Digital Identity as a Service

Section 1 Summary

Use Case Summary			
Use Case ID:	IDM-002	**Use Case Type:**	Horizontal
Submission Date:	October 11, 2018	**Is Use Case supporting SDGs**	No
Use Case Title:	Digital Identity as a service	**Domain:**	Cybersecurity
Status of Case	PoC	**Sub-Domain**	Mobile roaming Digital Services
Contact information of person submitting/ managing the use-case	Full Name: Alexander Yakovenko Job Title: Project Director E-mail address: ayakovenko@clementvale.com Telephone number: +7-985-991-2048 Social media: https://www.linkedin.com/in/alexander-yakovenko Web site: https://www.blockchaintele.com		
Proposing Organization	Clementvale Baltic OU, Estonia		
Short Description	This use case is a proposal to implement Digital identity with the use of DLT and use it as a service		
Long description	This use case is a proposal to implement Digital identity with the use of DLT and use it as a service		
SDG in Focus (when applicable)			
Value Transfer:		Number of Users:	100+
Types of Users:	Private users who need to supply personal data to get services, service providers.		
Stakeholders	Any service provider identifying their customers. Mobile operators validating their customers.		
Data:	Hashes of validated personal data		
Identification:	Mobile operator verifies personal data by request of their customer and publishes its hash in blockchain		
Predicted Outcomes:	Decentralized approach, which allows exchanging of personal data, compliant with "General Data Protection Regulation" (GDPR)		

Overview of the Business Problem or Opportunity

It is critical for mobile operators and mobile service providers to know with whom they are interacting. Growing IoT market and IoT services make this problem even more prominent. Traditionally a person who needs to identify himself must visit office of organization and present his passport and other documents. For private person this is inconvenient and time-consuming procedure. For organizations this is significant item of expenditure.

Usually mobile operators possess all information necessary to identify their customers. They can use blockchain to effectively assist customers to identify themselves to other participants by supplying identity verification services. The approach is developed to be fully compatible with "General Data Protection Regulation". ***No actual transfer of personal information is expected between organizations.***

Why Distributed Ledger Technology?

Distributed Ledger is an optimal solution for this use case because:

- *Verification of identity information (without disclosing identity information itself) can be shared across all participants of decentralized platform.*
- *Different mobile operators as well as other authorized organizations can provide digital identity services in similar standardized way.*
- *Identity services are immediately available to multiple service providers and consumers through the same Distributed Ledger platform for telecom.*

Section 2 Current process

Current Solutions
Currently private users need to visit office of organization with identity documents, such as passport, driving license, social security, etc. *Each organization providing online identification for their customers have to re-implement corresponded software platform and take care about fraud data.*

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.		

Process scheme (as-is)

Data and information (as-is)		
Data	**Type**	**Description**
1		

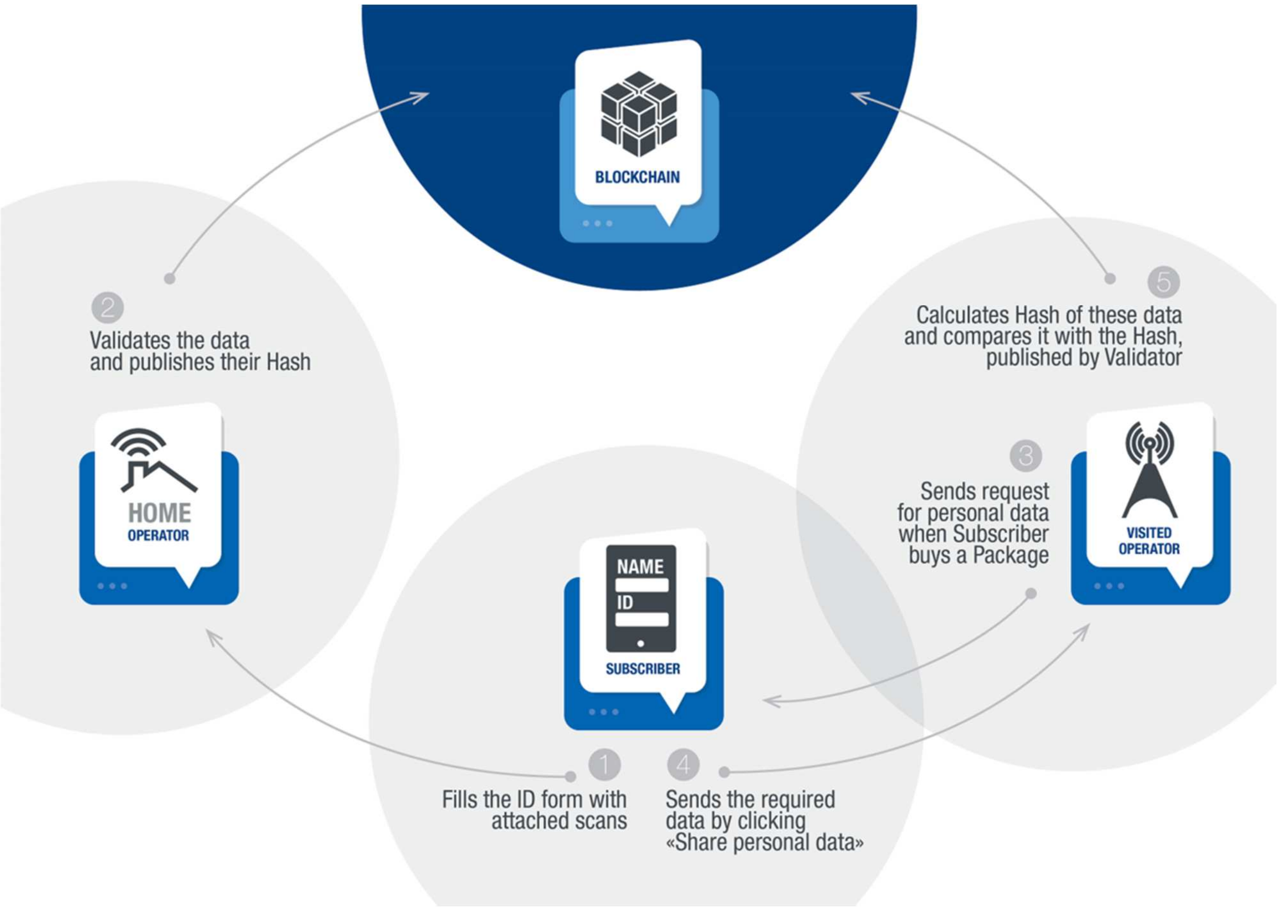
Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1		

