

EEMA INTELLIGENCE

# WILL *DISTRIBUTED IDENTITY* EVER BE INTELLIGIBLE TO THE AVERAGE CITIZEN?

www.eema.org

Issue 1 of a series to be published

*05.02.2021*

# SURVEY QUESTION:
# ''WILL *DISTRIBUTED IDENTITY* EVER BE INTELLIGIBLE TO THE AVERAGE CITIZEN?''




**Overall Respondents**




**Additional Comments**




**No. of Countries Reached**

**ANSWERS:**

a. **It's too complicated and will not succeed.**
b. **It needs to be invisible to the average person.**
c. **It is easy to understand with some public education.**

## 1. ANALYSIS OF THE SURVEY

In the very first edition of the 'EEMA Intelligence' we are proud to state that ninety-two people have participated in the intelligence gathering project within our network of international experts.

As a start we have chosen a question related to 'Identity'. Our audience is educated to an expert level standard and we have decided to give more voice to their opinion.

The first survey question shows that twenty-five percent of the respondents have answered that distributed identity is a concept that is 'too complicated and will not succeed' when it comes to general understanding.

Followed by the second group of people which has selected that it will be 'easy to understand with some public education'. Almost thirty two percent believe that this is the key to make 'Distributed Identity' intelligible to the average citizen.

However, we must admit that the gap between the chosen answer options is respectively six and eleven counts.

On the other hand, the majority of the people who participated in our survey chose that this is a concept which 'needs to be invisible to the average person'. This answer solidifies its number one position by being chosen forty times.

As a result, our network of experts has expressed that 'Distributed Identity' must be invisible to the general public.

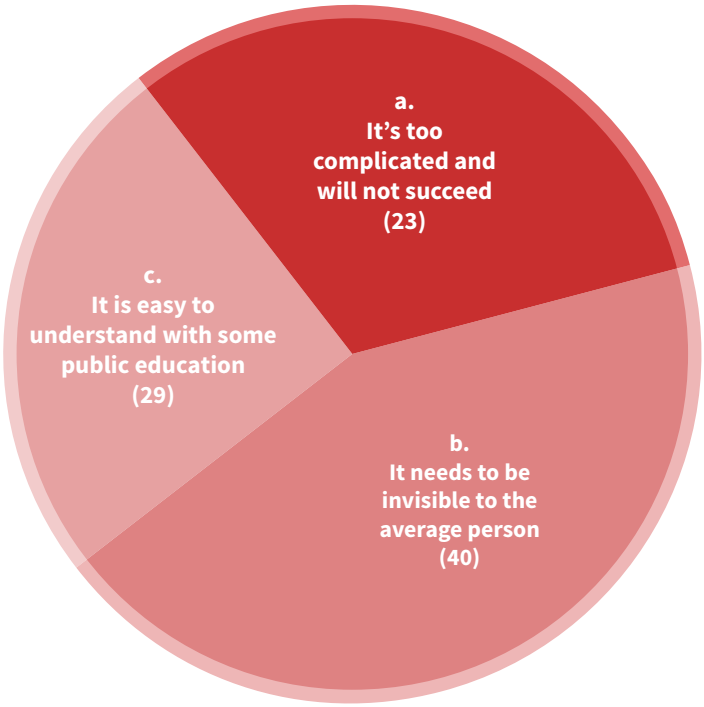



**Fig. 1 Responses to 'Distributed Identity' Survey**

# CONTRIBUTORS



**Jon Shamah** is the Chair of **EEMA**, specialising in maximising the operational value chain programmes. In 2017 Jon was listed in the One World Top 100 Leaders in Identity.



**John Erik Setsaas**, VP of Identity and Innovation at Signicat. He is responsible for ensuring digital identity services are at the forefront of innovation, whilst solving the needs of customers, partners and end users.



**Marc Sel**, Founder and director of Trust Warp. Formerly Director of Advisory Services at PwC, specialising in eIDAS Trust Services regulations and implementation.



**Arkadiy Kremer**, RANS Russia. He has extensive practical experience with many years of managing projects in information and telecommunication technologies.

## 2. COMMENT FROM JON SHAMAH

''Distributed Identity is the new buzz-phrase for the identity industry. Distributed Identity, or variants, are not for the faint-hearted typical consumer, and realistically may be too complicated to explain to them. We should not be surprised. How many people know how a cell phone works? How many people know why it is even called a "Cell Phone"? Nor do they care. Yet the cell phone demonstrates how a truly complex (and expensive) piece of technology can be successfully adopted at global scale. And... Identity is even a more personal issue.

