TRISA Hackathon

TRISA

Introduction

Frank Steegmans
SVP Engineering
CipherTrace

Jelle Vink
Senior Director Cloud Engineering
CipherTrace

TRISA

Hackathon Agenda: Day 1, Tuesday

- Morning common with Compliance Track

- 1:00 PM 2:00 PM Hosted Lunch
- 2:00 PM 2:20 AM Technical Overview and Code Walk Through
- 2:20 AM 3:00 PM Kickoff + Introductions
- 3:00 PM 3:30 PM Project and Team Selection
- 3:30 PM 3:50 PM Networking Break
- 3:50 PM 5:30 PM Hackathon team work
- 5:30 PM 7:30 PM Hosted Networking Reception
- 7:30 PM Continued hacking

TRISA

Hackathon Agenda: Day 2, Wednesday

• 8:00 AM	9:00 AM	Carbs and Coffee
• 9:00 AM	9:15 AM	Stand-up
• 9:15 AM	10:30 AM	Hackathon continued
• 10:30 AM	10:45 AM	Networking Break
• 12:30 PM	1:30 PM	Hosted Lunch
• 1:30 PM	2:30 PM	Hackathon continued
• 2:30 PM	2:45 PM	Submissions due
• 2:45 PM	3:00 PM	Networking Break
• 3:00 PM	5:00 PM	Project Presentations
• 5:00 PM	5:30 PM	Judging & Winners

TRISA

Travel Rule Information Sharing Architecture

TRISA Technical Design Proposal

TRISA

TRISA High Level Goals

- Enable compliance with the FATF and FinCEN Travel Rules for cryptocurrency transaction identity info
- Without modifying the core blockchain protocols
- Without incurring increased transaction costs or modifying virtual currency peer-to-peer transaction flows.

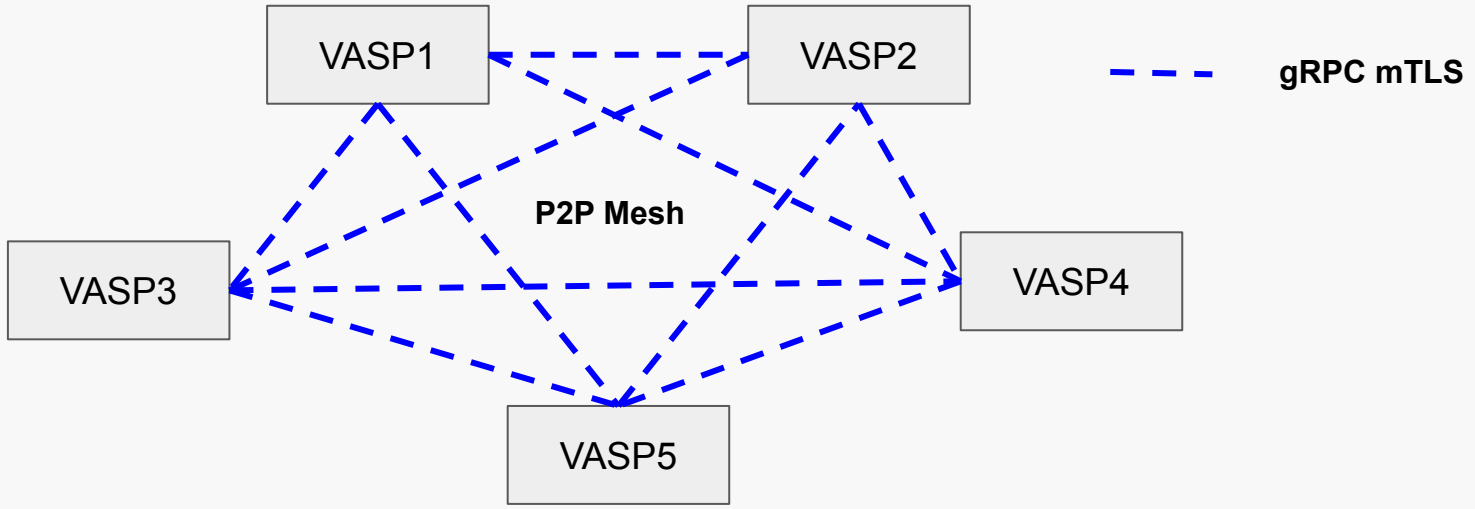
TRISA

TRISA Technical Design Goals

- Open source model, community governed
- Peer-to-peer network using industry trust standards
- Easy to integrate using TRISA libraries or TRISA APIs
- Extensible message format and transport
- Incorporate other trust networks