Other Notes

Section 3 Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Subscriber: Fills the ID form, attaches scans of passport and other documents, stores the ID file in his smartphone	n/a
2.	Subscriber: Sends the ID file to his home operator.	n/a
3.	Home operator: Verifies the data in ID file, calculates the hash of the data and sends hash to DLT system in signed transaction.	n/a
4.		Verifies digital signatures of transaction and makes hash of ID file available to all participants.
5.	Subscriber: On request to identify himself from visited operator or service provider, sends ID file prepared on step (1.)	n/a
6.	Visited operator: Calculates hash of ID file and requests DLT system for the validity of the hash	n/a
7.		Looks up hashes available and, if found, returns validity status of ID file along with validating organization details.

Process scheme (to-be)


BLOCKCHAIN
2
Validates the data and publishes their Hash
HOME OPERATOR
5
Calculates Hash of these data and compares it with the Hash, published by Validator
3
Sends request for personal data when Subscriber buys a Package
VISITED OPERATOR
NAME
ID
SUBSCRIBER
1
Fills the ID form with attached scans
4
Sends the required data by clicking «Share personal data»

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Subscriber*	Subscriber of mobile service, who needs to identify himself.
2	*Home operator*	Mobile operator hosting Subscriber in his native country (or other authorized organization), which can identify Subscriber and verify identity information.
3	*Visited operator*	Another mobile operator (for example, foreign operator in visited country) or service provider which need to get identity information from a customer to supply services.

Data and information		
Data	**Type**	**Description**
1	*Documents*	Scans of passport and any other documents which customer may be requested to present. It is essential that organizations never share those data with each other. Instead, they request customer to supply data to get some services and use DLT system to verify supplied data.

Data and information		
Data	**Type**	**Description**
2.	*ID file*	A collection of documents stored in a special file at customer's smartphone.
3.	*Hash*	Digital hash of ID file transmitted via blockchain by home operator to make identification status available to other participants.

Security and privacy
1. Identity status (hash of ID file) is protected by digital signature of home operator within corresponded transaction within DLT system
2. No private data are stored in the DLT system.
3. No any personal data is transmitted from home operator to another operators or service providers
4. Hashes can be transmitted without any linkage to the person, so no one could actually use shared hashes unless the person explicitly decide to disclose his data to some participants.

Main Success Scenario
DLT-based global market place where different mobile operators and other participants (telecom and non-telecom service providers, content providers, software vendors, etc) can supply their services to customers of other operators all over the world. Digital identity is an essential and integrated part of this solution.

Conditions (pre- or post-)
n/a

Performance needs
Although not strictly required, fast transactions (within a few seconds) are desirable to distribute identity status among participants.

Legal considerations
Solution is assumed to be compliant with "General Data Protection Regulation" because participants never share personal data with each other. They use DLT system only for validation of personal data supplied by customer.

Risks
n/a

Special Requirements

1. Participants must agree about format of ID file

2. Users must be supplied corresponded software to prepare ID files

3. Hashing algorithm must be agreed or recorded in the ID file

External References and Miscellaneous

https://blockchaintele.com

https://wiki.blockchaintele.com/index.php/Main_Page

https://wiki.blockchaintele.com/index.php/Use_cases#New_revenue_stream_on_.22Identity-as-a-Service.22

Other Notes

____