DIGID Innovative Procurement - Summary

February 2020

Overview:

The “Dignified Identities in Cash [assistance] - a Route to Scale” project (DIGID) is led by a consortium of four organizations: Norwegian Red Cross, Norwegian Refugee Council, Norwegian Church Aid, and Save the Children Norway. They have come together to address the challenge faced by lack of recognized ID’s, which is a problem both for recipients of humanitarian aid as well as for humanitarian organizations.

The DIGID project leveraged an innovative procurement process following the guidelines of the Norwegian Government. This process stressed the importance of gathering learnings through broad multi-stakeholder consultations to find new solutions that may already exist in the market. In particular, the DIGID project employed the following innovative procurement process activities: Needs Assessment and Market Dialogue.

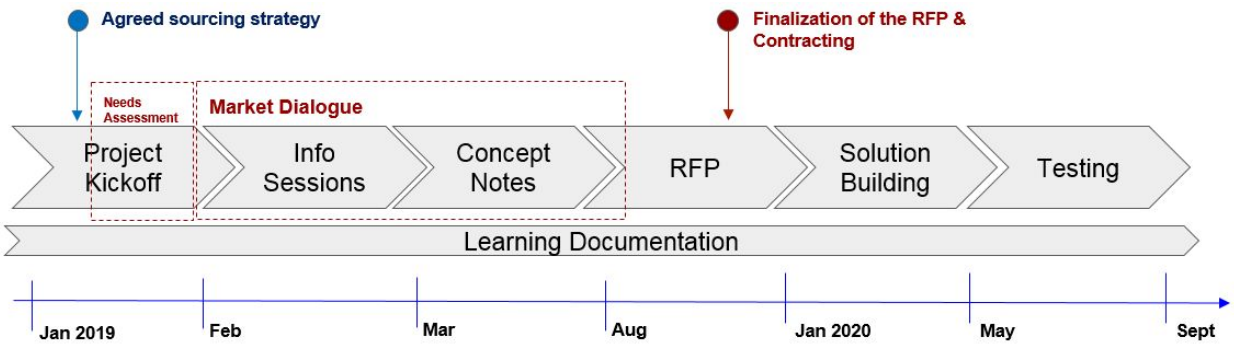

Figure 1: High-level timeline for the project indicating the innovative procurement activities.

Needs Assessment:

The consortium consisting of four humanitarian organizations was committed to the same goal, however they are still bound by their individual organization’s processes, needs, and priorities. The needs assessment was done immediately after the project kickoff in January 2019. In order to facilitate solving common--if not the same--needs, each organization developed their own *user personas* and *user journeys*. This helped map the various stakeholders in a cash

assistance programme and helped understand the motivations, challenges, and needs of the affected population. The consortium compared the user personas and user journeys to identify the common elements across the different organizations. This process then helped develop the problem statements that the project will focus on.

