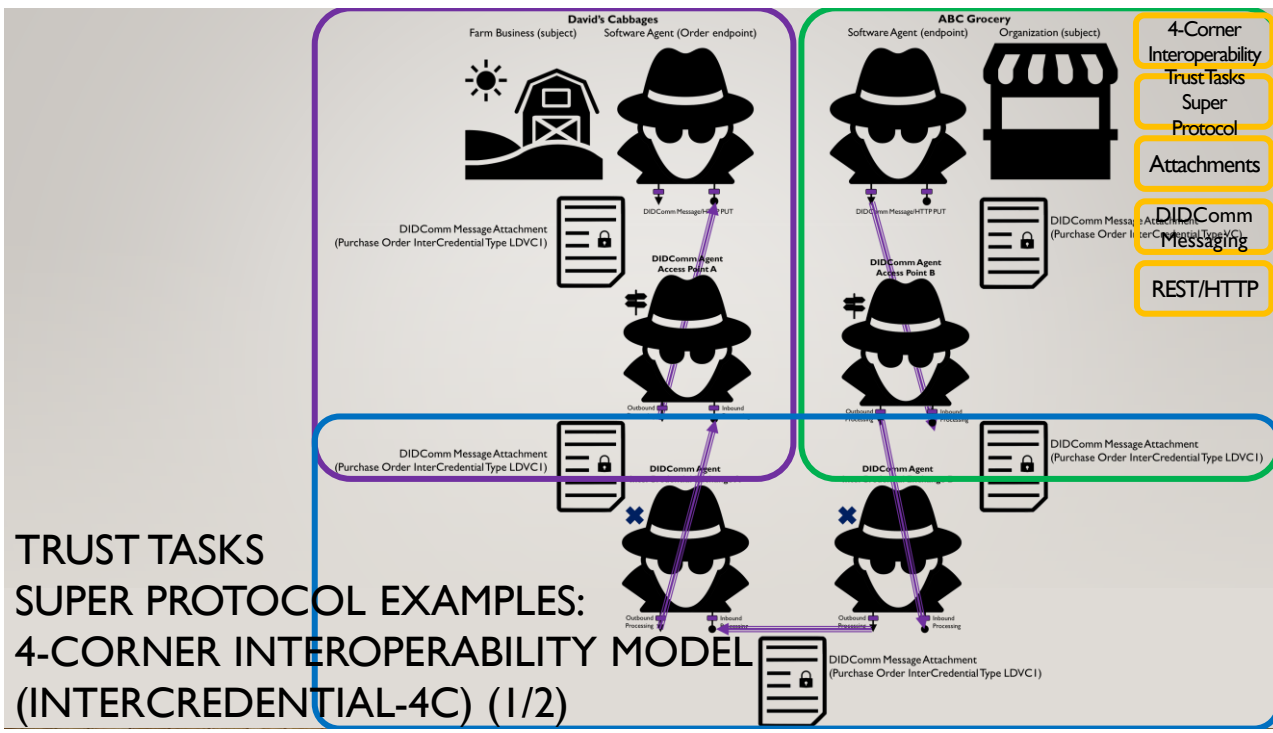
TRUST TASKS SUPER PROTOCOL OVERLAYS (SPECIALIZATIONS)

A specific Trust Tasks Super Protocol Overlay (Specialization) includes (among other things):

1. Select *basis protocol to overlay*: the Base Protocol or a particular Super Protocol/Subprotocol
2. Additional process-specific messages formats/schemas
3. Additional process-specific (or generic standardized) message attachments schemas
4. Override inbound & outbound *message processing overlay* phases (if required)
5. Override specific executable business process workflow template (e.g an OASIS BPMN process workflow template serialized in the OASIS BPMN defined XML serialization format)
6. Additional governance such as business rules, policies, procedures, process (3P) documentation
7. (Optionally) Trust/security/privacy policies for external attachments (see next slide)

Assumption: the Receiver and Sender agents each have an embedded or decentralized workflow engine available to run the business process workflows (true in Web 7.0).

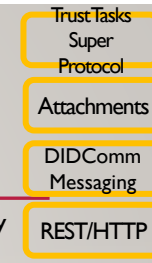
69



TRUST TASKS SUPER PROTOCOL EXAMPLES: 4-CORNER INTEROPERABILITY MODEL (INTERCREDENTIAL-4C) (1/2)

70

EMBEDDED ATTACHMENTS vs. EXTERNAL ATTACHMENTS



1. Embedded Attachments – the attachment content (bytes) is attached to a message by embedding the content directly as a subelement of the message.
   - For embedded attachments, trust/security/privacy can be handled by:
     - a) the attachment format (e.g. as a verifiable credential), and
     - b) the attachment format wrapped by message format (e.g. DIDComm Message auth-encryption)
2. External Attachments – the attachment content (bytes) is stored independently of (external to) the message. The attachment content is "attached" to a message by reference (e.g. a URL message subelement that dereferences to a blob stored on IPFS)
   - Referenced attachments: trust/security/privacy is specified using a Trust Tasks Trust Tasks super protocol
   - While trust/security/privacy of the message (containing the reference to the attachment) is handled by the Trust Spanning Layer Base Protocol, trust/security/privacy of the external attachment (data path) is specified/handled by a Trust Tasks Trust Tasks super protocol (signal/control path)

72

72

ISSUER-HOLDER-VERIFIER MODEL TRUST TASKS SUPER PROTOCOL

73

73

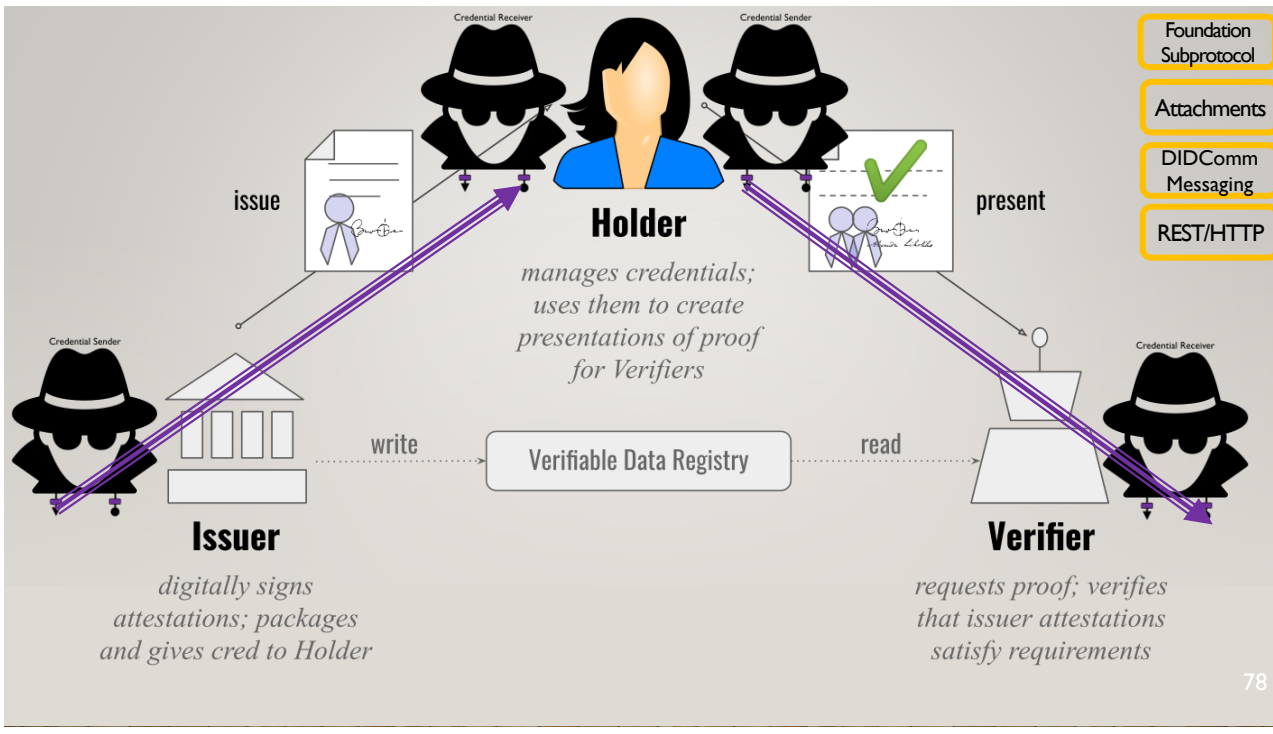
PROPOSAL 4 :TRUST SPANNING PROTOCOL TASK FORCE

- Mission
  - The mission of the TSWG is to draft the ToIP Trust Spanning Protocol V1.0 Specification to meet the requirements for ToIP Layer 2 as specified in the ToIP Technology Architecture V1.0 Specification.
- Deliverables
  - The deliverable of this Task Force is the ToIP Trust Spanning Protocol Specification that must meet the
  - 18 requirements for the ToIP Layer 2 protocol as specified in the ToIP Technology Architecture V1.0 Specification.

