

A photograph of three women sitting outdoors, looking at mobile phones. The woman in the center is wearing a blue face mask and a yellow and blue patterned top. The woman on the left is wearing a red top and a blue face mask. The woman on the right is wearing a floral top and an orange face mask. They are all looking at their phones, which are held in their hands.

**ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ
ЛИЧНОСТИ
АНАЛИЗ
ДЛЯ ГУМАНИТАРНОГО
СЕКТОРА
МАЙ 2021 Г.**



Перевод подготовлен
Лингвистическим центром
Российского Красного Креста

ВЫРАЖЕНИЕ БЛАГОДАРНОСТИ

Выражаем благодарность за поддержку в подготовке данного отчета следующим организациям:



Подготовка данного отчета стала возможной благодаря финансированию со стороны Американского Красного Креста.

За проведение консультаций и подготовку отчета отвечал Оксфордский центр развития и технологий. Авторы отчета – Эйден Славин, Франциска Путц и д-р Эмре Эрен Коркмаз.



Мы также выражаем благодарность всем респондентам проведенных интервью за их вклад в подготовку данного отчета.

© Международная федерация обществ Красного Креста и Красного Полумесяца, Женева, 2021 г.

Любая часть данной публикации подлежит цитированию, копированию, переводу на другие языки или адаптации для использования на местном уровне без предварительного разрешения Международной федерации обществ Красного Креста и Красного Полумесяца при условии четкого указания источника.

С нами можно связаться:

Пожалуйста, направляйте запросы на воспроизведение данного материала в коммерческих целях в Секретариат МФОККиКП:

Адрес: Chemin des Crêts 17, Petit-Saconnex, 1209 Geneva, Switzerland

Почтовый адрес: P.O. Box 303, 1211 Geneva 19, Switzerland

T +41 (0)22 730 42 22 | **F** +41 (0)22 730 42 00 | **E** secretariat@ifrc.org | **W** ifrc.org

Фотография сделана Кенийским обществом Красного Креста. Из проекта 121, реализованного Кенийским обществом Красного Креста, - инициативы 510 Нидерландского Красного Креста и Британского Красного Креста. При финансировании GSMA.

СОДЕРЖАНИЕ

Резюме	2
Введение	3
Выводы и рекомендации	5
Вопрос 1: В каких случаях могут применяться решения по цифровой идентификации, и что делает их подходящими? Каковы ограничения их применимости?	5
Вопрос 2: В настоящее время возрастает необходимость защиты данных получателей помощи, внедрения технологий самостоятельной идентификации, чтобы предоставить получателям помощи больше автономии в управлении и владении своими данными, а также уменьшения объемов конфиденциальных данных, хранящихся в централизованных базах данных. Ввиду перечисленного, как гуманитарные организации должны адаптировать свои системы и практику управления данными получателей помощи для обеспечения ответственной интеграции цифровых идентификационных решений?	8
Вопрос 3: Организации по оказанию помощи располагают ограниченными ресурсами. Принятие новых технологий может повлечь за собой барьеры в плане затрат, навыков и ресурсов (обслуживание, поддержка и т.д.). Какие экономические стимулы и устойчивые бизнес-модели для использования технологии цифровых идентификаторов применимы к гуманитарным организациям?	10
Вопрос 4: Что представляет собой операционная совместимость между гуманитарными организациями, использующими цифровые идентификаторы? При ответе на этот вопрос следует изучить функциональную совместимость данных независимо от технологий, используемых для их сбора и хранения (например, цифровые удостоверения, выданные различными технологиями цифровых удостоверений личности, но использующие такие стандарты, как децентрализованные идентификаторы, проверяемые удостоверения и т.д.), а также процессы и готовность обмена данными между организациями для предотвращения дублирования.	13
Вопрос 5: Перспективы самостоятельной идентификации зависят от нескольких факторов: цифровой грамотности конечных пользователей, степени развитости инфраструктуры и доступности средств связи, таких как смартфоны. Такие факторы являются барьерами в местах, где потенциальные получатели помощи могут быть одними из самых уязвимых групп населения. Как гуманитарные организации могут внедрять технологии цифрового удостоверения личности в условиях низкой доступности связи?	15
Вопрос 6: Существует противоречие между желанием отдельных лиц сохранить контроль над собственными данными (децентрализация хранения данных и контроля получателям помощи над ними) и желанием организаций использовать данные отдельных лиц в целях координации (чтобы избежать дублирования и мошенничества) и подотчетности перед донорскими организациями (чтобы продемонстрировать, что помощь оказывается реальным людям). Каковы компромиссы, связанные с разрешением этого противоречия? Как можно найти баланс? Каких подводных камней следует избегать?	16
Вопрос 7: Какое обучение грамотности в области данных требуется получателям цифровых идентификаторов для того, чтобы они могли безопасно ими пользоваться? В чем различия этих требований для пользователей смартфонов и телефонов?	18
Примеры	20
121 Консорциум прямой денежной помощи в Кении	20
Платформа по передаче цифровых активов компании Sikka на основе Ledger-технологий	
Программа усиления эффекта от реализации Целей устойчивого развития в Турции	31
Выводы	35
Список источников	36
Список дополнительных источников, использованных в данном отчете	39
Приложения	40
Приложение I: Вопросы интервью	40
Приложение II: Респонденты	41
Приложение III: Подробное описание методологии	42