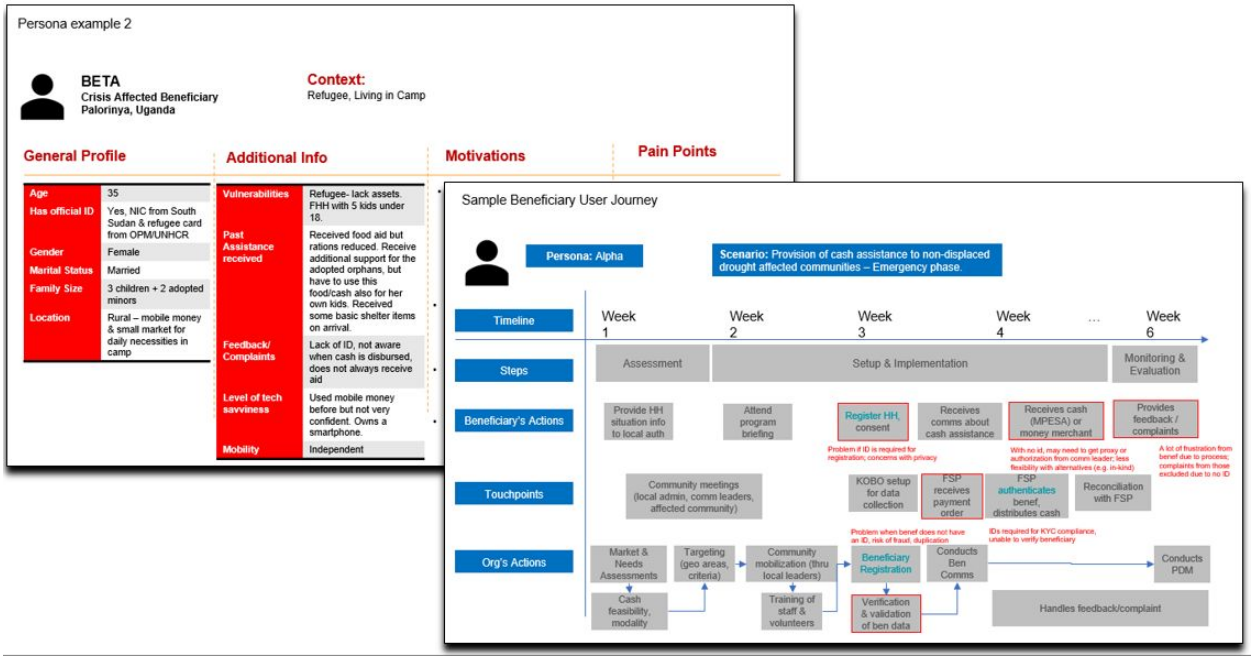

Figure 2: Sample User Persona and User Journey

Market Dialogue:

The Market Dialogue was critical in learning about the concepts around digital ID, the technologies being developed, and actors interested in solving the same problem. The DIGID project conducted the following activities through an open market dialogue to maximize the learning and get insight into the types of solutions that may exist: Information Sessions, Concept Notes Review, and Digital ID workshop in Kenya. Furthermore, a research was also done by Engineering for Change commissioned by the DIGID team to explore the concept of digital ID in cash assistance in East Africa.

I. Information Sessions (February - March 2019)

The objectives of conducting the public information sessions for the DIGID project were: (1) check if the problem statements and use cases developed were clear and if they resonated as a

shared need in the wider humanitarian sector, and (2) identify and engage with the actors interested in solving the same problem.

The DIGID team organized three online sessions and one in-person session in New York city. Over 90 signed up to take part in the information sessions, bringing together a combination of technology providers, civil society organizations, non-governmental organizations, academic institutions, and interested individuals. The information sessions initiated a broader ecosystem dialogue to further the global learning agenda on digital ID's for humanitarian assistance.

For a summary of the outcomes of the information sessions, please see *Appendix A*.

II. Concept Notes Review (March - April 2019)

Following the information sessions, the DIGID team requested short concept notes from interested participants. There were 19 concept notes received from private sector and institutions on how they think the problem with lack of ID's for cash assistance could be solved. Those that submitted a concept note were invited to a bilateral meeting to better understand their proposals and ideas, as well as discuss possible sustainable costing models and risk mitigations to ensure scalability of the solution. The key themes and trends from the concept notes were helpful in developing the requirements that were eventually used in the Request for Proposal (RFP) process to procure the solution.

For a summary of the concept notes review, please see *Appendix B*.

III. Digital ID Workshop in Kenya (May 2019)

Kenya was selected by the DIGID team as the first pilot location for its depth of local partners, experience in cash and voucher assistance, and pain points related to identities. The Kenya Red Cross Society (KRCS) estimated roughly one quarter of its case load as lacking an official, recognized form of ID making it difficult to provide cash assistance. The other consortium members also have local presence in Kenya and in some cases work in the same communities as the KRCS.

The Digital ID workshop conducted in May brought together representatives from the government, financial service providers (mobile money), technology providers, and local NGOs. The workshop explored the challenges with identities for the different stakeholders in the cash assistance process, the possibility of a digital ID or credential solution, the perceived risks for affected population, and possible governance considerations if such a solution is implemented, all in the context of Kenya. A discussion on how digital ID's might be deployed in difficult, low connectivity settings, where many of the affected communities reside, and requirements to

achieve a true self-sovereign identity where individuals themselves have autonomy to control and manage their personal information.

The workshop allowed the DIGID team to gather tangible and concrete needs that were translated as functional and non-functional requirements for the open tender process that followed the market dialogue.