- Proposal 4 represents a Unified Trust Spanning Layer Base Protocol solution based on readily available, proven, comprehensive, understandable Internet technologies and specifications

74

74



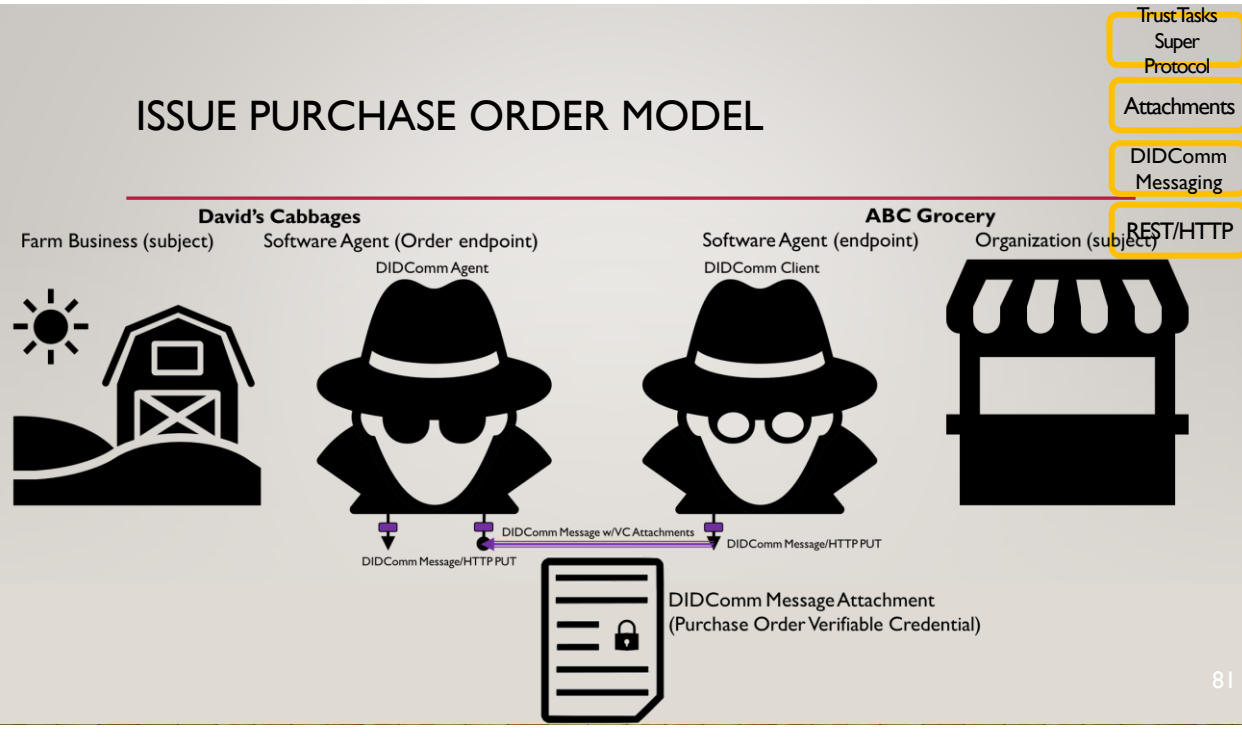
78

78

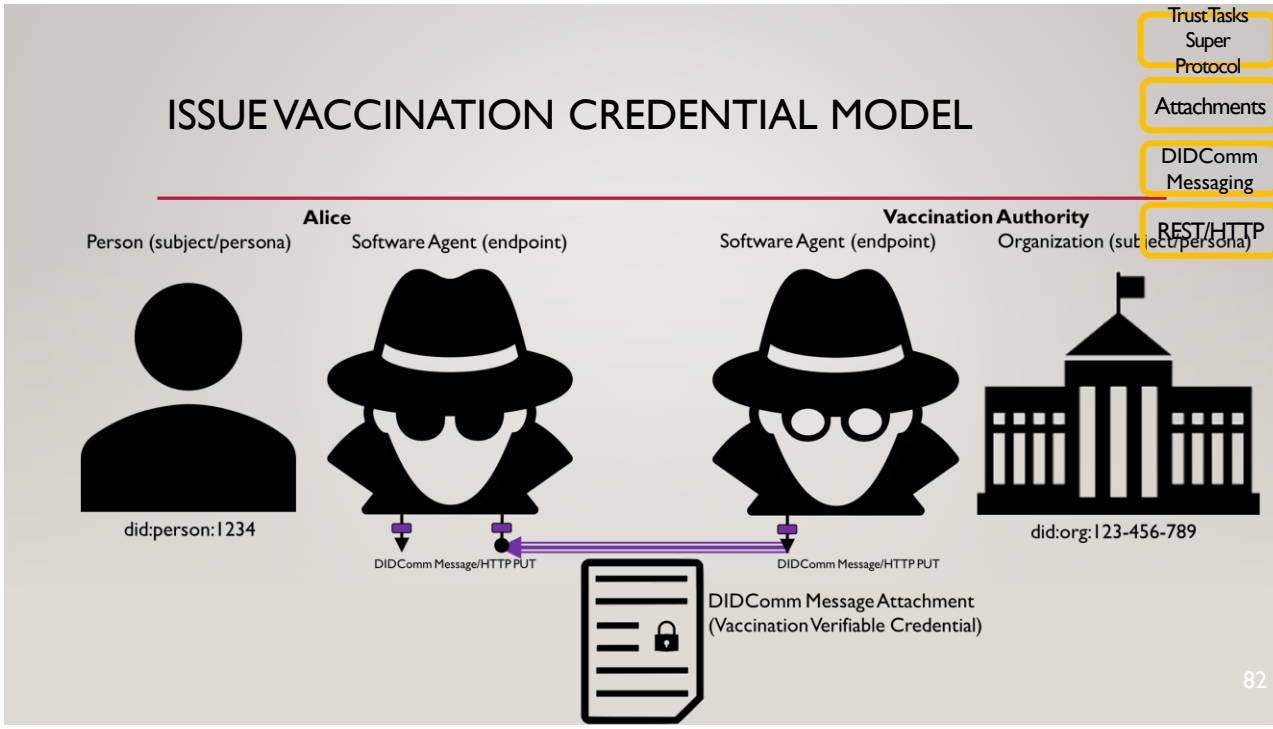
ADDITIONAL EXAMPLES
TRUST TASKS SUPER PROTOCOLS