TRISA

Peer-to-Peer Mesh



TRISA

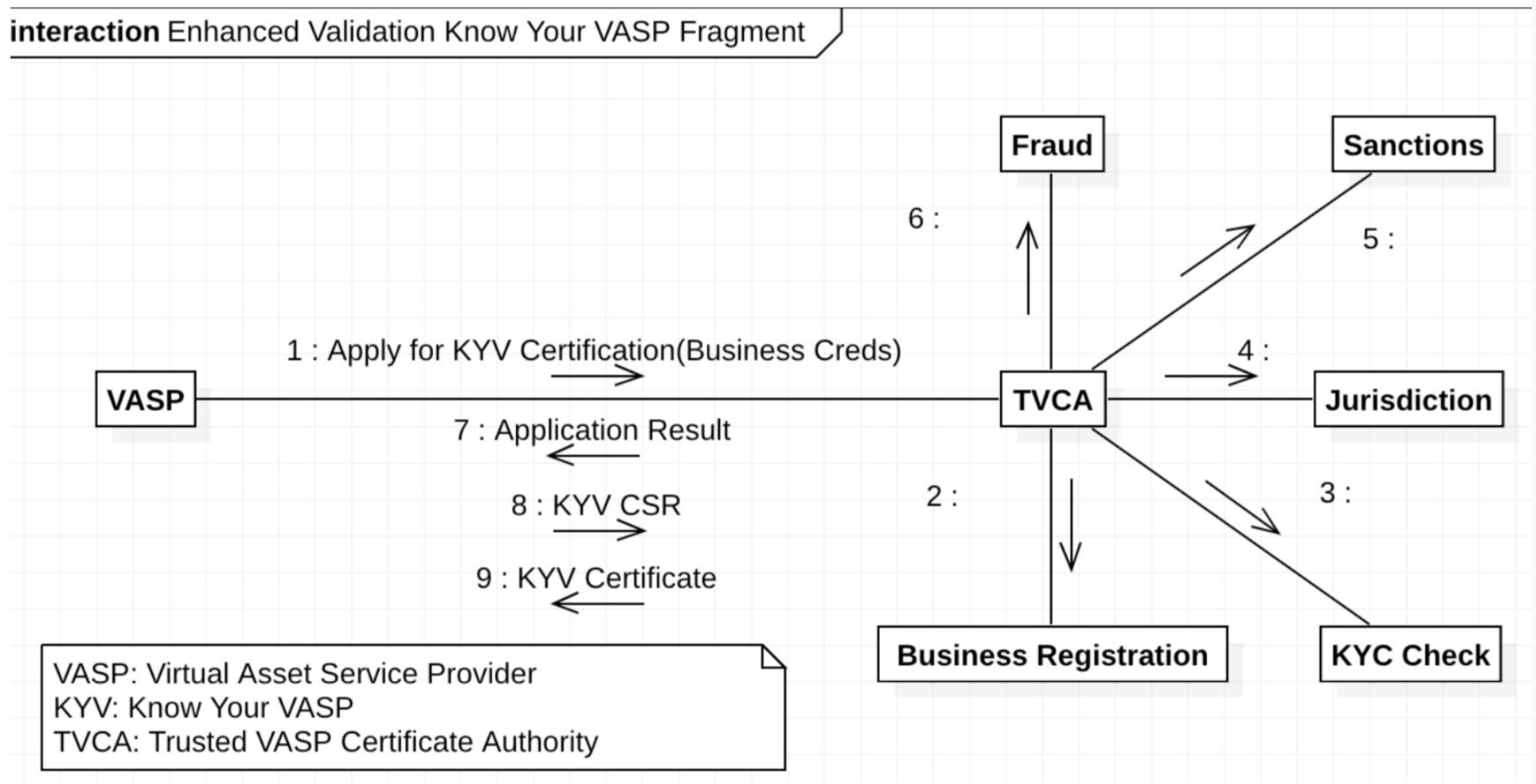
Trusted Communications Between VASPs

Trust Establishment

- Public Key Infrastructure
  - 3rd Party operated
  - Performs enhanced validation
  - Multi party trust model
  - Governed by TRISA community
- Use of mutual TLS on every connection
  - Ensures strong trust model

