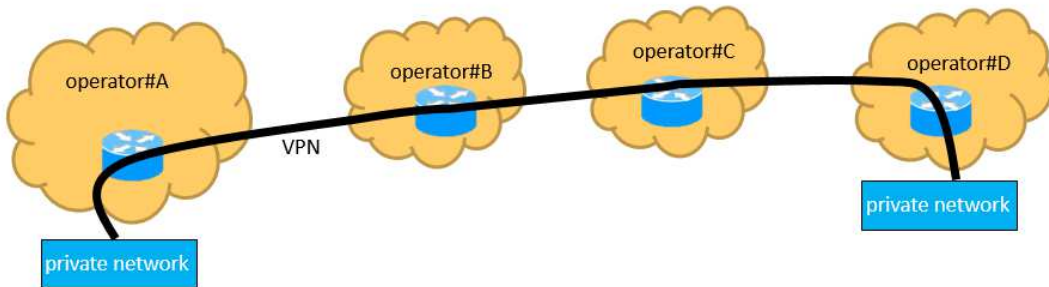


Distributed Ledger based Online Trading System for Cross-domain VPN Provision

Section 1 Summary

| Use Case Summary | | | |
|--|--|------------------------------------|--------------|
| Use Case ID: | ICT-004 | Use Case Type: | Vertical |
| Use Case Title: | Distributed Ledger based Online Trading System for Cross-domain VPN Provision | Is Use Case supporting SDGs | Yes |
| | | Domain: | Industries |
| Status of Case | Proof-of-Concept | Sub-Domain | IT and telco |
| Contact information of person submitting/ managing the use-case | <p><i>Xinpeng Wei</i> wexinpeng@huawei.com</p> <p><i>Bingyang Liu</i> liubingyang@huawei.com</p> | | |
| Proposing Organization | <i>Huawei</i> | | |
| Short Description | This use case is a proposal for utilizing DLT-based online trading system for cross-domain VPN (Virtual Private Network) provision services, which enables a custom to purchase cross-domain VPN service on-demand and flexibly. | | |
| Long description | <p>A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Usually the VPN connection will cross one or more networks operated by different operators, and the operators should have SLAs between each other to setup of end-to-end VPN connection for customers, the process of setup VPN could take a very long time both due to technology issues and SLA issues between operators, but because the VPNs are usually static provisioned and once setup it will maintained for a very long time, so the time taken for VPN setup is acceptable.</p> <p>But as the new cases that VPN should be setup in a more flexible and on-demand way, the existing solution for VPN setup is no longer acceptable, because it is usually unknown which operator's network to traverse and whether the en-route operators has SLAs between each other.</p> <p>This document provides a use case that DLT is used for on-demand VPN connection setup across different domains.</p> | | |
| SDG in Focus (when applicable) | <p>Goal 9: Industry, Innovation and Infrastructure</p> <p>9.3 Develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.</p> | | |

| | | | |
|----------------------------|--|-------------------------|-----------|
| Value Transfer: | Token which is used to pay for VPN service. | Number of Users: | thousands |
| Types of Users: | enterprise, residential customer network, network operator | | |
| Stakeholders | enterprise, residential customer network, network operator | | |
| Data: | 1. The data that VPN user sends to network operator for VPN provision. 2. The Service Level Agreement signed between different network operators. | | |
| Identification: | Full identification of each entity is required. | | |
| Predicted Outcomes: | 1. Minimize time to negotiate VPN provision process. 2. Eliminate the need of pre-sign SLAs between customer and service providers. | | |

| Overview of the Business Problem or Opportunity |
|---|
| <p>Currently in order to establish VPN connection across more than one operators' network, because the QoS of VPN connection needs to be provided along the whole connection path, so operators should have SLAs between each other and each operator makes its own provisions for the VPN connection. The process of setup VPN could take a very long time both due to technology issues and SLA issues between operators, but because the VPNs are usually static provisioned and once setup it will maintained for a very long time, so the time taken for VPN setup is acceptable.</p>  <p>Figure 1: VPN connection across different operators' network</p> <p>But for the new use case of on-demand VPN connection, the existing solution is hard to satisfy the requirements for the following reasons:</p> <ol style="list-style-type: none"> 1. The on-demand VPN is very dynamic, and it is hard to predict with network it will traverse. 2. The on-demand VPN could only exist for a short time, e.g. only a few days, so the time cost of establishing such as connection should be low enough. |
| Why Distributed Ledger Technology? |
| <p>DLT is to build a trust infrastructure, which helps the private network to set up trust relationship with the network providers for establishing VPN connection, and enables fast on-line trading between them to realize automatic VPN provision.</p> |

Section 2 Current process

Current Solutions

The current solution depends on the operators' SLA pre-signed with each other.