80

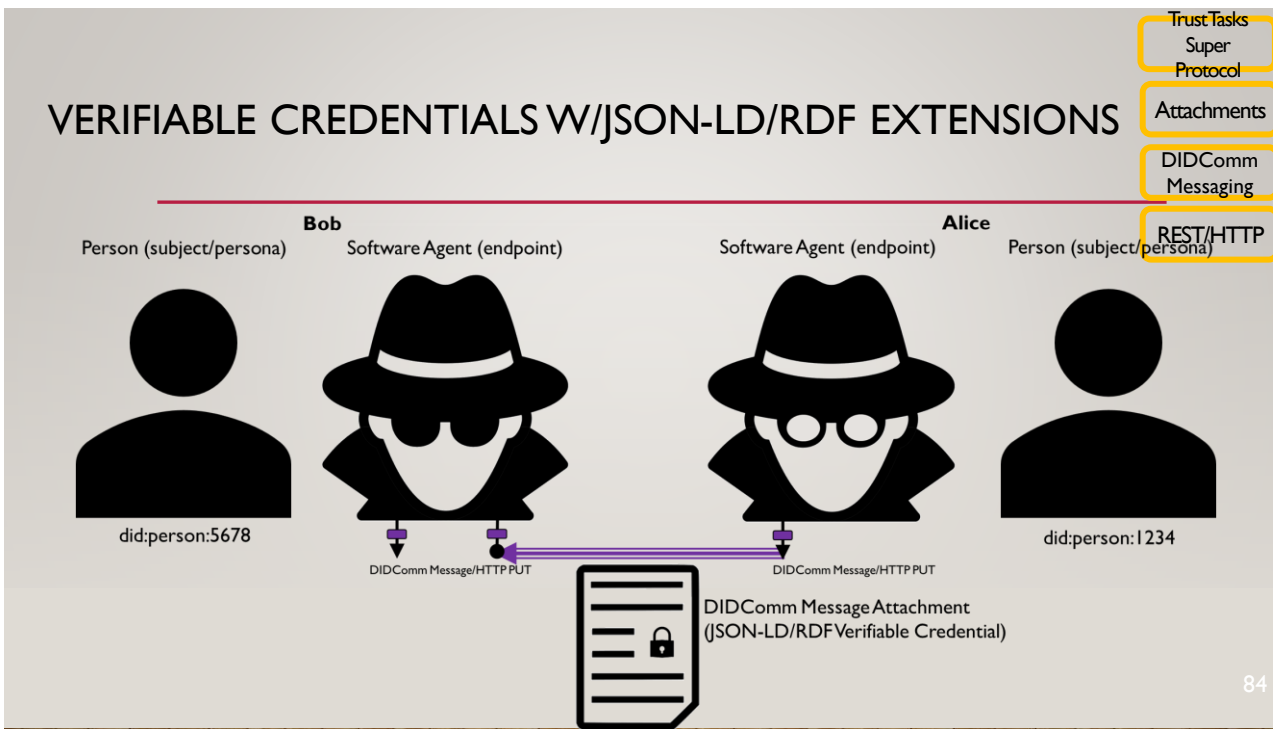
ISSUE PURCHASE ORDER MODEL



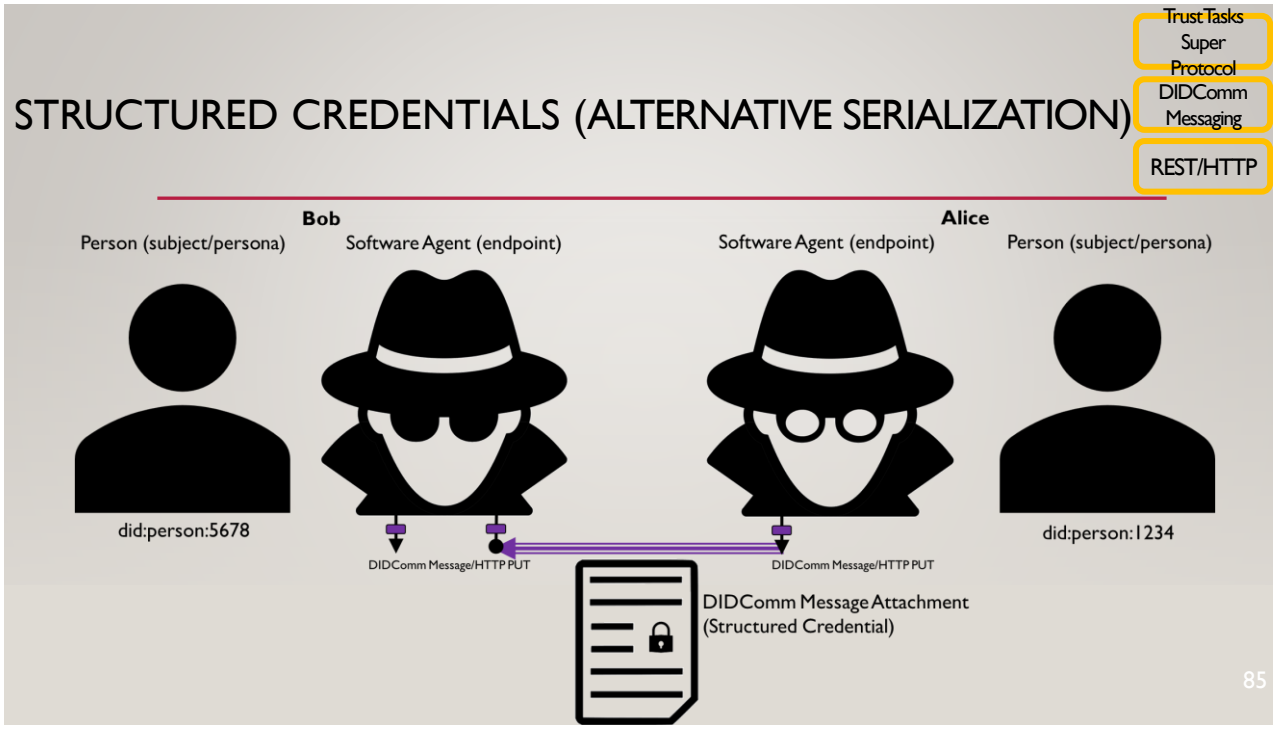
81


ISSUE VACCINATION CREDENTIAL MODEL
Trust Tasks Super Protocol
Attachments
DIDComm Messaging
REST/HTTP
Alice
Person (subject/persona)
Software Agent (endpoint)
Vaccination Authority
Software Agent (endpoint)
Organization (subject/persona)
did:person:1234
did:org:123-456-789
DIDComm Message/HTTP PUT
DIDComm Message/HTTP PUT
DIDComm Message Attachment
(Vaccination Verifiable Credential)
82