Figure 3: Facilitation of the Digital ID workshop in Kenya

Lessons Learned:

The innovative procurement was new to the consortium members and humanitarian actors in general. The process had to be fitted for the context of the project in consultation with Innovation Norway. The following are the key lessons learned in going through the process:

- The DIGID team spent more time on understanding the problem instead of jumping to solutions. Including the tender, the entire process has taken 12 months to complete. It does take time to systematically work on innovation. The concept of digital ID is complex and broad. It's still difficult to define it properly without causing confusion. It takes time to create consensus among the consortium members and to define the common needs and priorities; it takes time to learn the technology which was still evolving rapidly. But the

amount of learning and engagement that the team has developed set them well for implementation rather than with many critical unknowns.

- Having a consortium created credibility in tackling the problem across the humanitarian sector instead of being siloed to individual organizations. One of the key goals of the DIGID project is to address the issue of interoperability of data amongst humanitarian actors; particularly those assisting the same communities. Collectively analyzing the problems show an active step towards a durable solution.
- The process allowed the DIGID team to access a broad range of expertise and experience. This created strong interest to co-develop or brainstorm possible solutions, where there might be different approaches to solving the same problem.
- The public consultations attracted stakeholders from other organizations and donor communities to engage. And although led by Norwegian based NGOs, the learning came from all over the world and the team got inputs from global approaches to more contextualized, country specific solutions.
- In search of a solution, it is key to always remember to put the user at the center. Some discussions have focused narrowly on the efficiencies to be gained by humanitarian organizations, but it is important to keep in mind that the project is about the affected individuals and the success will be based on their experience. The whole project has been focused on exploring and learning the best ways to maximize the benefit impact as perceived by the individuals affected, and only then translating this into marginal efficiency gains for the agencies.

Appendix A: Summary of the DIGID Information Sessions

Overview:

The DIGID project conducted the information sessions between February and March 2019. Three online sessions and one on-site session were held, covering the different time zones. The objectives of the information sessions for the DIGID project were to:

1. Check if the problem statements and use cases developed were clear and if they resonated as a shared need in the wider humanitarian sector.
2. Identify and engage with the actors interested in solving the same problem.

Over 90 signed up to participate in the information sessions. Over 50% were from the private sector including tech and consulting firms. 24% represented humanitarian organizations, 14% indicated interested individuals and about 5% were from academic institutions.

