PDL ISG - PoC Proposal Template

1 PoC Project Details

1.1 PoC Project

PoC Number (assigned by ETSI)

PoC Project Name: **Decentralized Internet Infrastructure (DII)**

PoC Project Host: Universitat Politècnica de Catalunya (UPC)

Short Description: **Autonomous domains over the Internet have a number of security issues: prefix hijack, path hijack & route leak.** We use decentralized Distributed Leger Technology to prevent the information from being falsely manipulated by compromised entities. It will demonstrate how to make Internet infrastructures more secure and robust, create innovative decentralized ecosystems and how they would operate in coordination with the ledgers.

1.2 PoC Team Members

Table: 1-1

	Organization name	ISG PDL participant (yes/no)	Contact (Email)	PoC Point of Contact (see note 1)	Role (see note 2)	PoC Components
1	Universitat Politècnica de Catalunya (UPC)	Yes	acabello@ac.upc.edu	Albert Cabellos	Research Institute	Demo Space and presentation, Ideas & solutions
2	Telefonica	Yes	diego.r.lopez@telefonica.com	Diego Lopez	Service Provider & Operator	Demo Support
3	Huawei UK	Yes	liubingyang@huawei.com	Liubingyang (Bryan)	Manufacture	Equipment
4	UC3M	No	marcelo@it.uc3m.es	marcelo bagnulo braun	Research Institute	Demo Support

NOTE 1: Identify the PoC Point of Contact with an X.
NOTE 2: The Role will be network operator/service provider, infrastructure provider, application provider or other as given in the Definitions of ETSI Classes of membership.

All the PoC Team members listed above declare that the information in this proposal is conformant to their plans at this date and commit to inform ETSI timely in case of changes in the PoC Team, scope or timeline.

1.3 PoC Project Scope

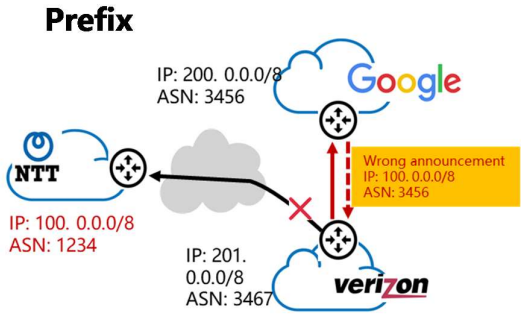
1.3.1 PoC Goals

DII (**Decentralized Internet Infrastructure)** for BGP Security: DII can not only prevent prefix hijacking, but also path hijacking and route leakage to build a complete BGP route security service. The three goals are to use DTL technology to address the three problems, illustrated below.

First goal, **Prefix Hijack**: Google (as an example of an OTT service provider) has announced an IP prefix that belongs to NTT As an example of an Operator) to Verizon (as an example of a second operator). The traffic from Verizon (operator 2) to NTT (Operator 1) is sent to Google (the OTT service provider), causing a large-scale network disconnection in Japan (as a remote country) for one hour [1].

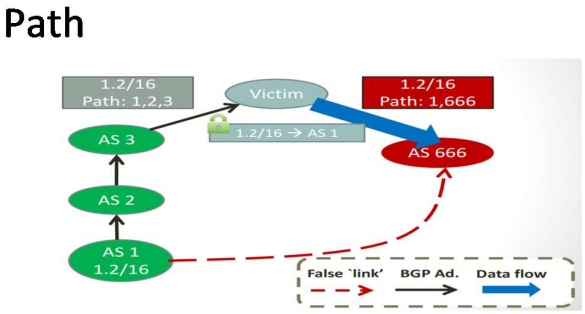
- DII maintains trusted **IP prefix ownership** info and **mapping info between the IP prefix and ASN** (Autonomous System Number), called ROA (Route Origin Authorization) info.
- Only the owner of IP Prefix (e.g.: NTT) can create such ROA info (10.0.0.0/8, AS1234).
- Based on the ROA info, For example: Verizon can prevent the hijacked route from Google.

Note: The company names are examples only. There is no suggestion of known problems in their networks.



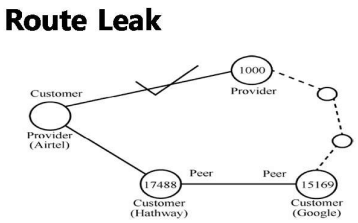
Second goal, **Path Hijack**: AS 666 (Autonomous System) announced false information, claiming that it has only one hop with AS 1. As a result, all traffic destined for AS 1 is hijacked to AS 666[2].