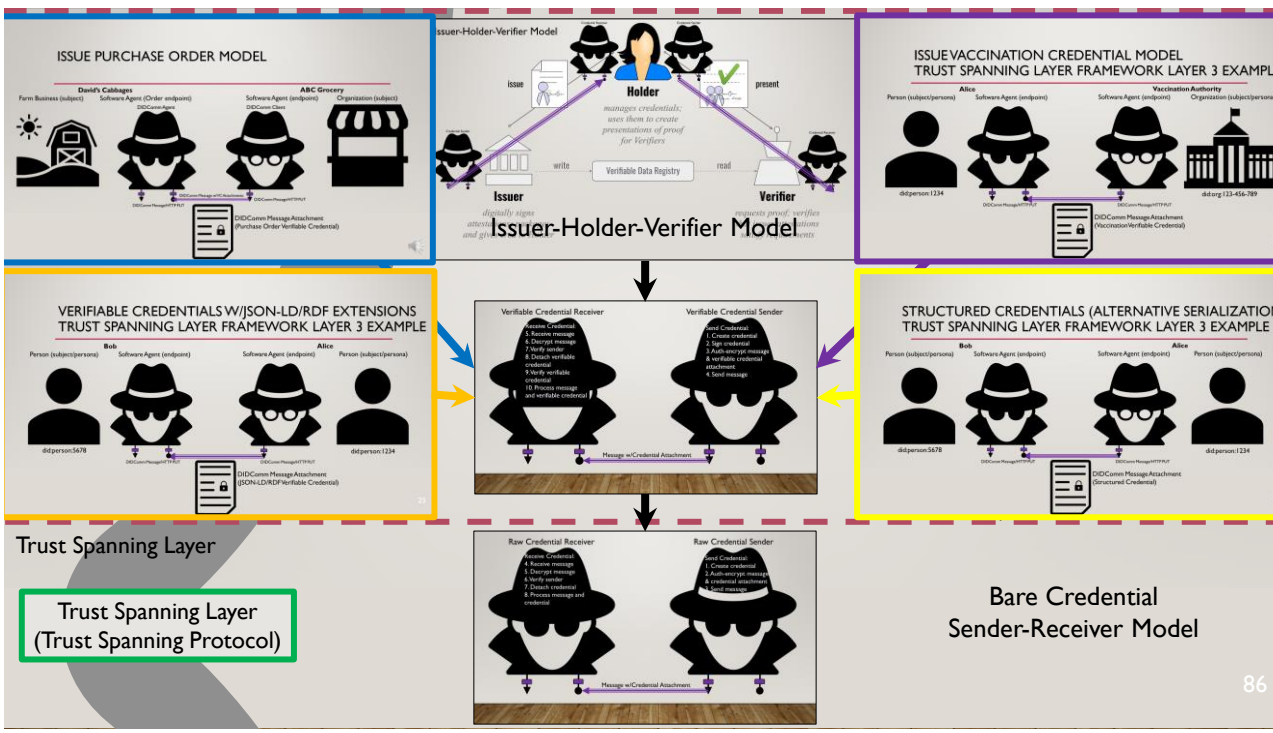
82


VERIFIABLE CREDENTIALS W/JSON-LD/RDF EXTENSIONS
Trust Tasks Super Protocol
Attachments
DIDComm Messaging
REST/HTTP
Bob
Person (subject/persona)
Software Agent (endpoint)
Alice
Software Agent (endpoint)
Person (subject/persona)
did:person:5678
did:person:1234
DIDComm Message/HTTP PUT
DIDComm Message/HTTP PUT
DIDComm Message Attachment
(JSON-LD/RDF Verifiable Credential)
84

84


STRUCTURED CREDENTIALS (ALTERNATIVE SERIALIZATION)
Trust Tasks
Super Protocol
DIDComm Messaging
REST/HTTP
Bob
Person (subject/persona)
Software Agent (endpoint)
Alice
Software Agent (endpoint)
Person (subject/persona)
did:person:5678
DIDComm Message/HTTP PUT
DIDComm Message/HTTP PUT
did:person:1234
DIDComm Message Attachment
(Structured Credential)
85

85


ISSUE PURCHASE ORDER MODEL
Issuer-Holder-Verifier Model
ISSUE VACCINATION CREDENTIAL MODEL
TRUST SPANNING LAYER FRAMEWORK LAYER 3 EXAMPLE
VERIFIABLE CREDENTIALS W/JSON-LD/RDF EXTENSIONS
TRUST SPANNING LAYER FRAMEWORK LAYER 3 EXAMPLE
STRUCTURED CREDENTIALS (ALTERNATIVE SERIALIZATION)
TRUST SPANNING LAYER FRAMEWORK LAYER 3 EXAMPLE
Trust Spanning Layer
Trust Spanning Layer
(Trust Spanning Protocol)
Bare Credential
Sender-Receiver Model
86

86

VALUE-ADD OF A UNIFIED, END-TO-END, SINGLE TRUST SPANNING LAYER BASE PROTOCOL

87

Automated Governance

SIDE BAR: WEB 7.0 AUTOMATIC AGENT CODE GENERATION

DIDCOMMAgent.tsl

```
23  struct DIDCOMMMessage
24  {
25      DIDCOMMEncryptedMessage encryptedMessage;
26  }
27
28  struct DIDCOMMResponse
29  {
30      long rc;
31  }
32
33  protocol DIDCOMMEndpoint
34  {
35      Type: HTTP;
36      Request:  DIDCOMMMessage;
37      Response: DIDCOMMResponse; // void;
38  }
39
40  server DIDCOMMAgent
41  {
42      protocol DIDCOMMEndpoint;
43  }
```


88

SIDE BAR: WEB 7.0 DIDCOMM DID REGISTRY GATEWAY: AUTOMATIC AGENT CODE GENERATION

POP QUIZ
a. Base Protocol
b. Subprotocol
c. Super Protocol
d. None of the above

Web7.DIDCom....Gateway.tsl

```
protocol Create
{
    Type: HTTP;
    Request: CreateDIDCommRequest;
    Response: CreateDIDCommResponse;
}

protocol Read
{
    Type: HTTP;
    Request: ReadDIDCommRequest;
    Response: ReadDIDCommResponse;
}

protocol Update
{
    Type: HTTP;
    Request: UpdateDIDCommRequest;
    Response: UpdateDIDCommResponse;
}

protocol Deactivate
{
    Type: HTTP;
    Request: DeactivateDIDCommRequest;
    Response: DeactivateDIDCommResponse;
}

server DIDRegistryGatewayServer
{
    protocol Create;
    protocol Read;
    protocol Update;
    protocol Deactivate;
}
```

89

89

CONCLUSIONS

94

94

PROPOSAL 4 : TRUST SPANNING PROTOCOL TASK FORCE

- Mission
  - The mission of the TSWG is to draft the ToIP Trust Spanning Protocol V1.0 Specification to meet the requirements for ToIP Layer 2 as specified in the ToIP Technology Architecture V1.0 Specification.
- Deliverables
  - The deliverable of this Task Force is the ToIP Trust Spanning Protocol Specification that must meet the
  - 18 requirements for the ToIP Layer 2 protocol as specified in the ToIP Technology Architecture V1.0 Specification.

- Proposal 4 represents a Unified Trust Spanning Layer Base Protocol solution based on readily available, proven, comprehensive, understandable Internet technologies and specifications

95

CREDENTIAL SENDER-RECEIVER PATTERN TRUST SPANNING LAYER BASE PROTOCOL

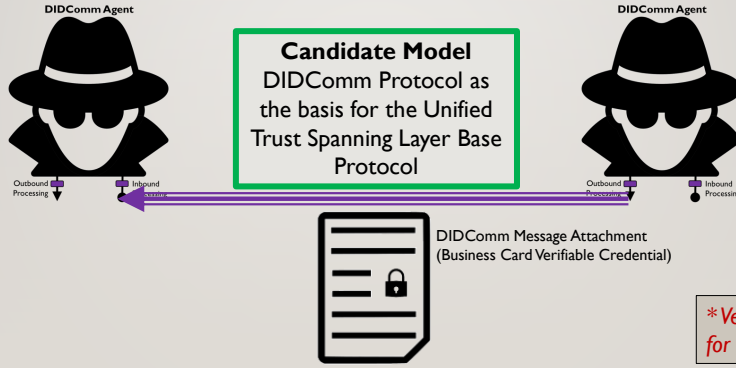
Attachments

DIDComm Messaging

REST/HTTP

Receiver Agent (Inbound Processing)

Sender Agent (Outbound Processing)