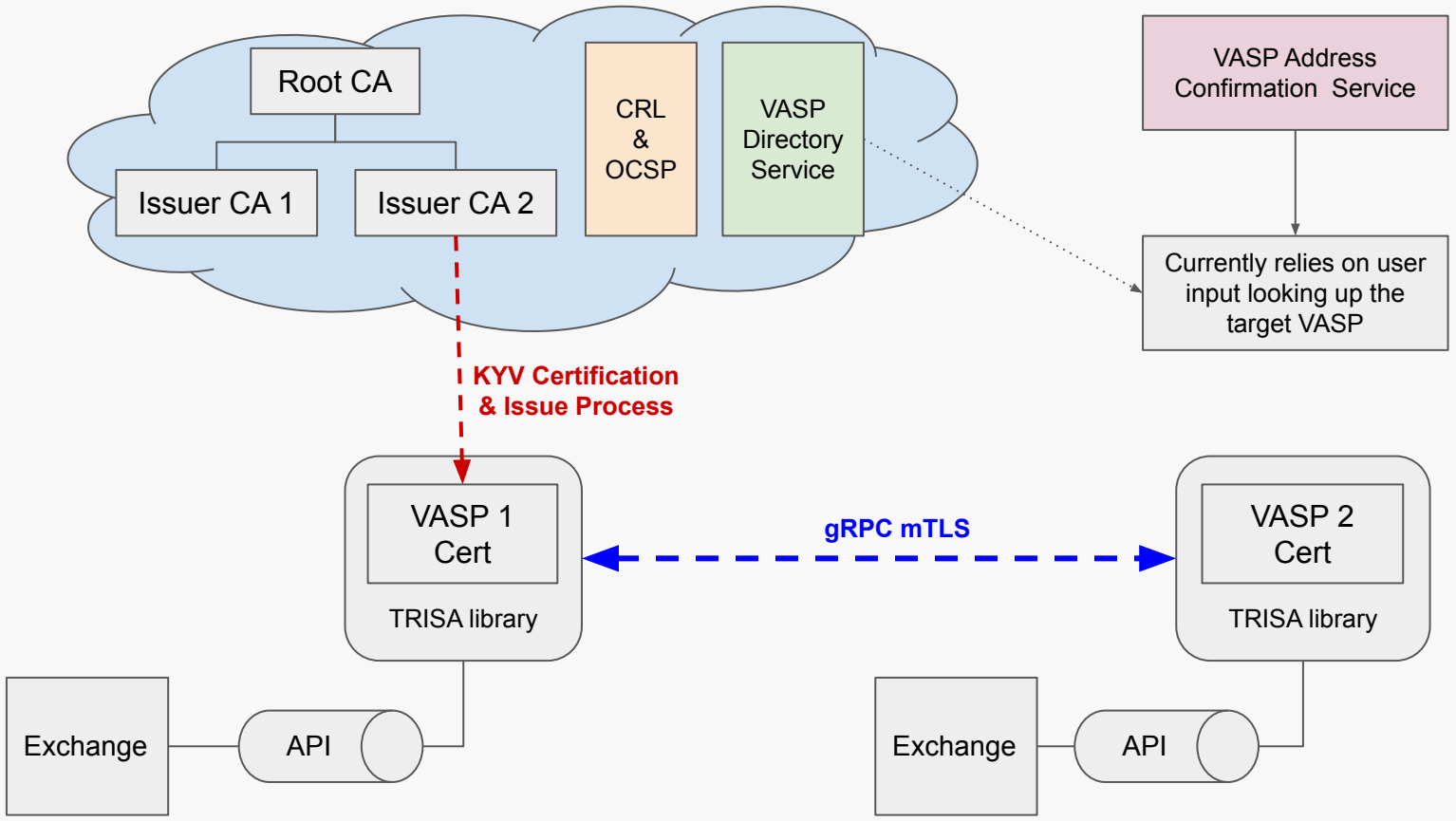
TRISA

PKI Enhanced Validation



TRISA

PKI Enhanced Validation



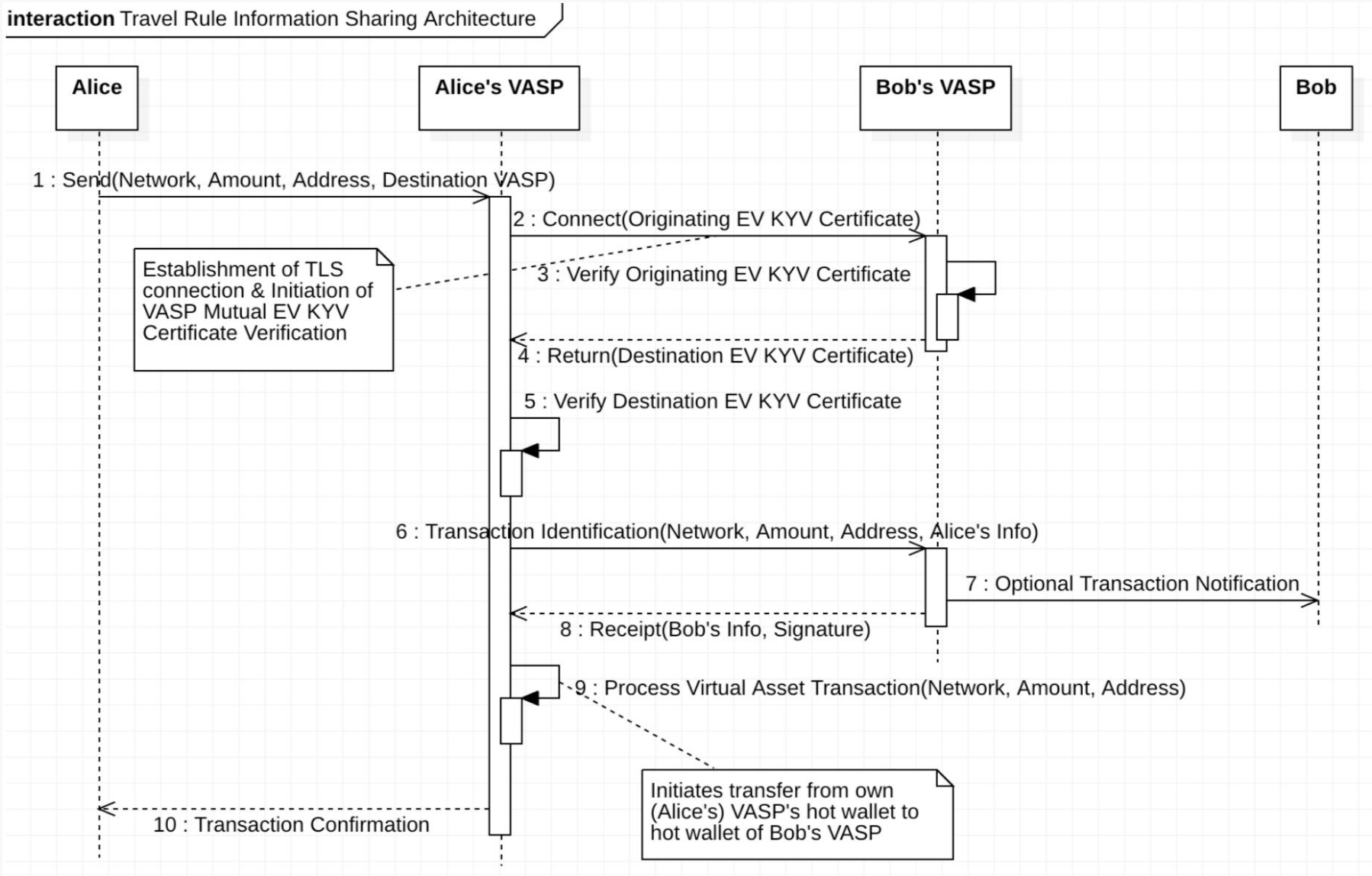
TRISA

Message Format

- Transaction data
  - Identity info
  - Blockchain info
- Extensible
  - Default fields
  - Custom/ad-hoc fields
- Transport
  - gRPC
  - protobuf