- DII maintains trusted **ASN ownership** info and **mapping info between the ASs**, called AS neighbor info.
- AS 666 cannot forge non-existent AS neighbor info.
- Based on this info, victim can prevent the Path hijacked route from AS 666.



Third goal, **Route Leak**: Hathway leaks the route learned from the peer provider (e.g.: Google) to the second provider (e.g.: Airtel). As a result, the route from the second provider (e.g.: Airtel) to the first provider (e.g.: Google) bypasses Hathway carrier, causing congestion [3].

- DII maintains trusted **ASN ownership** info and **trusted business relationships** between ASs .
- This info enables Airtel to filter out the advertisement of the Hathway because of route leakage.



EXAMPLE: ETSI GS PDL 005 extract of Table 1 in Clause 4.4 below.

Table: 1-2: Main Areas of CDPR & PDL Applications

HORIZONTAL DOMAIN	VERTICAL DOMAIN
Infrastructure Management	ICT: Internet resource management, Trust infrastructure (e.g. PKI), Network security

1.3.2 PoC Topics

PoC Topics identified in this clause need to be taken for the PoC Topic List identified by ISG PDL and publicly available, i.e. the three topics identified in clause 4.5 of the PDL PoC Framework. PoC Teams addressing these topics commit to submit the expected contributions in a timely manner.

Table: 2

PoC Topic Description	Related WI	Expected Contribution	Target Date
The PoC uses Smart contracts to enable the hyperlogic	PDL-004 Smart contracts	Review of requirements and validation	01.08.2020
The PoC uses many sites distributed over the globe	PDL-006 Interconnection	Review of the interworking	01.11.2020

1.3.3 Other topics in scope

List here any additional topic for which the PoC plans to provide input/feedback to the ISG PDL.

Table: 3

PoC Topic Description	Related WI	Expected Contribution	Target Date
Demonstration of Hyperledger fabric	PDL 001	unknown	
Demonstration of BGP	PDL-006	Interconnection proof of requirements	01.11.2020
Smart contract use	PDL-004	Smart contracts use and validation	01.08.2020
Interconnection of Ledgers	PDL-006	Security and use of BGP in the Interconnection of Ledgers	01.09.2020

1.4 PoC Project Stages/Milestones

Table: 4

PoC Milestone	Stages/Milestone description	Target Date	Additional Info
P.S	PoC Project Start	01.07.2020	
P.D1	PoC Demo 1	01.08.2020	ETSI Bright talk presentation
P.D2	PoC Demo 2	01.10.2020	Layer 123 demo(s) 1) Currently their website (https://events.layer123.com/sdn/agenda-live-1747TP-7409L4.html) they keep the 12-15 October 2020 dates. ETSI (Marion or David) knows how to co-ordinate 2) The project would seek to organize a webinar event. Event producers like Layer123 are eager for this kind of virtual events due to the impact of the pandemics on their business and visibility.
P.D3	PoC Demo 3	10-13.05.2021	IEEE INFOCOM (10-13 May 2021, Vancouver) (See Note 1 below)
P.D4	PoC Demo 4	7-11.12.2020	Demo proposal at IEEE GLOBECOM 2020 (deadline for the demo July 1st, notification of acceptance July 15th). Demo to be organized 7-11 Dec in Taipei, Taiwan. More information about the venue here: https://globecom2020.ieee-globecom.org (See Note 1 & 2 below)
P.C1	PoC Expected Contribution 1	01.08.2020	Smart contracts use and validation
P.C2	PoC Expected Contribution 2	01.09.2020	Interconnection of Ledgers
P.C3	PoC Expected Contribution 3	01.11.2020	Interconnection proof of requirements
…	…		
P.R	PoC Report	01.01.2021	
P.E	PoC Project End	01.02.2021	

NOTE 1: Given the current situation with the pandemic international conferences face a significant degree of uncertainty both in the dates and in the organization itself (virtual vs. physical). We will adapt this plan according to the upcoming events.

NOTE 2: The details are under consideration.