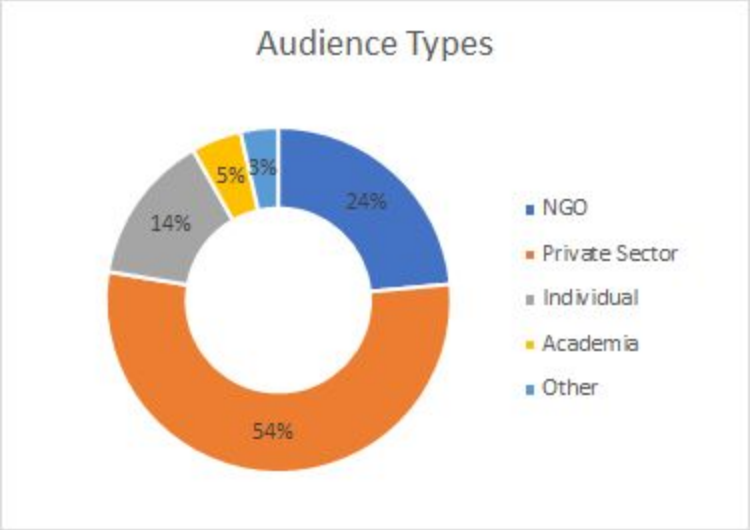

Figure 1: Different audiences that signed up in the Info Sessions

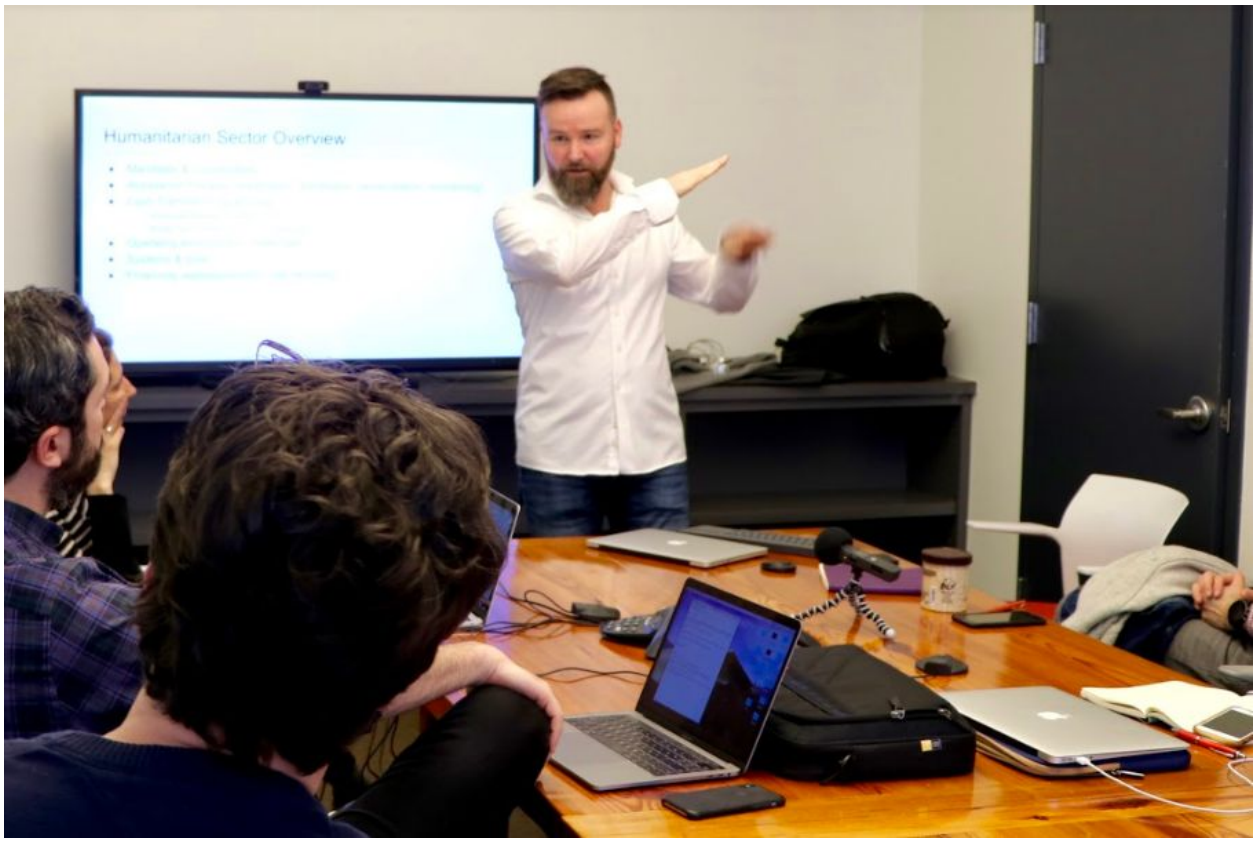

Figure 2: On-site Info Session in New York city

Methodology:

The information session was scheduled for two hours. The DIGID team presented the representatives of the consortium's technical working group facilitating the sessions, and provided an overview of the project and the innovation procurement process they were undergoing. A brief overview of the humanitarian sector and cash assistance was then presented to inform those who are not familiar with the actors and processes involved. This was followed by the presentation of the problem statements related to identities in cash programming; where appropriate, the user personas and user journeys were used. The rest of the time was given to the participants to ask questions, seek clarification of the problem, and have a discussion on certain topics related to identities and the DIGID project.

The session ended with an encouragement for the participants to submit a concept note if they were interested in addressing the issues together or explore solution options.

Question and Answer Summary:

The Q&A notes for most of the sessions are available in the Links section below. The following is a summary of the common topics that came up and the key takeaways during the information sessions:

The ID problem is longstanding, multi-sectoral, and already being addressed by several agencies within the humanitarian sector. Several participants alluded to the decades-long effort to solve the global identity problem. DIGID is not working to solve the global ID or the legal ID problem, but rather only a subset pertaining to humanitarian assistance. In the course of the information session several participants noted that there are ongoing, parallel efforts within the humanitarian sector to solve aspects of the ID challenge. These included the UNHCR tender on digital ID for refugees, the Red Cross/Red Crescent attempt to provide digital ID for volunteers and for peer-to-peer payments. Unlike these projects, however, DIGID takes an active collaboration of NGOs to work together and solve the problem. Rather than work on a one-off solution in a silo, DIGID is attempting to build an interoperable platform that could be scaled and sustained taking into account the low connectivity settings where many of the affected populations are located.