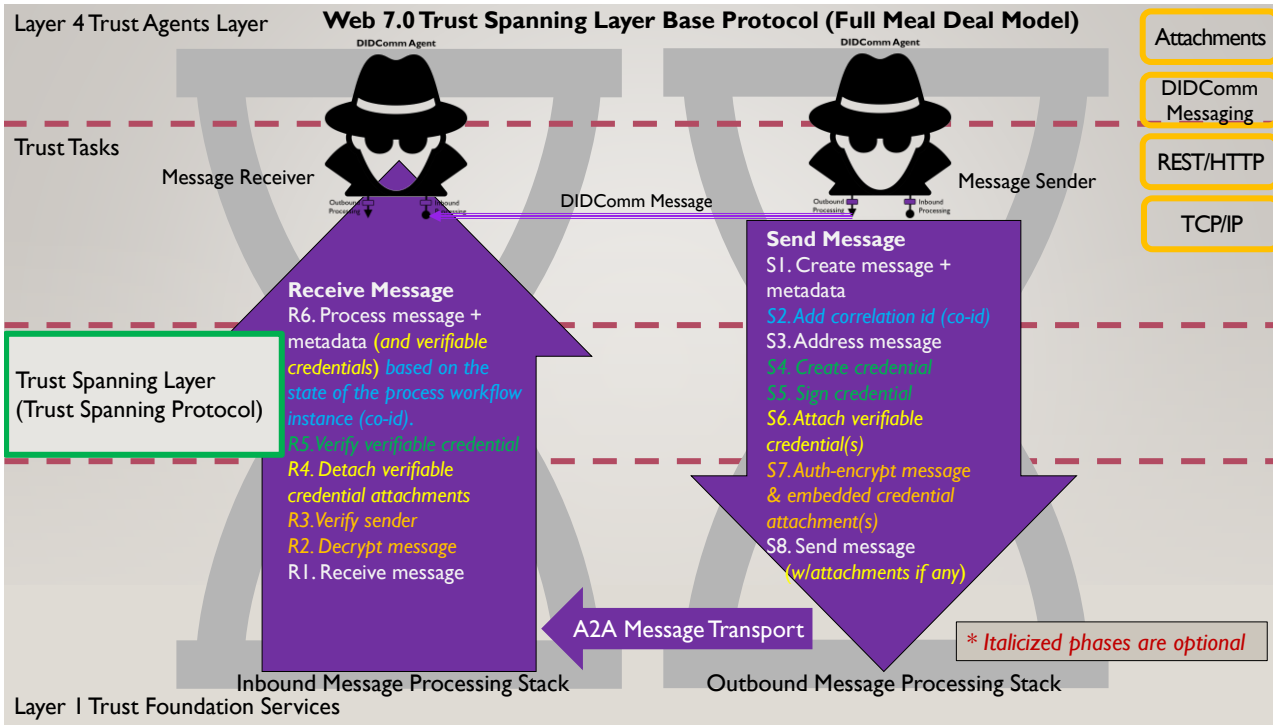


Candidate Model
DIDComm Protocol as the basis for the Unified Trust Spanning Layer Base Protocol

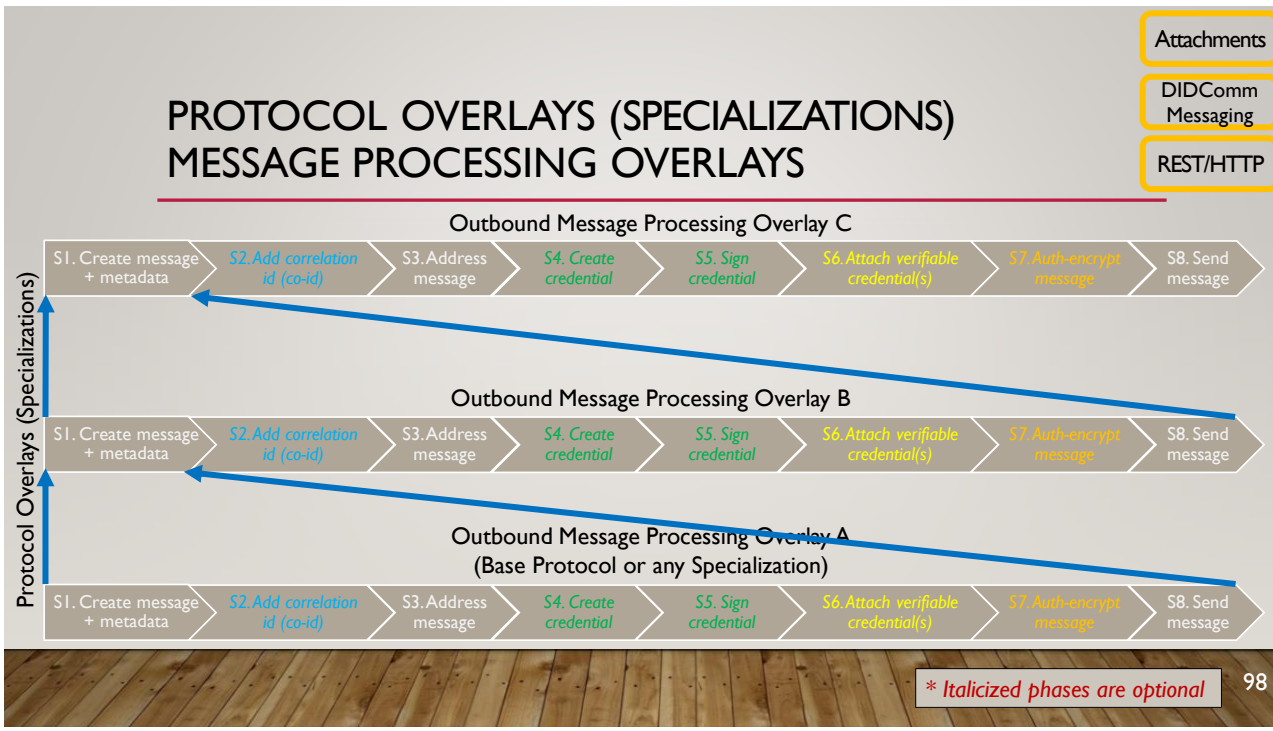
DIDComm Message Attachment
(Business Card Verifiable Credential)

**Verifiable Credentials are used for illustrative purposes only.*

96


Layer 4 Trust Agents Layer
Web 7.0 Trust Spanning Layer Base Protocol (Full Meal Deal Model)
Attachments
DIDComm Messaging
REST/HTTP
TCP/IP
DIDComm Agent
DIDComm Agent
Trust Tasks
Message Receiver
DIDComm Message
Message Sender
Send Message
S1. Create message + metadata
S2. Add correlation id (co-id)
S3. Address message
S4. Create credential
S5. Sign credential
S6. Attach verifiable credential(s)
S7. Auth-encrypt message & embedded credential attachment(s)
S8. Send message (w/attachments if any)
Trust Spanning Layer (Trust Spanning Protocol)
Receive Message
R6. Process message + metadata (and verifiable credentials) based on the state of the process workflow instance (co-id).
R5 Verify verifiable credential
R4. Detach verifiable credential attachments
R3. Verify sender
R2. Decrypt message
R1. Receive message
A2A Message Transport
* Italicized phases are optional
Inbound Message Processing Stack
Outbound Message Processing Stack
Layer 1 Trust Foundation Services

97


Attachments
DIDComm Messaging
REST/HTTP
PROTOCOL OVERLAYS (SPECIALIZATIONS)
MESSAGE PROCESSING OVERLAYS
Outbound Message Processing Overlay C
Outbound Message Processing Overlay B
Outbound Message Processing Overlay A
(Base Protocol or any Specialization)
Protocol Overlays (Specializations)
S1. Create message + metadata
S2. Add correlation id (co-id)
S3. Address message
S4. Create credential
S5. Sign credential
S6. Attach verifiable credential(s)
S7. Auth-encrypt message
S8. Send message
* Italicized phases are optional
98

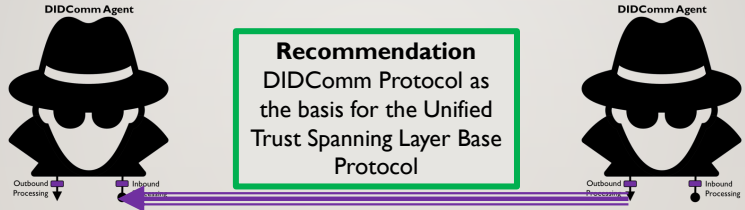
98

CREDENTIAL SENDER-RECEIVER PATTERN TRUST SPANNING LAYER BASE PROTOCOL

Attachments
DIDComm Messaging
REST/HTTP

Receiver Agent (Inbound Processing)

Sender Agent (Outbound Processing)