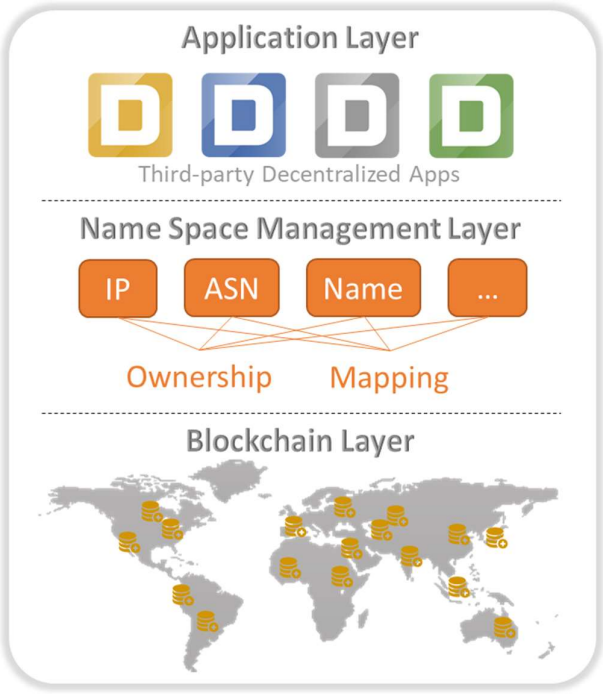
1.5 Additional Details

We will report the outcome of the demo in an academic paper submitted to a top IEEE ComSoc open-access journal with high impact factor. A potential candidate for this is *IEEE Access*.

2 PoC Technical Details

2.1 PoC Overview

DII uses decentralized blockchain to prevent the information from falsely manipulating by compromised entities. It will make Internet infrastructures more secure and robust, and create innovative decentralized ecosystems [4].



3rd-party trusted Apps

- Decentralized PKI
- Near-source DDoS mitigation

Trusted name spaces

- IP→ ASN: trusted BGP routing
- Name → IP: **trusted DNS**

Global Block-chain infrastructure

The PoC will demonstrate the following requirements.

Requirement of DII	Descriptions	Related Feature of PDL
Permissioned control	The participants of DII needed to be authorized.	**Access Control**
Resistance to Single point failure	The resource management in DII doesn't depend on single authority.	**Decentralized consensus protocol** Peer-to-peer trust model. Agreement is made by a decentralized consensus protocol, run by all peers.
	The creation of records in DII should be trustable.	
	The records are tamper-resistant.	**Decentralized data management** Data is maintained by all peer nodes. All data operations are transparent, and data availability is much higher.
Trustable autonomous procedure	Autonomous procedure can avoid the configuration errors and misbehavior.	**Smart contract**

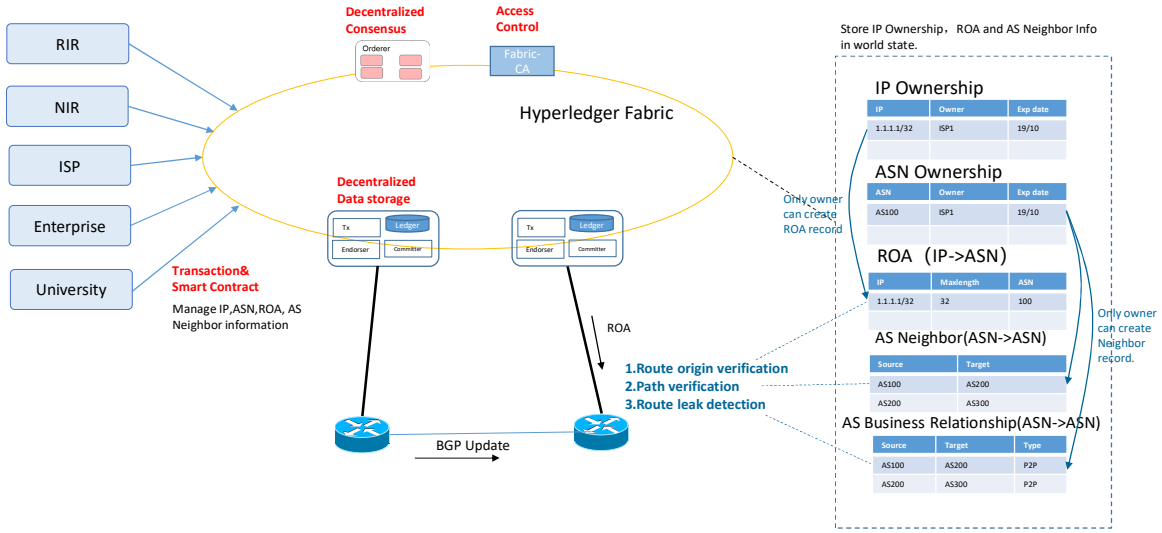
		A Turing-complete computation model to support any decentralized application.
Trustable Transaction Capability	Trustable transaction capability is important to Internet resource.	**Transaction** Peer nodes can send transactions between each other, enabling service monetization with inherent trust.