Interoperability is essential to the long-term success of the project. In order to design a future-proofed digital ID system, DIGID will need to invest resources upfront. DIGID needs to build to scale both vertically (in terms of number of beneficiaries reached) and horizontally (in terms of number of services offered). There are several ways to build for interoperability. DIGID needs to engage key ecosystem partners like UNHCR, WFP, consortium of NGO's such as CCD, and the Red Cross Red Crescent Movement, in addition to key ecosystem processes and compliance such as KYC regulations. Other interim steps like looking for solutions with open application programming interfaces built on open standards will be essential to move towards true interoperability.

A modular approach can offer a path to long-term interoperability. Rather than developing a one-size fits all solution for all use-cases, DIGID could instead solicit the development of discrete components that serve specific functions, and scale those vertically (in terms of number served) and horizontally (in terms of services offered). For example, DIGID could solicit a biometrics provider to develop an authentication mechanism that could be integrated with an identity service provider to develop a robust, flexible solution that could be deployed in several different contexts.

Potential and challenge of Self-Sovereign ID (SSI)/Decentralized ID (DID). Several participants raised the possibility of leveraging emerging technologies in order to develop SSI/DID. The key advantage of SSI/DID is shifting the focus of control over information

from organizations to individuals. With individuals managing their own data, verification can be reimagined as a process done on an ongoing as-needed basis as beneficiaries attempt to access specific services, rather than a one-time event per agency. However, both DIGID and providers noted that there remain several unanswered questions regarding SSI/DID. For instance, many individuals have trouble managing passwords, how can these beneficiaries be expected to manage repositories filled with data? DIGID noted that education will certainly be a part of any solution in deployment, but will need to be coupled with alternative options. For this reason, solving for the challenges of guardianship, whereby one entity is empowered to act on the behalf of another, is paramount. However, any system of guardianship/custodianship will need to operate in accordance with KYC/AML/CTF regulations, as well as with GDPR-like frameworks.

Importance of building regulation-adaptable technologies. Cash-based programming, perhaps the most opportune use-case for digital ID in the humanitarian sector, needs to operate in accordance with relevant regulation including KYC/AML/CTF and GDPR. Therefore, DIGID and providers alike noted the importance of building regulation-adaptable technologies. DIGID also noted the importance of following government lead on these regulations, which providers should be building with in mind. Conversation with government agencies and regulatory bodies should be included in the wider consultation.

Need to address data mismanagement and leakage in the humanitarian sector (data protection risks). The humanitarian sector already faces challenges of data mismanagement and leakage. The transfer of information on spreadsheets and through centralized databases pose potential risks to the information of some of the world's most vulnerable population. Many of these concerns are process related more than technology, however, it was noted the importance of (where possible) limiting the amount of personally identifying information in the course of information exchange. In the process of collecting data, it was also noted the importance of ethical or data responsibility frameworks. One participant noted that there remain several concerns regarding the humanitarian use of biometrics, for instance.

Links:

- Information Session slides: https://hiplatform.org/s/Dignified-IDs-Info-Session-published-march-05-2019.pdf
- Minutes from the information sessions: https://hiplatform.org/s/INF_-20190300-DIGID-INF-Minutes-from-Information-Sessions-presented-content.pdf
- Compiled Q&A: https://hiplatform.org/s/INF_-20190300-DIGID-INF-Questions-and-Answers-combined-from-sessions-1-5.pdf
- Link to Concept Note template: https://hiplatform.org/s/DIGID-Concept-Note-Template.pdf

APPENDIX B: Summary of the Concept Notes Review

Overview

Following the information sessions, the DIGID team requested short concept notes from interested participants. A template was provided to help organize the topics to discuss. There were 19 concept notes received from private sector and institutions on how they think the problem with lack of ID's for cash assistance could be solved.

Those that submitted a concept note were invited to a bilateral meeting to better understand their proposals and ideas, as well as discuss possible sustainable costing models and risk mitigations to ensure scalability of the solution. Bilateral meetings were done between March and May 2019.

The key themes and trends from the concept notes were helpful in developing the requirements that were eventually used in the Request for Proposal (RFP) process to procure the solution.

Key Themes & Learnings from the Concept Notes

The following is a summary of the key themes and general learning from reviewing the concept notes and having bilateral meetings with the vendors.

#1: The term "digital ID" means different things to different people. Inconsistent definitions cause confusion. The term "self-sovereign ID" is also defined in different ways.