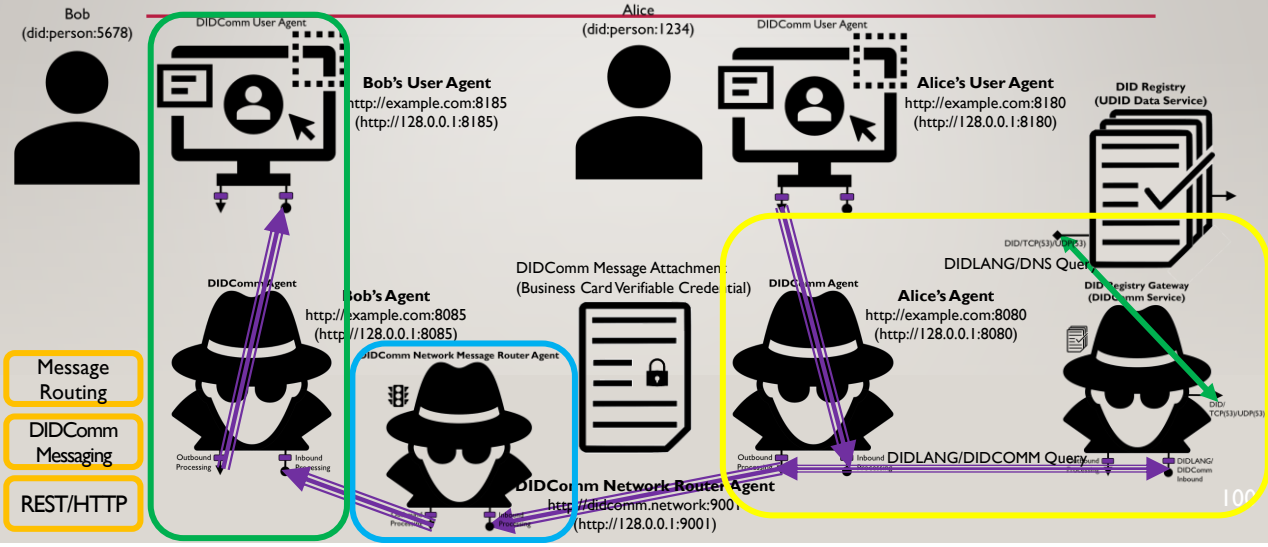
Recommendation
DIDComm Protocol as the basis for the Unified Trust Spanning Layer Base Protocol

DIDComm Message Attachment
(Business Card Verifiable Credential)

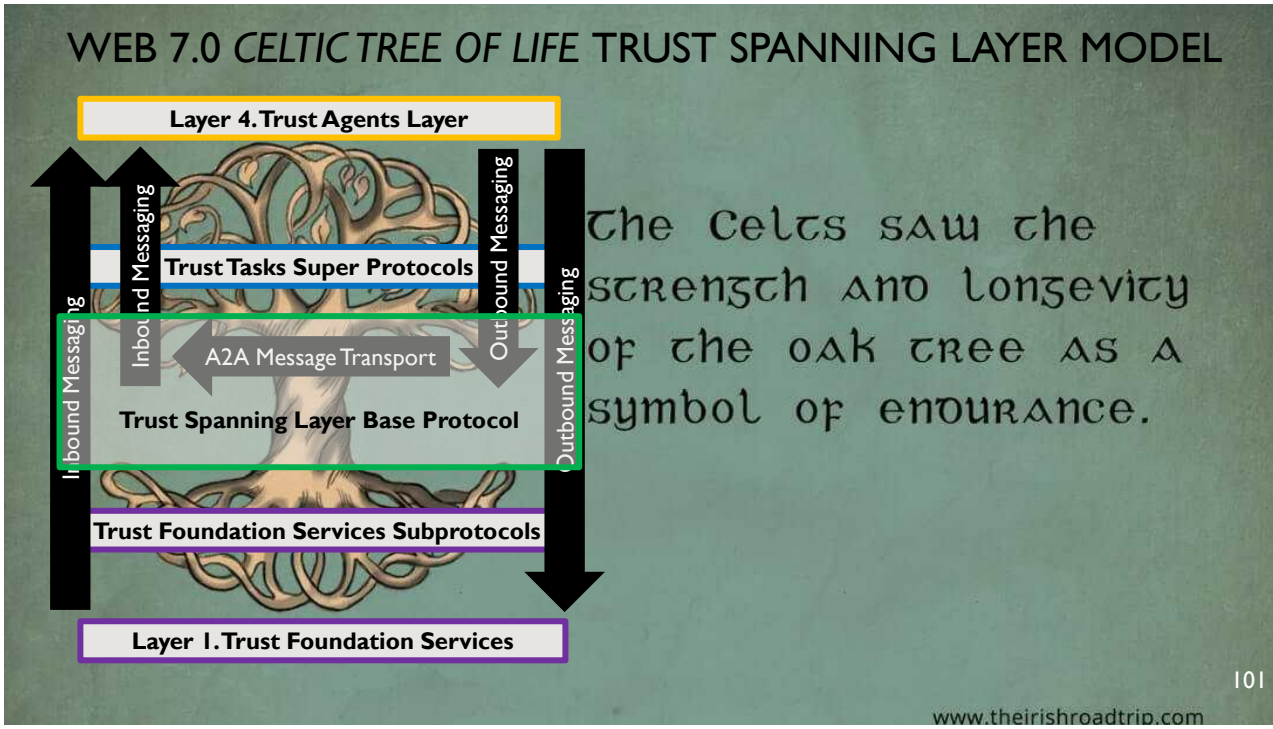
**Verifiable Credentials are used for illustrative purposes only.*

99

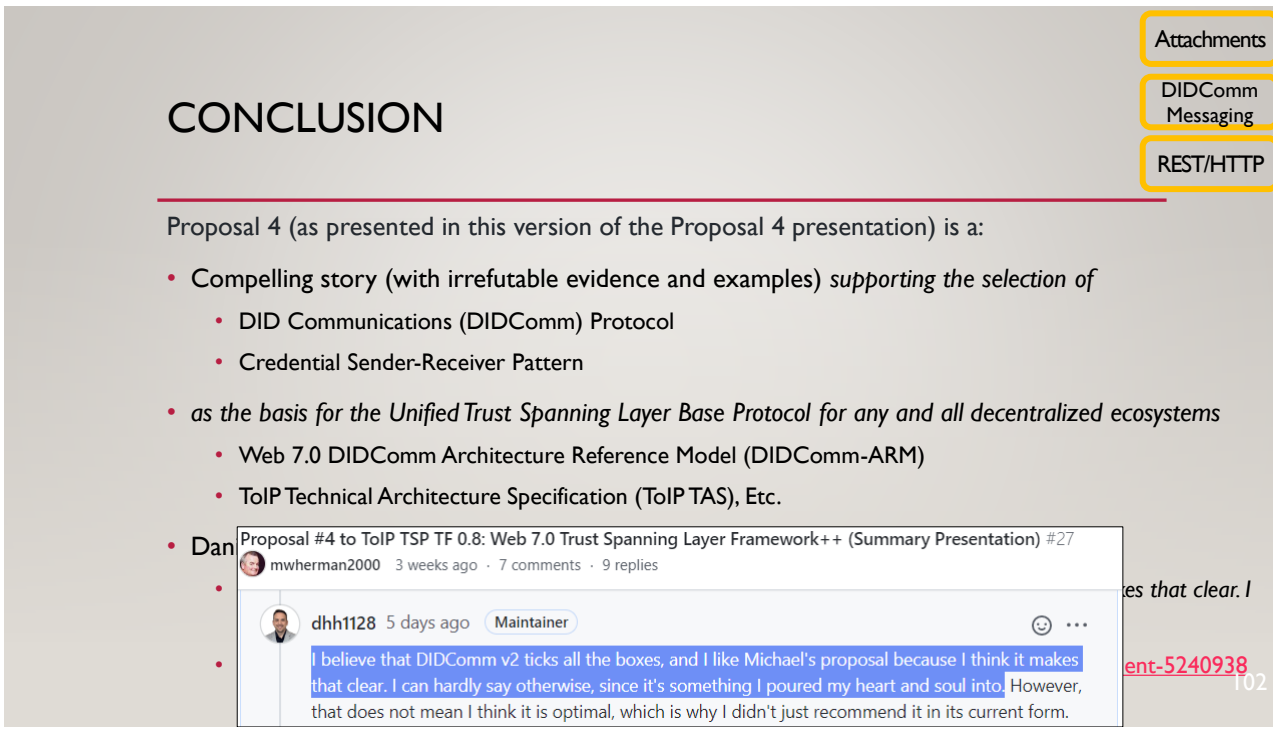
DIDCOMM NETWORK LAYER 4 DEMO CHAT/DIDCOMM/HTTP/NETWORK + VC ATTACHMENTS



100


WEB 7.0 CELTIC TREE OF LIFE TRUST SPANNING LAYER MODEL
Layer 4. Trust Agents Layer
Inbound Messaging
Inbound Messaging
Outbound Messaging
Outbound Messaging
Trust Tasks Super Protocols
A2A Message Transport
Trust Spanning Layer Base Protocol
Trust Foundation Services Subprotocols
Layer 1. Trust Foundation Services
The Celts saw the strength and longevity of the oak tree as a symbol of endurance.
101
www.theirishroadtrip.com