Existing Flow (as-is)

| Step | User Actions | System Actions |
|------|--|----------------|
| 1. | The VPN user (owner of private network) sends out a request to the operator it directly connected to establish VPN connection between private networks. | N/A |
| 2. | The network operator provision its own network devices to provide VPN connection and ask for the next network operator to provide VPN connection in its network according to SLA, and so on until the end-to-end VPN is fully provisioned. | N/A |

Process scheme (as-is)

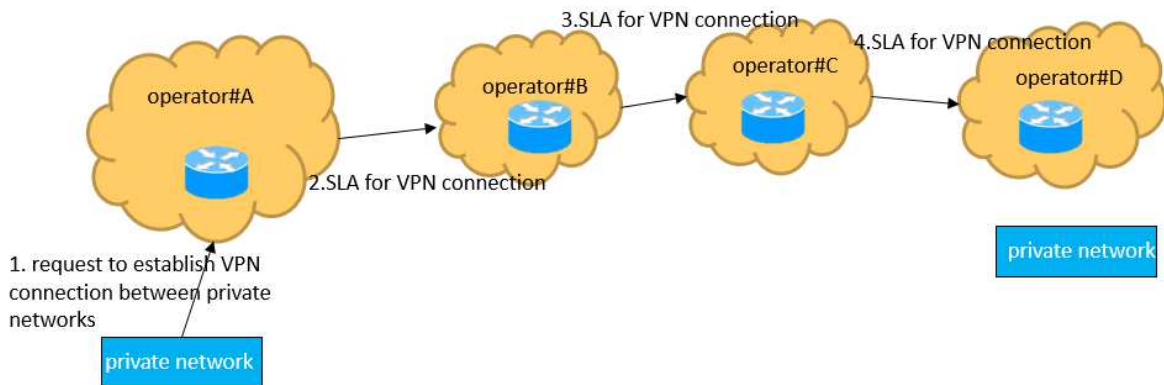


Figure 2: VPN provision procedure

Data and information (as-is)

| Data | Type | Description |
|------|-----------------------|---|
| 1 | VPN provision request | The data that VPN user sends to network operator for VPN provision. |
| 2 | SLA | The Service Level Agreement signed between different network operators. |

| Participants and their roles (as-is) | | |
|--------------------------------------|------------------|---|
| Actor | Type/Role | Description |
| 1 | VPN user | The entity who wants to establish VPN connection. |
| 2 | Network operator | The entity who operates the network. |

| Other Notes |
|-------------|
| N/A |

Section 3 Expected process

| Expected Flow (to-be) | | |
|------------------------------|---|--|
| Step | User Actions | System Actions |
| 1. | VPN user gets en-route networks' information between private networks. | Ledger records networks' information about the VPN service they can provide. |
| 2. | VPN user sends request to network operator's smart contract to establish VPN connection between private networks. The VPN configuration-related parameters will be included in the request. | Ledger checks the VPN user is authorized to send out the transaction, and the target network operator's smart contract exist. If true, DLT record the transaction. |
| 3 | Network operator gets VPN configuration-related parameters from the ledger. | Ledger provides VPN configuration-related parameters information to network operator. |
| 4 | Network operator acknowledges VPN service. | Ledger records network operator's transaction for VPN service acknowledge. |

Process scheme (to-be)