Any technology must cross the chasm to the consumer domain, and quite often the success of new technology does not depend on the quality of the technology alone. The list is failures to be successful is endless, and those of success few. All must demonstrate an ease of use that is almost inconceivable at the beginning of the technology's journey.

The key for distributed identity is to offer functionality that can require no additional effort (or thought) by the consumer. Therefore, an almost plug-and-play changeover must be offered. Not easy if the paradigm is so different, and Distributed Identity is indeed different.

In my opinion that are lots of new technologies that, in the rush to market and to show a Return-On-Investment (ROI) a key component may have been neglected. This component is the Transition Path from what is the currently accepted status of technology/usage/policy etc to the new methodology.

I cannot recall any presentations at conferences ever, that have addressed the issue. Again, are we surprised? New technology is conceived by technologists. Start-ups are usually driven by ROI and quarterly results. There are few demand-driven new enterprises. There is just a lack of holistic planning. The downside is that revolutionary ideas will have a bigger barrier to overcome.

The classic case of Satellite TV comes to mind where the specification was determined: "No more complicated to buy than a video recorder," and "the same price." "No more than €100 to install," "invulnerable to cheating" and providing an ongoing affordable revenue stream." Not a lot of technology described there.
"Impossible," became
"possible," became "achieved," driven by deep pockets and economies of scale. Suddenly a large segment of the population had cheap TV beamed from 70,000 km away! (via geostationary satellite). Satellite TV, like mobile phones is now commodity.

**SO HOW DO WE ACHIEVE THIS?**
It should be taught in both business schools and more importantly on technology courses at all levels, that "Whilst Adoption is King, Transition is the King-Maker"

## 3. COMMENT FROM JOHN ERIK SETSAAS

''One of the major challenges we are facing with digital identity, is how to bind the physical user to the user's digital counterpart, which I will call the avatar.
There are two situations where this binding is important: when establishing the avatar and whenever using it. The establishment of the avatar is done only once (possibly with re-validation some years later), and we can accept a process where we scan identity papers or other means such as a video call identity verification. But when using the avatar on a regular basis for accessing various services, this must be simple.

The main access to the avatar is knowledge-based (“please create a unique password with upper- and lower-case letters, numbers and special symbols”), possibly with some second factor (which increases security, but the usability suffers). In some cases, biometrics are being used, but still passwords will be used when the biometrics fail, so this is still in the end knowledge-based.
Most people will (either by choice or by accident) share their passwords, as well as forget them. So even though we trust the binding of the avatar to the user, do we know who is controlling the avatar right now?

Neither centralized nor distributed identity has solved this issue. Most distributed solutions I have seen are even worse, because the users are told to take good care of the private key, with no means of recovery when if you lose it. A quick look to Twitter and all the people who have lost their Bitcoin proves that this is not a viable solution.

That said, distributed identity is the way forward. I, the user, must be able to provide other parties with selected information about myself in a way that the receiver can trust, and this should work also in a face-to-face scenario.

A very relevant example is proving that I am COVID-19 negative or have received the vaccine. The current “vaccine passports” are paper-based, and you can buy forgeries online for 10 EUR, if you don’t want to Photoshop one yourself. Distributed identity is still in its infancy. And the solutions are way too technical, even for identity nerds. There must be more focus on the users, recognizing that most people do not understand (or care) about digital identity.

In the village, everybody knows who I am, without me having to do anything. I think this is implanted in our brains, so why do I constantly have to tell those I meet who I am.
The end goal should be that people and organizations recognize me, without any effort on my side.''

## 4. COMMENT FROM MARC SEL

''The different interpretations of 'distributed identity' share that they refer to an identity that is not based on centralized elements. For natural persons this is contrary to most if not all government-issued identities, which rely on an official assessment followed by an assertion that binds a physical person to a unique identifier. This identifier can be a unique string such as a national register number, or the combination of a set of attributes that is considered to be sufficiently unique.

Distributed identity promises new solutions to challenges of centralized identity systems. This includes privacy and self-sovereignity. Solutions based on centralized identity struggle to effectively protect their users against the linkability that is the consequence of using a unique identifier. Some countries resorted to legislation that forbids using the identifier unless it is explicitly permitted.

Nevertheless, as legal enforcement is less than perfect it did not stop e.g.. some banks in the past to use the identifier in their data mining for commercial purposes. Other countries such as Austria and recently The Netherlands use a system of sector-specific (or more granular) identifiers based on cryptographic transformation.

Distributed identity solutions such as those from the Decentralised Identity Foundation (DIF) are working towards including privacy-preserving authentication and transfer of certified attributes. Such techniques have been integrated into the Hyperledger Fabric blockchain and the self-sovereign Sovrin network. They are also making their way in Tim Berners-Lee's 'Solid' project, which allows people to keep control over their attributes. The protocols that make of these possible are however not for the faint-hearted.