101


Attachments
DIDComm Messaging
REST/HTTP
CONCLUSION
Proposal 4 (as presented in this version of the Proposal 4 presentation) is a:
• Compelling story (with irrefutable evidence and examples) supporting the selection of
• DID Communications (DIDComm) Protocol
• Credential Sender-Receiver Pattern
• as the basis for the Unified Trust Spanning Layer Base Protocol for any and all decentralized ecosystems
• Web 7.0 DIDComm Architecture Reference Model (DIDComm-ARM)
• ToIP Technical Architecture Specification (ToIP TAS), Etc.
• Dan
Proposal #4 to ToIP TSP TF 0.8: Web 7.0 Trust Spanning Layer Framework++ (Summary Presentation) #27
mwherman2000 3 weeks ago · 7 comments · 9 replies
dhh1128 5 days ago Maintainer
I believe that DIDComm v2 ticks all the boxes, and I like Michael's proposal because I think it makes that clear. I can hardly say otherwise, since it's something I poured my heart and soul into. However, that does not mean I think it is optimal, which is why I didn't just recommend it in its current form.
es that clear. I
ent-5240938
102

102

Attachments

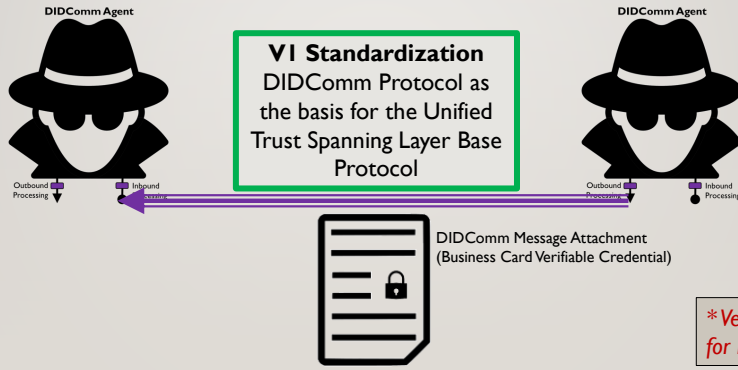
DIDComm Messaging

REST/HTTP

CREDENTIAL SENDER-RECEIVER PATTERN TRUST SPANNING LAYER BASE PROTOCOL

Receiver Agent (Inbound Processing)

Sender Agent (Outbound Processing)



V1 Standardization
DIDComm Protocol as the basis for the Unified Trust Spanning Layer Base Protocol

DIDComm Message Attachment
(Business Card Verifiable Credential)

**Verifiable Credentials are used for illustrative purposes only.*

103

QUESTIONS?

TWEET QUESTIONS TO @FREDDYARCHITECT

104

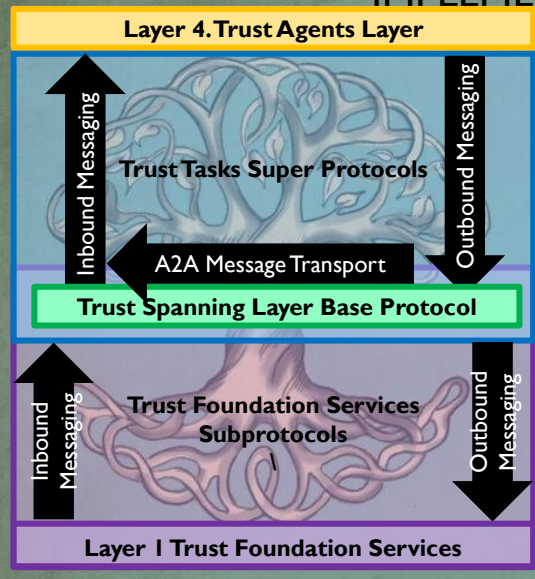
APPENDIX A

Web 7.0 *Celtic Tree of Life* Trust Spanning Layer Model: Implementation View and Layer 1 Trust Foundation Services View

105

105

WEB 7.0: *CELTIC TREE OF LIFE* TSL MODEL IMPLEMENTATION VIEW

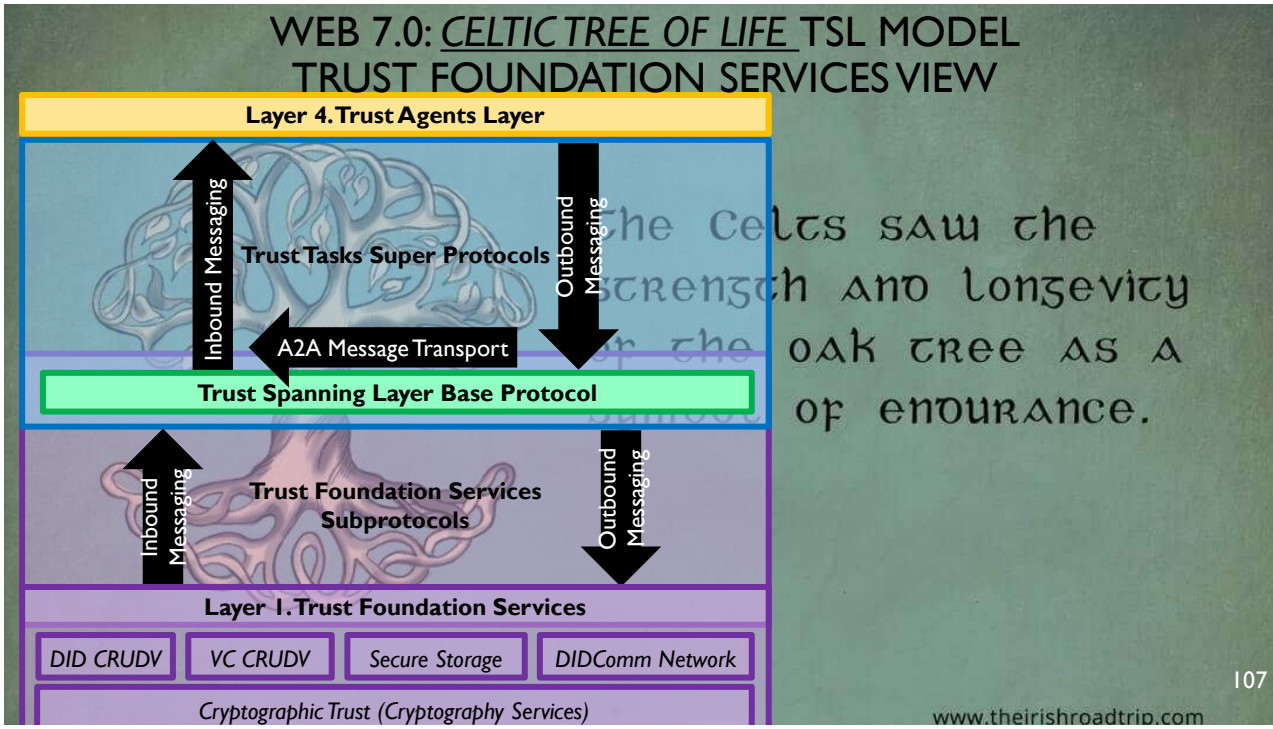


The Celts saw the strength and longevity of the oak tree as a symbol of endurance.