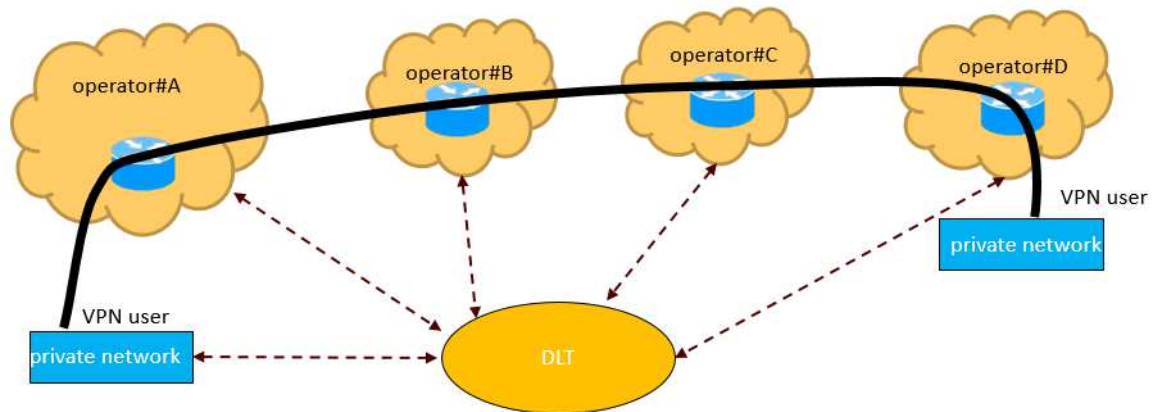


Figure 3: Overview of DLT and VPN Provision System

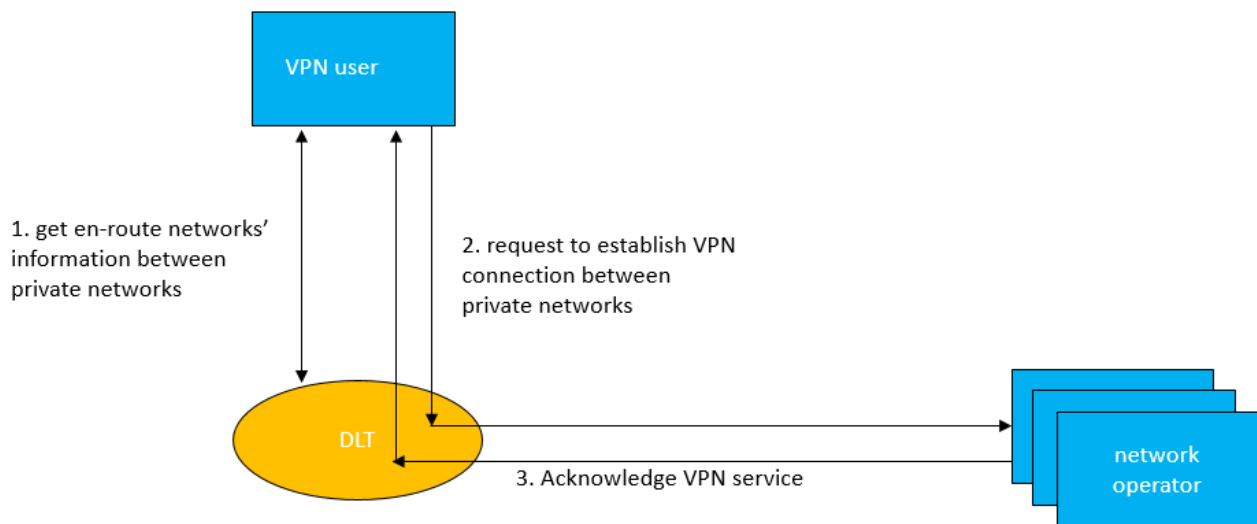


Figure 4: Procedures of VPN Provision Service

Participants and their roles

| Actor | Type/Role | Description |
|-------|------------------|---|
| 1 | VPN user | The entity who wants to establish VPN connection. |
| 2 | Network operator | The entity who operates the network. |

Data and information

| Data | Type | Description |
|------|---------------|--|
| 1 | Token account | Token representing money value. It is used to transfer value between VPN users and network operator. |

| Data and information | | |
|----------------------|--------------------------------------|---|
| Data | Type | Description |
| 2 | Service request transactions | The VPN users use service request transaction to ask for VPN provision service from network operators, and payment for the service will also be included. |
| 3 | VPN service information | The information is maintained at the smart contract in ledger, it includes the SLA that the network operator can provide for VPN provision. |
| 4 | Network-related information | Each network provides its own network information to the Ledger, this information is used by VPN users to figure out the en-route networks that the VPN connection will traverse. |
| 5 | VPN configuration-related parameters | These parameters are used to configure VPN connection properly, the VPN user decide these parameters and the Ledger will record these parameters. |
| 6 | VPN service acknowledge transaction | This transaction is used by network operator to accept the VPN provision request from VPN user. |

| Security and privacy |
|---|
| 1. The network operator's service information recorded in DLT system should be trustable. |

| Main Success Scenario |
|---|
| 1. All information exchange and payments occur in Distributed Ledger in automatic mode. 2. Payment and service are exchanged without human intervention. |

| Conditions (pre- or post-) |
|---|
| 1. The token must be created in some way. 2. All parties are connected to DLT system. 3. All parties should have a recognizable identity. |

| Performance needs |
|--|
| 1. Transactions processing near real time; 2. 24/7/365 availability; 3. Volume of transactions > 1000 TPS. |

| Legal considerations |
|----------------------|
| N/A |

| Risks |
|-------------------------------|
| 1. DLT-related security risk. |

| Special Requirements |
|-----------------------------|
| N/A |

| External References and Miscellaneous |
|--|
| N/A |

| Other Notes |
|--------------------|
| N/A |

Appendix 1

Domains and subdomains for use cases categorization

Vertical:

1. Finance
 - a. Financial management & accounting
 - b. International & interbank payments
 - c. Clearing and settlement
 - d. Reduction of Fraud
 - e. Financial messaging
 - f. Asset lifecycles and history
 - g. Trade finance
 - h. Regulatory compliance & audit
 - i. AML/KYC
 - j. Insurance
 - k. Peer-to-peer transactions
2. Healthcare
 - a. Pharma
 - b. Biotechnology
 - c. Medicine
3. Industries
 - a. Manufacturing
 - b. Energy
 - c. Chemical
 - d. Retail
 - e. Real estate
 - f. IT and telco
 - g. Supply chain management
 - h. Transportation
 - i. Agriculture
4. Government and public sector
 - a. Taxes
 - b. Government and non-profit transparency
 - c. Legislation, compliance & regulatory oversight
 - d. Voting
 - e. Taxation and customs
 - f. Intellectual property management
 - g. Land Registries

Horizontal:

1. Identity Management
2. Security Management
 - a. Public Key Infrastructure

3. Internet of Things
4. Data processing, storage and management
 - a. Data Validation (includes provenance)