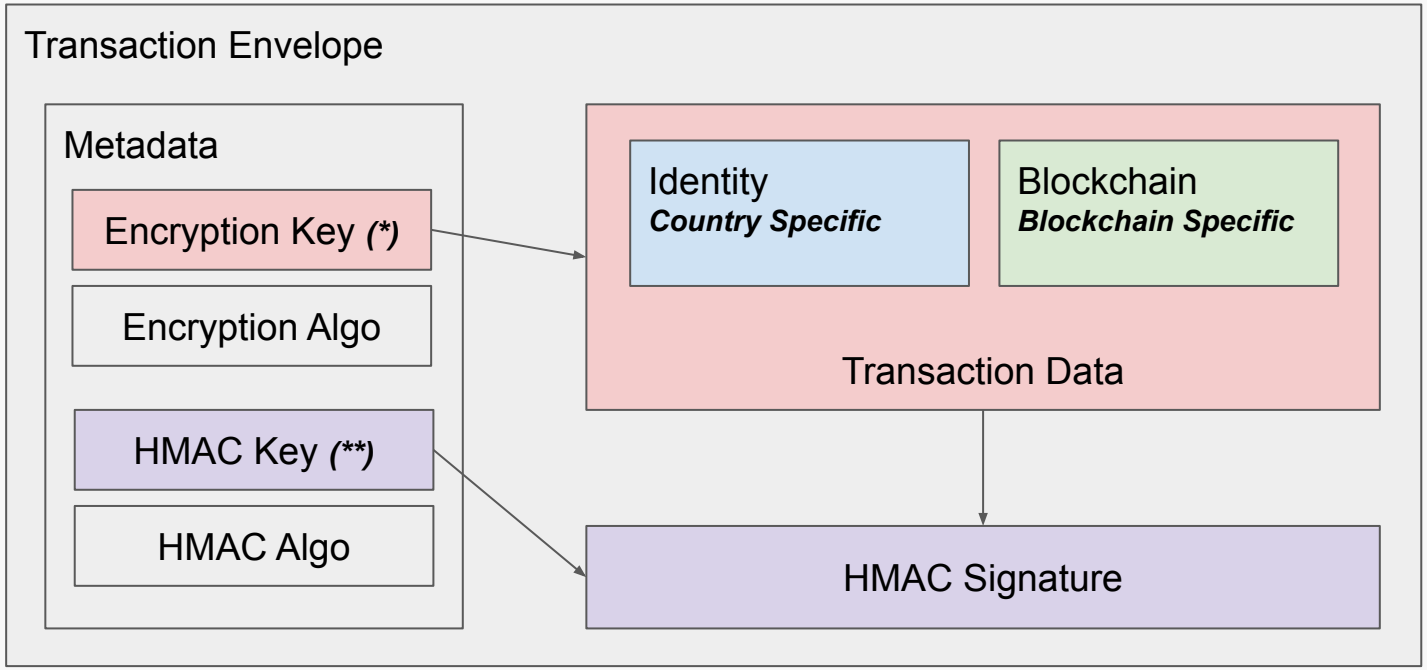
TRISA

Message Flow



TRISA

Message Format



(*) Encrypted using Pub Key of receiving VASP
(**) Encrypted using Priv Key of sender VASP

TRISA

Transaction Data

```
message Transaction {
    // The transaction identifier generated by the sender. Any response
    // to a transaction request needs to carry the same identifier.
    string id = 1;

    // Encrypted TransactionData
    bytes transaction = 2;

    // Encryption key used to encrypt the transaction blob. This key itself
    // is encrypted using the public key of the receiver.
    bytes encryption_key = 3;

    // The encryption algorithm used to encrypt the transaction blob.
    string encryption_algorithm = 4;

    // HMAC signature calculated from encrypted transaction blob.
    bytes hmac = 5;

    // The HMAC secret used to calculate the HMAC signature. This secret
    // itself is encrypted using the public key of the receiver.
    bytes hmac_secret = 6;

    // The algorithm used to calculate the HMAC signature.
    string hmac_algorithm = 7;
}
```

```
message TransactionData {
    // Identity contains any valid identity structure.
    google.protobuf.Any identity = 1;

    // Data contains the network specific data.
    google.protobuf.Any data = 2;
}
```