106

www.theirishroadtrip.com

106



107

APPENDIX B

Data Replication (Subscribe/Publish) Scenario: Publisher-Notify/Subscriber-Pull Super Protocol

108

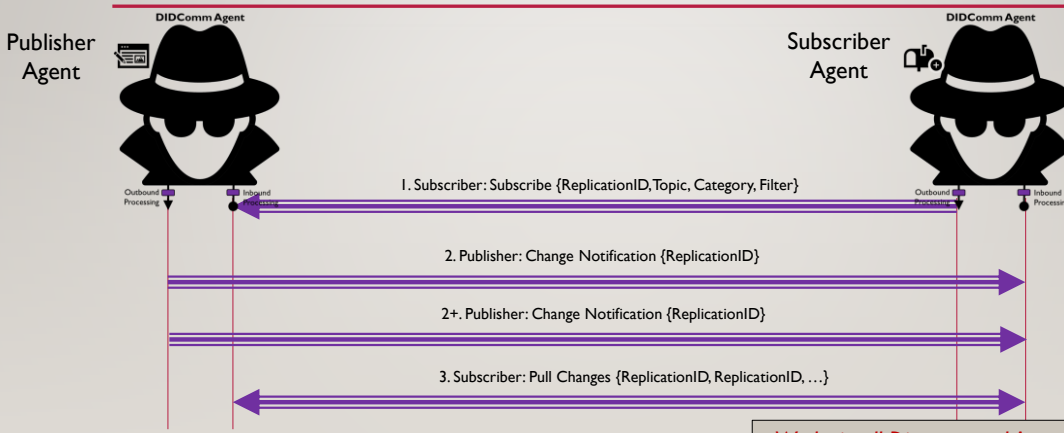
108

DATA REPLICATION (SUBSCRIBE/PUBLISH) SCENARIO PUBLISHER-NOTIFY/SUBSCRIBER-PULL SUPER PROTOCOL

Replication Super Protocol

DIDComm Messaging

REST/HTTP

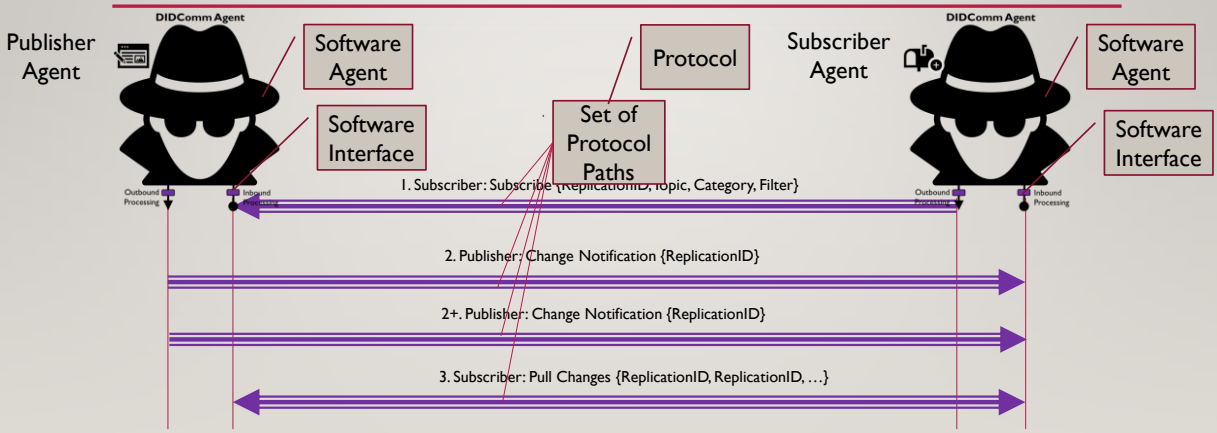


- *Works in all Disconnected Agent scenarios.*
- *No unnecessary risk of clogging the DIDComm Global Network.*

109

109

EFFECTIVE PROTOCOL DIAGRAMS DEPICT PROTOCOLS AS A *SET PROTOCOL PATHS BETWEEN PAIRS OF SOFTWARE INTERFACES*



110

110

APPENDIX C

Trust Protocol Profile-Trust Spanning Layer Framework: Trust Protocol Profile Example Scenarios

TRUST PROTOCOL PROFILE-TRUST SPANNING LAYER FRAMEWORK: TRUST PROTOCOL PROFILE EXAMPLE SCENARIOS

** A Trust Protocol Profile defines a protocol configuration for communication between a pair of software agents. Interoperability is achieved using the Base-Protocol 4-corner interoperability model.*

Trust Protocol Profile X

Verifiable Messaging Protocol (L2 Base)	Identifier Service A (L1 Sub)	Payload Service A (L1 Sub/L3 Super)
Verifiable Message Format(s) *e.g. DIDComm/HTTP Messages* *e.g. DIDComm/AnyTransport Messages*	Verifiable Identifier Specification A Verifiable Identifier Registry A Verifiable Identifier Registry Protocol A	e.g. Verifiable Credential Specification (L1) e.g. Credential Sender-Receiver Pattern (L3)

Trust Protocol Profile Y

Non-Verifiable Messaging Protocol (L2 Base)	Identifier Service B (L1 Sub)	Payload Service B (L1 Sub/L3 Super)
Non-Verifiable Message Format(s) *e.g. REST/HTTP Messages* *e.g. REST/AnyTransport Messages*	Verifiable Identifier Specification B Verifiable Identifier Registry B Verifiable Identifier Registry Protocol B	e.g. mDL Specification (L1) e.g. Credential Sender-Receiver Pattern (L3)

TRUST PROTOCOL PROFILE-TRUST SPANNING LAYER FRAMEWORK: PROPOSAL 4 ASSESSMENT

Proposal	Profile	Messaging Protocol Stack	Message Format	Identity System	Message Payloads (Attachments)
Proposal 4	4A	Verifiable Messaging Protocol: - Attachments - DIDComm Messaging - REST/HTTP - Any Transport (e.g. HTTP)	DIDComm AuthEncrypt Verifiable Messages w/Embedded and/or External Attachments	DID-CORE: - DIDs - Service Endpoints - DID Documents - DID Registry	Verifiable Credentials V2
	4B				mDLs, X.509 Certificates, …
	4C	Non-Verifiable Messaging Protocol: - Basic Messaging - REST/HTTP - Any Transport (e.g. HTTP)	Non-Verifiable Plain Text Messages (e.g. JSON) w/Embedded Attachments		Office Documents, PDF files, …
	4D				XML Data, CSV files, UBL Business Documents, …

115

115

TRUST PROTOCOL PROFILE-TRUST SPANNING LAYER FRAMEWORK: ASSESSMENT OF OTHER PROPOSALS

Proposal	Profile	Messaging Protocol Stack	Message Format	Identity System	Message Payloads (Attachments)
Proposal 3	3A	?	?	?	?
Proposal 2	2A	?	?	?	?
Proposal 1	1A	?	?	?	?

** Admissibility of Proposals 1, 2, and 3 is indeterminant => Withdraw these proposals from further consideration (allow for resubmission)*

116

116

APPENDIX D

Two Layer Honey-Peanut Buffer-Jelly Model for Trust Spanning Layer Frameworks

WEB 7.0 TWO-LAYER HONEY-PEANUT BUTTER-JELLY (HPBJ) MODEL FOR TRUST SPANNING LAYER FRAMEWORKS

Layer 4. Trust Agents (Software) Layer

Trust Tasks Super Protocols (Jelly)

Trust Spanning Layer Base Protocol (Peanut Butter)

Trust Foundation Services Subprotocols (Honey)

Layer 1. Trust Foundation Services (Software) Layer

THE END

TWEET QUESTIONS TO @FREDDYARCHITECT

119