2.2 PoC Architecture

Include a schema outlining how the different PoC components fit in the PoC architecture.

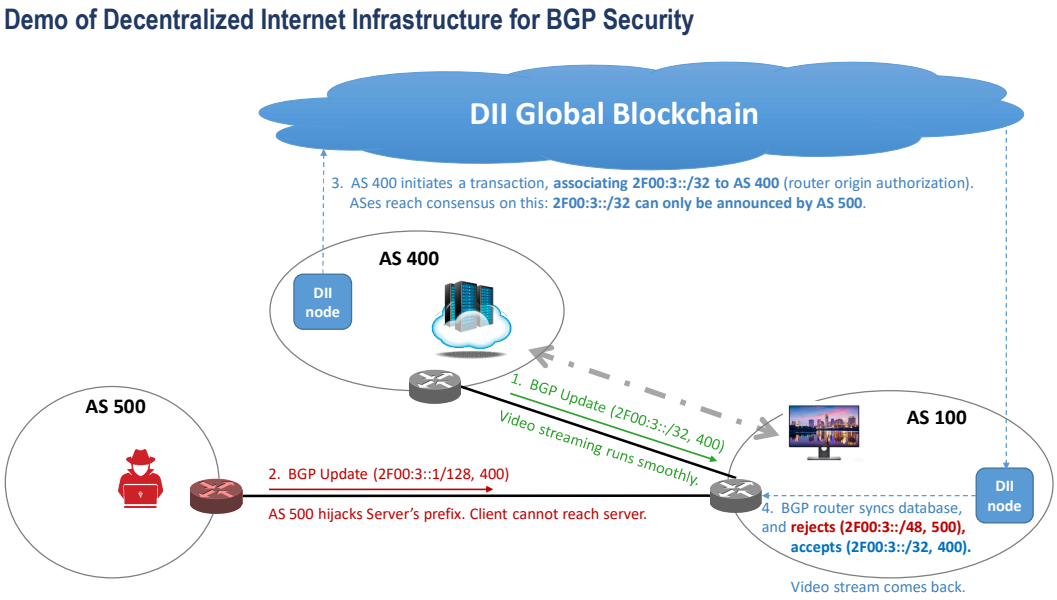
DII based on Permissioned Distributed Ledger. The General DLT Architecture using Hyperledger fabric shown in Figure 1 below uses secure address tables and BGP to secure the IP ASN Prefix, the Path & the Route taken over routers to avoid BGP attacks. Especially when routed globally.

Figure 1: General Hyperledger architecture



The Figure 2 Below shows how a Hacker attempts a Path & Address hijack and the DTL infrastructure is self-healing and uses the Smart contract to correct and re-establish the address and the path.

Figure 2: Demonstration of a Prefix Hijack attack and corrective self–healing behaviour



2.3 PoC Success Criteria

The DII PoC success is measured by showing that BGP on Hyper-ledger Fabric can mitigate and automatically heal situations where prefix hijacking, path hijacking and route leakage are a likely risk to networks and the services delivered. To build a service with security. There is a need to demonstrate:

- **Access Control**;
- **Decentralized consensus protocol**, Peer-to-peer trust model, where agreement is made by a decentralized consensus protocol, and run by all peers;
- **Decentralized data management**, where data is maintained by all peer nodes, all data operations are transparent, and data availability is much higher;
- **Smart contract**, a Turing-complete computation model to support any decentralized application and
- **Transaction control**, peer nodes can send transactions between each other, enabling service monetization with inherent trust.

2.4 Additional information

Include additional information as useful.

References:

[1] https://www.thedrum.com/news/2017/08/28/google-hijack-made-japan-land-no-internet-more-30-minutes

[2] https://datatracker.ietf.org/meeting/98/materials/slides-98-rtgarea-jumpstarting-bgp-security-with-path-end-validation-00

[3] http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjHkdqIrY_qAhXo-GEKHYleBq04ChAWMAJ6BAgFEAE&url=http%3A%2F%2Fwww.infocomm-journal.com%2Fcjnis%2FCN%2Farticle%2FdownloadArticleFile.do%3FattachType%3DPDF%26id%3D160313&usg=AOvVaw0j_1MmF7mUYqxr2xYOsw_-

[4] T17-SG13-190304-TD-WP3-0224!!MSW-E, ITU-T SG-13 Q2 WI-DNI