- In simple terms "Digital ID" can be referred to as any system that supports the identification lifecycle by using digital technologies. The terminology itself is very broad, so the discussion easily trails from Facebook ID's, to digital legal ID's, to biometrics, to beneficiary databases used by aid organizations. When discussing digital ID for the project, it was helpful to use concepts such as functional ID's vs. foundational ID's--a difference in terms of being authenticated to receive a service or function versus being able to prove who they are--and identification vs. authentication--to help level set people's understanding.
- In simple terms "self-sovereign ID" refers to a system that supports the identification lifecycle by placing the user in control of their identity attributes. Though there is general agreement on this definition of self-sovereign identity, several providers submitted

proposals for forms of self-sovereign ID with different functionalities, features, and degrees of user-centricity.

- For example, one provider defined SSI as a system where identity is owned, managed, and controlled directly by identity owners, rather than third parties and noted that DLT, and other emerging technologies, can make this possible at the technical level.
- Another provider defined SSI as a personal datastore online to enable persistence of ID, user-centric focus, personal ID account, informed consent, portable ID based global standards, data custodianship and trust, financial inclusion, offline environment, verifiable credentials.
- Other providers highlighted the fact that they do not intend to build self-sovereign ID, but rather identity data repositories and the functionalities of a claim verification network, where by steward organizations can store encrypted backups of ID documents on behalf of individuals.
- Still other providers simply intended to serve as custodians of data, acting as a trusted entity (like a bank) to help individuals manage their data in a reliable way.

- Nonetheless, some common attributes of SSI did emerge. One element common across multiple providers was portability: In essence, portability is the capacity to transfer logic across multiple platforms without losing meaning. Importantly, portability is distinct from interoperability, which is the ability for different software and hardware to communicate. Though theoretically desirable, data portability remains practically unrealized.
- Article 20 of the European Union's General Data Protection Regulation (GDPR) urges that individuals have the right to data portability. The GDPR is not alone in its push for data portability. Similar efforts to enhance data portability have been taken in the financial sector. The European Commission's Payment Services Directive (PSD2) mandates that banks give third-party providers access to customer data via application programming interfaces. These, and other regulations, have attempted to mandate data portability in law.
- Though the exact meaning of the term "self-sovereign identity" remains unclear, it is clear that portability is a desired outcome of the DIGID project, among consortium members and members of the technical ecosystem, alike. However, there remain important unanswered questions regarding SSI, like guardianship. At the technical level, there are several competing ways to realize guardianship. However, in practice, realizing guardianship is complex and must be calibrated for local context. SSI providers have yet to offer clarity on how they plan to realize guardianship in practice.

#2: Widespread agreement on the importance of open source/open standards for interoperability, and avoidance of vendor lock-in, in order to support long-term functionality:

- Like the Domain Name System (DNS), which looks up over 100 billion domain names per day, several providers described potential platform offerings for global digital ID functionality, whereby every individual would have one decentralized identifier for every relationship. Critical to this infrastructure is that only decentralized IDs of credential verifiers are stored on chain (if blockchain is used), with all personal data stored off-chain, enabling any party using this system can prove: source of the claim (issuer), that the data was issued to the identity owner only, that it has not been tampered with, and that it has not been revoked. Could this improve data sharing among humanitarian organizations? If constructed as a utility, like the DNS, such a system could prove resiliently interoperable digital ID solutions in the years to come.
- The need for open standards for interoperability was also cited by a number of providers. Several made reference to the work of the Decentralized Identity Foundation (DIF) and the W3C standard for verifiable credentials. Most, however, asserted that there remains significant need to develop further standards to enable true interoperability.
- Providers also noted that interoperability can be, at least partly, achieved through simple measures like using open standards such as DIDs and verifiable credentials, or by building wallets that can be accessed thru an API in order allow individuals to read and write consent for certain actions. Several providers noted that the use of widely recognized data exchange formats like JSON Web Tokens can be used as a standard for signing digital ID docs, as validated by W3C, can be a useful mechanism for realizing interoperability.

#3: Digital ID is dependent on a number of technologies, many of which are emerging and untested globally, and are especially new to humanitarian contexts:

- Providers called out a number of emerging technologies that could be used to realize digital ID, including frontier biometry and emerging distributed ledger technology. Several of the functions that providers seek to build depend on the use of this technology. However, many of these technologies are still nascent and relatively untested. Given the challenging environments common to humanitarian work, it is critical that providers build robust, resilient stacks that can be deployed in low to no power and connectivity conditions.
- One such emerging technology, blockchain or distributed ledgers (DLT), pose a potential concern to humanitarian organizations. Though some, including DIGID consortium members, have piloted distributed ledger technology, there remains limited buy-in for it in the sector. As such, systems that leverage DLT should ask, does it add

value or would a simple database with privacy protecting elements be enough? What about data protection when such technology is used? These risks need to be considered carefully.