РЕЗЮМЕ

Способность подтвердить свою личность становится все более важным аспектом функционирования современного общества. Действительно, Цели устойчивого развития ООН включают задачу 16.9: «К 2030 г. обеспечить юридическую идентификацию личности для всех, включая регистрацию рождения». Однако идентификация личности может представлять собой серьезную проблему для получателей гуманитарной помощи. Развитие технологий открывает большие перспективы в области цифровой идентификации. Однако, когда гуманитарные организации берутся за изучение таких решений, они должны решить ряд вопросов, от технических – как внедрить цифровую идентификацию в усложняющуюся экосистему и как обеспечить применение таких цифровых решений в местах с низким уровнем охвата связью, где проживают многие уязвимые группы населения – до этических – как обеспечить сбор данных получателей помощи таким образом, чтобы соблюсти конфиденциальность их частной жизни и обеспечить им больше независимости в управлении их личными данными – и как обеспечить устойчивость этих решений.

Данный исследовательский отчет был подготовлен по заказу Международной федерации обществ Красного Креста и Красного Полумесяца при поддержке консорциума проекта Достоинство личности при оказании денежной помощи (ДЛДП) и выполнен Оксфордским центром технологий и развития.

В настоящем отчете представлены семь основных вопросов, которые гуманитарным организациям необходимо рассмотреть, прежде чем инвестировать в решения в области цифровой идентификации личности. Эти вопросы, в свою очередь, легли в основу ряда интервью с 24 экспертами, обладающими соответствующими знаниями и опытом в области цифровой идентификации. Свод данных, полученных в трех тематических исследованиях, дополняет и иллюстрирует выводы, сделанные по результатам проведенных интервью.

Данный отчет начинается с краткого анализа того, как в частном секторе используются технологии цифровой идентификации личности. Далее в отчете рассматриваются примеры использования цифровой идентификации и потребности гуманитарного сектора, в которых могут быть применены такие технологии. Достижение операционной совместимости было отмечено как важнейшее требование для реализации основных преимуществ цифровой идентификации в гуманитарном секторе. Такая совместимость имеет две составляющие: решения в области цифровой идентификации должны быть интегрированы с другими технологиями, основанными на данных, и данные должны использоваться различными субъектами, чтобы личность получателя помощи была признана в широком масштабе, а не в изолированных системах. Изменение культуры управления данными и политическая воля для достижения функциональной совместимости с участием многих заинтересованных сторон являются важными соображениями, помимо тех, которые касаются непосредственно технической реализации.

Существуют препятствия для внедрения и принятия решений по цифровой идентификации, поскольку многие гуманитарные организации работают в условиях, которые не всегда благоприятны для цифровых технологий с точки зрения доступа к связи, устройствам, таким как мобильные телефоны, и уровня грамотности конечных пользователей. Важно помнить об уязвимых сообществах при разработке таких цифровых решений и сохранять сбалансированный взгляд на их преимущества для организации и для самих получателей помощи. Что касается развертывания и обслуживания решений по цифровой идентификации, поставщики технологий и организации, работающие с сообществами, должны интегрировать возможности обучения и тренинга для получателей помощи.