TRISA

Identity Information

```proto
message TransactionData {
    // Identity contains any valid identity structure.
    google.protobuf.Any identity = 1;

    // Data contains the network specific data.
    google.protobuf.Any data = 2;
}
```

```proto
package trisa.identity.us.v1alpha1;

option go_package = "github.com/trisac

message Identity {
    string first_name = 1;
    string last_name = 2;
    string ssn = 3;
    string state = 4;
    string driver_license = 5;
}
```

```proto
package trisa.identity.be.v1alpha1;

option go_package = "github.com/trisac

message Identity {
    string first_name = 1;
    string last_name = 2;
    string national_number = 3;
    string city_of_birth = 4;
}
```

TRISA

Network Data

```
message TransactionData {
    // Identity contains any valid identity structure.
    google.protobuf.Any identity = 1;

    // Data contains the network specific data.
    google.protobuf.Any data = 2;
}
```

```
package trisa.data.bitcoin.v1alpha1;

option go_package = "github.com/trisa

message Data {
    string source = 1;
    string destination = 2;
    int32 amount = 3;
}
```

```
package trisa.data.ethereum.v1alpha1;

option go_package = "github.com/trisa

message Data {
    string source = 1;
    string destination = 2;
    int32 amount = 3;
}
```

TRISA


TRISA
Hackathon Kick-off
3:19
Search
BITCOIN
Crypto
$3,812.57
+$10.72 (0.28%) TODAY
LIVE 1D 1W 1M 3M 1Y 5Y
The Robinhood Crypto chat is currently unavailable.
Buy

Hackathon Rules

- Participants
  - Contribute to multiple teams
  - Only be part of 1 primary team (eligibility for prices)
- Project & Teams
  - To qualify for competition need to be submitted by 5:30 pm Tuesday
  - Project summary
  - Team members (designate roles such as lead, speaker, PM, dev, etc.)
- Basic TRISA interoperability needs to be maintained & demonstrated
  - Show test transactions with the test bed VASP nodes

TRISA

TRISA Hackathon Judging Dimensions

- Industry relevance
- Innovation
- Technical complexity
- Presentation

TRISA

Project Proposals and Ideas

TRISA Improvement Proposals

- https://trisacrypto.github.io/trisa_improvement_proposal/
- Improvement proposals:
  - TIP-1 Add Transaction details exchange between VASPs post-transaction
  - TIP-2 Add Life Cycle Events based Plug-in system
  - TIP-2 Create VASP Directory Service Protocol
  - TIP-3 Create Address Directory Service Protocol
  - TIP-4 Create DNS Guidelines
  - TIP-5 Add compliance configurability
  - TIP-6 Add FATF and Regulation Business Logic and configurability

TRISA

Other Ideas

- Integrating transaction processing and monitoring
- Integrating with KYC solution
- Transaction message standards
- BIP 75 message translation
- Certificate extensions – to support multi-key types

TRISA

Other Ideas

- Top-level coalition formation and management
- Selective disclosure of user data
- Privacy-preserving identity credential attestation
- Encryption mechanisms to protect PII at rest and in transit
- Transparency reporting mechanisms for VASPs
- Extending TRISA to other plug-ins and languages

Project and Team Selection


TRISA
TRISA Code Repositories
3:19
Search
BITCOIN
Crypto
$3,812.57
+$10.72 (0.28%)
LIVE
1D
1W
1M
3M
1Y
5Y
The Robinhood Crypto chat is currently unavailable.
Buy

Community Governance

- Nurture a non-political open source community
- Bylaws to have a clean decision process:
  - Protocols
  - Trust Network

- Github repo: https://github.com/trisacrypto/trisa
- Documentation: https://trisacrypto.github.io/
- Docker: https://cloud.docker.com/repository/docker/trisacrypto/trisa