#4: Whatever technology is leveraged, it must be built and integrated in a way that ensures privacy-by-design, protecting the identifying information of beneficiary communities, which could include some of the world's most vulnerable individuals:

- Privacy is a right recognized in the Universal Declaration of Human Rights and explicitly articulated in the constitutions of many countries. Providers noted that offline identity is private by nature. Few, if any, institutions have access to all of your credentials in an offline world.
- Online, however, it becomes possible to aggregate data and form a single comprehensive log that can, under analysis, reveal identity.
- Several providers noted the danger inherent in using identity technologies to service some of the worlds most vulnerable and cautioned against, for instance, putting any personally identifiable information (PII) on-chain in a system that makes use of DLT.
- Many suggested potential mechanisms for ensuring user privacy including, holding on to signatures of claims by issuers on a distributed ledger.
- Others noted that destroying biodata can be a useful measure to protect against re identification by malicious actors.
- In the process of securing user-data, respondents also highlighted the critical role that must be played by informed consent. Key to developing true informed consent is education. Several providers noted that educating beneficiaries on factors including user-control, key recovery, decentralization, biometrics, vendor lock-in, third-party sharing, and the like, would be key to generating meaningful informed consent. However, when dealing with emergency assistance where the vulnerable individual is asked to consent in order to receive aid does not seem to indicate that consent is the most appropriate legal basis.

#5: In order to build functional, responsible digital ID systems, there is a need for fit-for-purpose guidance and regulation:

- Historically, regulation in Europe has tended to focus on personal data, rather than PII. The European Data Protection Directive defines personal data as any information relating to a "[...]natural person who can be identified, directly or indirectly, in particular by reference to one or more factors specific to his physical or social identity." The phrase "directly or indirectly" is key. It suggests that data cannot only exist in correspondence with identity, but also in corollary. By joining disparate pieces of information, it becomes possible to identify an individual through indirect means.

- Several respondents noted GDPR-compliance (or at least attempted compliance) but continued to caution that fit-for-purpose regulation relevant to the humanitarian sector would be useful in designing technologies.

#6: Digital ID is only useful if it's usable:

- Several providers argued that there is little point in mounting a complex and costly ID-based system, unless the applications for the user are clearly evident and obviously compelling. Without providing access to a specific good or service, digital ID programs risk quickly falling into disuse. In order to prove their utility, digital ID programs ought to be tied immediately to a good or service.
- Several respondents proposed means of proving value to beneficiaries including:
    - Offering a platform that facilitates certification and verification of skill identity.
    - Providing a credentialing system to issue secure, verifiable digital records at scale that can be used to facilitate access to aid, to improve efficiency, to establish trust, improve accountability, increase user control, function offline.

#7: Though there are an increasing number of providers in the marketplace, there is as yet no clear market leader.

- Several providers submitted proposals for systems that could perform the functions DIGID requires. However, the method by which they achieve these functions, and the underlying technologies in use differ widely from provider to provider.
- Bottom-line: this is a young ecosystem with a wide variety of providers offering a diversity of products. It is possible that in the next five years the marketplace will have rallied around a few reliable enterprise-grade systems. Very few providers in the ecosystem have surpassed the pilot phase.
- This is especially possible because there is clear interest in the space in developing sharing standards towards interoperability and offering specific guidance that goes beyond the principles-based approach of frameworks like "privacy by design."
    - It may be argued that such existing frameworks lack the specificity required to move the marketplace towards an end-to-end solution that could achieve all the functionalities required by DIGID and other value-aligned organizations.

#8: Lack of clarity regarding pricing model:

- Though the concept notes offered specifics regarding past use-cases of a technology they did not go into detail regarding pricing. It is likely that pricing has not yet been standardized in this space and, therefore, most providers are developing proposals on a case by case basis. This presents a challenge for DIGID and other organizations seeking to project cost and develop comprehensive budgets.
- Beyond a total cost, there was also no specificity offered in terms of budget line items.

- It is also unclear how the providers, beyond a simple licensing model, plan to monetize their products. There is a particular concern in the ecosystem around the potential for the monetization of the data of vulnerable populations. Though not yet a problem, several providers have raised the possibility.