Внедрение систем цифровой идентификации может быть дорогостоящим, и для обеспечения успешного расширения масштабов после проведения пилотного проекта необходимо наличие устойчивых бизнес-моделей. Затраты могут усугубляться тем, что донорские организации воспринимают их как «бэк-офисные» технологии. Поэтому организации должны четко обосновать непосредственные преимущества для получателей помощи. Опять же, другие сектора могут послужить примером. Например, лицензирование программного обеспечения как услуги может быть более эффективным в долгосрочной перспективе, чем (ряд) единовременных грантов на развитие.

В целом, технологии цифровой идентификации действительно перспективны в плане расширения гуманитарных услуг для новых получателей помощи и улучшения существующих услуг для нынешних получателей помощи, а также с точки зрения выгоды для самих гуманитарных организаций. Однако их применение требует тщательного планирования и рассмотрения для обеспечения их пригодности и эффективности с учетом местных требований и условий.

ВВЕДЕНИЕ

Цели устойчивого развития ООН (ЦУР), основанные на успехах и выводах из реализации Целей развития тысячелетия, включают 17 целей, которые международное сообщество должно достичь к 2030 г. Цель 16 «Мир, справедливость и сильные институты» включает задачу 16.9: «К 2030 г. обеспечить законную идентификацию для всех, включая регистрацию рождения». В рамках работы над выполнением задачи 16.9 были мобилизованы в широкую коалицию государственные и частные организации для работы над устранением разрыва, который существует в мире, когда речь идет о доступе людей к удостоверению личности.

Возможность подтвердить свою личность все чаще становится необходимым условием для получения доступа ко многим услугам в государственном и частном секторах. В то время как процесс идентификации традиционно облегчали документы на бумажных носителях, сегодня он все больше зависит от цифровых технологий [1]. Сегодня для гуманитарных организаций и агентств по развитию как никогда важно изучить преимущества и недостатки цифровых технологий идентификации. Сегодня организации, включая поставщиков телекоммуникационных услуг, финансовые учреждения, правительства и другие организации, начинают предпринимать новые усилия по цифровизации, чтобы адаптироваться к новым разработкам в области управления идентификацией, обеспечения доступа к идентификации и децентрализации процесса идентификации [2].

Система цифровой идентификации (ID) – это не одна технология, а набор технологий, которые в совокупности облегчают процесс идентификации. Решение для обеспечения цифровой идентификации – это набор технологий, обеспечивающих поддержку в процессе идентификации [3]. Цифровая идентификация все еще определяется по-разному различными заинтересованными сторонами. Цифровой идентификатор может представлять собой цифровую копию документа, удостоверяющего личность, набор атрибутов, представляющих человека в транзакции, или метасистему цифровых идентификаторов, которые в совокупности могут однозначно идентифицировать человека [4].

Частный сектор видит потенциал цифрового удостоверения личности в повышении экономической ценности для компаний, правительств, сотрудников, потребителей и налогоплательщиков. Ключевой демографической ценностью, к которой организации частного сектора стремятся получить доступ с помощью технологий цифровой идентификации, являются более 1,7 миллиарда человек во всем мире, которые в настоящее время исключены из традиционного финансового сектора по причине отсутствия у них официального удостоверения личности.