TRISA

Transaction Sample VASP1 —> VASP2

```
INFO[0009] sent transaction d55723cd-c1e6-42a5-9cec-31792ff9e6c9 to vasp2.example.com:8092
  identity="first_name:\"John\" last_name:\"Doe\" ssn:\"001-0434-4983\" state:\"CA\" drive
r_license:\"FA-387463\" " identity-type=trisa.identity.us.v1alpha1.Identity network="sourc
e:\"baba71c0-72b2-479e-aa5c-57a562c9ccb5\" destination:\"06cdd762-d87d-458c-99e3-134609055
043\" " network-type=trisa.data.bitcoin.v1alpha1.Data
```

TRISA

Transaction Received by VASP2 (raw)

```
INFO[0076] protocol envelope for incomingtransaction e12ffe21-6fb1-4568-8e03-b5b6af804d0c
 direction=incoming enc_algo=AES256_GCM enc_blob="[175 58 218 144 123 97 217 173 242 65 21
0 199 10 49 24 243 108 251 234 65 79 252 76 43 39 79 97 86 235 138 129 17 96 73 142 1 180
167 216 194 137 116 98 160 148 99 107 73 239 218 11 104 20 0 163 155 165 110 95 1 211 55 1
76 102 14 20 205 162 116 48 235 250 217 163 133 125 158 62 75 75 169 232 248 214 223 0 213
 94 78 14 63 244 121 78 195 251 157 51 113 99 222 114 238 235 79 131 46 170 178 59 241 115
 197 47 184 160 82 189 66 86 173 143 23 72 118 121 32 174 180 172 28 239 223 229 96 225 57
 202 52 23 104 213 248 201 113 133 188 136 203 112 110 1 108 135 146 76 151 189 123 9 15 1
1 196 142 128 233 198 23 76 88 129 161 113 179 184 240 198 184 14 213 71 149 62 231 194 92
 233 81 8 219 90 140 76 144 191 145 133 16 124 73 106 154 32 31 15 123 8 72 232 176 175 33
 228 26 59 239 253 154 76 138 227 151 209 233 229 62 99 74 36 222 115 52 222 198 239 56 10
8 166 233 148 214 32 162 66 126 20 138 30 249 116 155 249 23 114 189 230 48 226 149 50 113
 177 55 193 246]" hmac="[187 105 5 236 197 35 67 92 142 246 253 98 193 2 75 100 13 226 247
 243 71 149 124 134 133 132 22 87 4 196 67 219]" hmac_algo=HMAC_SHA256
```

TRISA

Transaction Exchange (decoded)

```
INFO[0076] received transaction e12ffe21-6fb1-4568-8e03-b5b6af804d0c from vasp1.example.co
m  identity="first_name:\"John\" last_name:\"Doe\" ssn:\"001-0434-4983\" state:\"CA\" driv
er_license:\"FA-387463\" " identity-type=trisa.identity.us.v1alpha1.Identity network="sour
ce:\"de077145-bd08-48b0-80c3-a3b1ae441c58\" destination:\"d901bc52-7197-40a5-b722-b7bf1ba6
cda6\" " network-type=trisa.data.bitcoin.v1alpha1.Data
```

```
INFO[0076] sent transaction response for e12ffe21-6fb1-4568-8e03-b5b6af804d0c to vasp1.exa
mple.com  identity="first_name:\"Jane\" last_name:\"Foe\" national_number:\"109-800211-69\
" city_of_birth:\"Zwevezele\" " identity-type=trisa.identity.be.v1alpha1.Identity
```

TRISA

PKI Testnet

- Playground to easily test drive against a real-world environment
- Integration testing environment & conformance testing
- Useful to validate functionality without disrupting production

http://testnet.trisa.ciphertrace.com/

TRISA

Testnet Online VASPs

- vasp1.trisa.ciphertrace.com
- vasp2.trisa.ciphertrace.com
- vasp3.trisa.ciphertrace.com

TRISA

Local Demo Setup

```
make demo-docker
```

- Running VASPs locally using docker compose
- See https://trisacrypto.github.io/getting_started/demo/

TRISA

Thank you


TRISA