Therefore, it seems uncertain when, if ever, a general population will understand the impact of centralized as well as distributed identity systems on privacy and Self-Sovereignity.
One can but hope that some 'distributed identity' solutions will proof their value in practice, while respecting the law including the protection of its users privacy. After all, many people are capable of driving a car without understanding the details of its inner working.''

## 5. COMMENT FROM ARKADIY KREMER

''Distributed identity technologies will play an important role in ensuring the compatibility of identity domains, strengthening confidence and security in the use of information resources located in different national jurisdictions.

National laws and regulations must be complimented with standards which regulate technical, procedural, and organizational details. Cyberspace does not recognize national boundaries. Therefore, security needs international standards. The development of standards in an open forum that comprises international experts from a wide variety of environments and backgrounds provides the best possible opportunity to ensure relevant, complete, and effective standards.
Going forward, we really need to know which standards are being used (and which are not being used), how widely they are used, and how effective they are. The number of standards produced is irrelevant: what is important is the impact they have.
The sufficient level of standardization is essential for successful implementation of any new technology. It is reasonable to recognize an appropriate international standards development organization (SDO), which should be targeted as a basic in the area.

Based on my personal experience of the ITU-T SG 17 (Security) chairmanship, I would suggest looking carefully at this international group of experts as the basic body for development standards on distributed identity technologies.  It’s important that this international group of experts discussed and adopted the first Recommendation on IdM terms and definitions which is widely recognized and used.''

A Joint Coordination Activity for Identity Management (JCA-IdM) has been operational by the ITU-T SG 17 since 2007. The purpose of the JCA IdM is to coordinate the IdM work within ITU-T and with external organizations. The JCA has established an IdM information resource web page that identifies identity management-related documents of ITU-T and other SDOs classified by categories, organizations, and the status of their work.
IdM within the ITU-T SG 17 is studying as a complex technology which includes:

- establishing, modifying, suspending, archiving and terminating identity information.
- recognizing partial identities that represent entities in a specific context or role.
- establishing and assessing trust between entities; and
- locating an entity's identity information (e.g., via an authoritative identity provider that is legally responsible for maintaining identifiers, credentials, and some or all of the entity's attributes).

EEMA may play an important role in integrating and providing technical contributions for development of relevant standards on distributed identity.

## 3. ADDITIONAL COMMENTS SUBMITTED BY THE RESPONDENTS OF THE SURVEY.

''The registration for the service needs to be able to accommodate a wide diversity of users from the person who has a basic account because he must the advanced user who wants to register credentialing services he requires (educational institutions, banks, government departments etc.).

Will it ever be delivered?

I believe that it is quite complicated and difficult for the average person to understand. There are too many areas regarding privacy that are incomprehensible to the average person. The majority do not even understand the European Data Protection laws!

It needs packaging like 1password and as such will become standard.

More choices please. It is a complicated concept.

Perhaps the scope of the word identity is too broad to get a consistent response.

Distributed identity is not really settled term. What does it mean that an identity is distributed? Does it mean there are independent identifiers & cryptography for independent services? Does it mean there is blockchain involved? In what sense is it distributed? Is it from the perspective of trust, data distribution or cryptography used for authentication? Until there is a clear definition it is hard promote distributed identity.

“Zero-friction” flows are needed for most end-users. *However,* it needs to be clear for the rest of the IT industry. Privacy and security issues seem to be challenging still.

Some people can be overwhelmed by the concept of data at different (and often unknown) locations. The mechanics of the ‘Web’ are irrelevant to most folk, i.e., you do not need a detailed knowledge of how an engine works to drive a car.

Invisibility does not imply lack of transparency with the system architecture, what the privacy concerns are, and ultimately who has access to the transaction stores/ ledgers (regardless of the level or depth of information recorded on the ledger).

All current solutions are FAR too complicated and require individuals to take extra actions over and above those needed today.

Invisibility does not imply lack of transparency with the system architecture, what the privacy concerns are, and ultimately who has access to the transaction stores/ ledgers (regardless of the level or depth of information recorded on the ledger).

All current solutions are FAR too complicated and require individuals to take extra actions over and above those needed today

An average citizen has no clue about ‘identity’, and you cannot teach it, so it has to be invisible.

I would tend to use the phrase “awareness building” rather than “education”... more relevant esp. when covering issues such as liability.

All new things and concepts seem at first sight impossible or very difficult...''

*Views expressed disclaimer. Please be aware that the views, thoughts, and opinions expressed in the text belong solely to the authors, and not necessarily to the author's employer, organization, committee or other group or individual. They are not necessarily the views of EEMA.