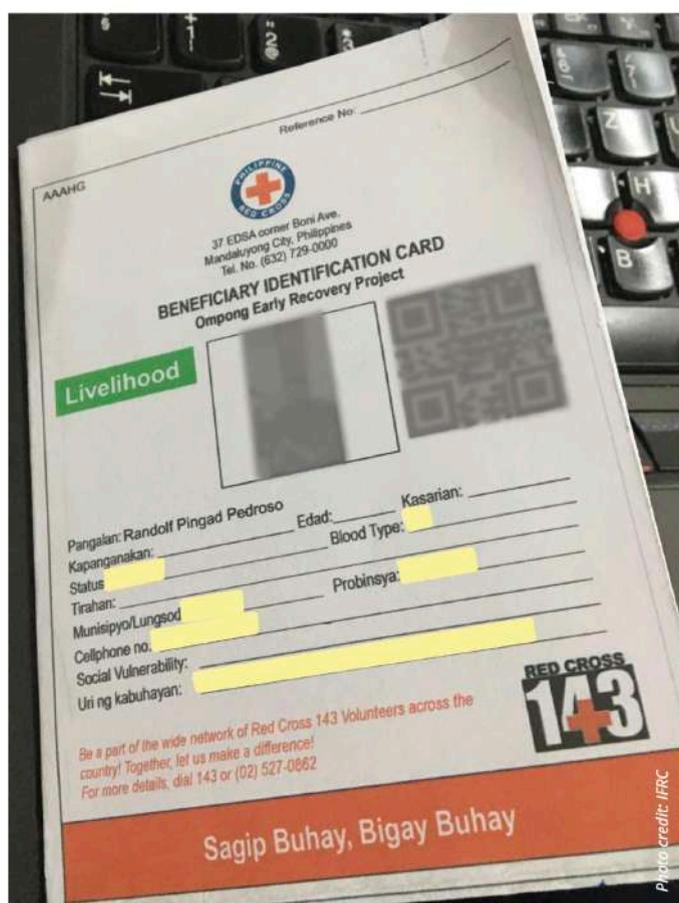
Частный сектор видит значительную возможность в том, чтобы с помощью систем цифровой идентификации оптимизировать предоставление услуг электронного правительства, таких как социальная защита и прямые выплаты пособий. По оценкам McKinsey Global Institute, системы цифровой идентификации помогут сэкономить примерно 110 миллиардов часов, которые в настоящее время уходят на распределение государственных услуг. Потенциально такая экономия времени представляет собой значительную возможность получения прибыли для организаций частного сектора, желающих предоставлять услуги государственному сектору. Возможности экономии затрат не ограничиваются государственным сектором: благодаря снижению затрат на регистрацию и отслеживанию случаев мошенничества при начислении заработной платы с помощью усовершенствованных «умных» методов аутентификации, использование систем цифровой идентификации может привести к экономии в размере 1,6 триллиона долларов США во всем мире.

Преимущество от использования этих систем получают не только организации, но и отдельные граждане. Предлагая людям возможность экономической и политической интеграции, системы цифровой идентификации могут проложить дорогу к более широкому равенству доступа и контроля над информацией [8].

По мере того как Международная федерация обществ Красного Креста и Красного Полумесяца (МФОКК и КП) и другие гуманитарные организации расширяют свои цифровые предложения, они начинают изучать возможности цифровой идентификации как способа улучшения качества существующих услуг для получателей помощи и предоставления новых. МФОКК и КП руководит технической работой по реализации проекта Dignified Identities in Cash Assistance (DIGID) [9] совместно с консорциумом крупнейших НПО Норвегии, включая Норвежский Красный Крест, Норвежский совет по делам беженцев, Норвежскую церковную помощь и Норвежский Фонд спасения детей. Вместе они стремятся решить проблемы, связанные с предоставлением гуманитарной денежной помощи людям, не имеющим признанных удостоверений личности.

Данный отчет был подготовлен по заказу МФОККиКП при поддержке консорциума DIGID для анализа использования решений по цифровой идентификации в гуманитарном секторе. Мы надеемся, что этот отчет будет полезен всем представителям гуманитарного сектора, которые хотят инвестировать или разработать решения по цифровой идентификации для своей организации.

Данный отчет основан на исследовании, проведенном смешанным методом и включающем обзор литературы, интервью с экспертами и тематические исследования. Интервью были построены на семи важнейших вопросах, составленных МФОККиКП, которые часто задают гуманитарные организации, изучающие решения в области цифровой идентификации (список вопросов приведен в Приложении I). Было опрошено 24 эксперта из гуманитарных организаций и частного сектора, обладающих знаниями и опытом в данной области (список приведен в Приложении II). Ответы, полученные в ходе интервью, были проанализированы, а выводы и рекомендации обобщены ниже. Наконец, в целях анализа сложности, возникающих при внедрении систем цифровых идентификаторов, были изучены три конкретных примера: платформа Sikka компании World Vision International в Непале, стартап Digital ID компании SDG Impact Accelerator в Турции и пилотный проект, заверченный консорциумом 121 в Кении в конце декабря 2020 г. Подробное описание методов исследования см. в Приложении III.



Филиппины, 2018 г.: Реагируя на последствия тайфуна Мангхут Филиппинский Красный Крест (ККК) выдал идентификационные карты получателей помощи тем, кто получал помощь в виде жилья и средств к существованию. Уникальный идентификационный QR-код был включен в карту, что облегчало сотрудникам и волонтерам проведение проверки подлинности личности получателя, поскольку данные были связаны с системой управления информацией о получателях помощи PRC.

ВЫВОДЫ И РЕКОМЕНДАЦИИ

Вопрос

1

В каких случаях могут применяться решения по цифровой идентификации, и что делает их подходящими? Каковы ограничения их применимости?

Гуманитарные организации начали апробировать решения по цифровой идентификации в самых разных контекстах. Среди наиболее часто обсуждаемых – программы денежных переводов, медицинские услуги и предоставление удостоверений личности для получателей помощи, не имеющих официально признанной формы удостоверения личности [2]. Каждый случай характеризуется уникальными преимуществами и недостатками. Помимо краткого описания этих преимуществ и недостатков, в данном разделе предлагаются определения базовых и функциональных идентификаторов.

Основной сферой использования цифровой идентификации гуманитарными организациями является регистрация или включение получателей в программы помощи. Предоставляя цифровые инструменты для подтверждения того, что человек является тем, за кого себя выдает, решения для цифровой идентификации могут облегчить процесс регистрации или зачисления в гуманитарном секторе двумя способами.

Во-первых, гуманитарные организации могут предоставлять важнейший идентификатор получателям помощи, у которых нет официально признанной формы удостоверения личности. Важнейший идентификатор – это форма идентификации, которая обладает высокой степенью надежности или доверия, например, паспорт. Он позволяет пользователям получать доступ к широкому спектру услуг. Предоставляя форму важнейшего удостоверения личности, гуманитарные организации могут обеспечить получателям помощи доступ ко многим услугам как в гуманитарном контексте, так и за его пределами. Такой идентификатор не обязательно должен обладать таким же уровнем надежности или доверия, как паспорт, но он все равно может быть полезен для получателей помощи в долгосрочной перспективе как форма идентификации [10]. Примеры важнейших гуманитарных удостоверений личности включают удостоверение беженца УВКБ ООН. В Египте в 2018 г. поставщики телекоммуникационных услуг начали признавать удостоверения беженцев УВКБ ООН в качестве действительного документа для подтверждения личности при покупке мобильной SIM-карты [11]. Таким образом, гуманитарные удостоверения могут служить целям, выходящим за рамки их ограниченной сферы применения в качестве средства содействия распределению помощи, и могут способствовать социально-экономическому развитию получателей помощи в долгосрочной перспективе [#1]. Важно отметить, однако, что такое положение является основополагающим для мандата УВКБ ООН [12].

Во-вторых, гуманитарные организации могут предоставить получателям помощи форму масштабируемого, функционального идентификатора, который со временем может накапливать историю транзакций и, вместе с ней, способствовать повышению степени доверия к традиционным поставщикам услуг. Функциональный идентификатор – это форма идентификатора, выдаваемого для предоставления доступа к одной услуге или одному классу услуг [13]. Этот вторичный механизм аналогичен тому, как поставщики услуг используют альтернативные источники данных для создания альтернативной кредитной истории с целью повышения «банковской состоятельности» уязвимых групп населения.

Несколько гуманитарных организаций также начали изучать возможность использования цифровых идентификационных решений для предоставления учетных данных волонтеров. Австралийский Красный Крест разработал онлайн-кошелек для хранения и идентификации учетных данных волонтеров [#2]. Используя стандарт World Wide Web Consortium (W3C), поставщик технологий TurеHuman разработал приложение, которое анонимно отслеживает данные о поведении добровольцев для поддержки клиентских и бизнес-процессов с помощью цифровых идентификационных решений нового поколения [14]. Ссылки, которым предшествует символ #, относятся к интервью. Имена и должности интервьюеров см. в Приложении I.

Наконец, возможно также, что наиболее часто применяемым в гуманитарном секторе пилотным вариантом использования цифровых идентификационных решений на сегодняшний день являются программы денежных переводов. В рамках таких пилотных проектов получателям помощи предоставляется доступ к финансовым услугам посредством применения функционального идентификатора. Одна из таких систем, разработанная компанией Tuckr и опробованная в сети Sovrin, позволяет осуществлять транзакции через централизованную архитектуру. Другой такой системой является децентрализованный идентификатор RedRose, который может быть использован для осуществления платежей на основе денежных переводов. Следствием использования цифровой идентификации для поддержки программ денежных переводов является использование цифровой идентификации для финансирования на основе прогнозов, чтобы облегчить перевод средств в преддверии стихийного бедствия, что позволяет более оперативно и рационально реагировать. Хотя технология цифровой идентификации может внести ненужные и обременительные трения в ситуации оказания чрезвычайной помощи (например, из-за зависимости от мобильной связи, которая не всегда доступна), она также обладает потенциалом для обеспечения поддержки долгосрочных инициатив по оказанию помощи и развитию. Например, Джимми Снук из Tuckr описал сценарий, при котором люди, которые были идентифицированы для предыдущих инициатив по оказанию помощи, могут продолжать получать поддержку в виде прямых денежных переводов, когда прогнозируется наводнение и им, вероятно, понадобятся ресурсы для укрепления своей деревни [#3].

Рекомендация 1А

Способствовать секторальной и межсекторальной операционной совместимости.

Создание долгосрочной, пригодной для использования системы идентификации для оказания поддержки в процессе регистрации или зачисления получателей помощи, сверки удостоверений волонтеров и разработки программ денежных переводов требует операционной совместимости и обмена информацией между организациями, оказывающими и не оказывающими помощь. Чтобы облегчить использование учетных данных за рамками их первоначальной функции, системы хранения гуманитарных данных должны быть совместимы с системами организаций, к которым получатель помощи стремится получить доступ [15]. Например, используя общую схему здравоохранения и формат обмена данными, гуманитарная организация может позволить получателю помощи обмениваться своими медицинскими данными с поставщиком медицинских услуг, тем самым улучшая результаты лечения. В этом случае операционная совместимость должна быть установлена не только внутри гуманитарного сектора, но и с системой здравоохранения. Это требует знания и готовности разрабатывать системы в соответствии с установленными процессами в других секторах, включая, например, спецификацию ресурсов оперативной совместимости в здравоохранении [16]. Еще один потенциальный случай использования, требующий операционной совместимости, - облегчение доступа к официальным сферам в таких случаях, как взаимодействие с банками или телекоммуникационными компаниями.

Стоит отметить, однако, что эксперты скептически относятся к тому, что гуманитарные организации могут предоставить базовые идентификаторы, необходимые для обеспечения надежной, масштабируемой идентификации. Один из респондентов [#4] выразил категорическое несогласие с оптимистическим видением данной тенденции:

«Я не вижу, чтобы эта тенденция (включение людей, не имеющих банковского счета) имела место. На самом деле банки сами становятся поставщиками идентификационных данных. Они предоставляют услуги, а затем интегрируют свои услуги с государственными органами для того, чтобы установить личность получателя услуг. Таким образом, наличие счета в банке создает возможность для идентификации вашей личности органами власти. Это совершенно противоположная тенденция, за которой стоит гораздо большая сила, чем стремление привлечь не охваченных банковским обслуживанием людей в банковскую систему с помощью введения гуманитарной системы идентификации».

Тем не менее, поскольку как гуманитарные, так и негуманитарные организации стремятся предоставить получателям помощи высокофункциональные формы удостоверения личности, им придется развивать отраслевую и межсекторальную совместимость, чтобы обеспечить пригодность для использования удостоверений личности.

Рекомендация 1В

Продвигать преимущества и признавать недостатки цифровых идентификационных систем для мобилизации политической воли и технического ноу-хау.

Достижение операционной совместимости часто является скорее вопросом политической воли, чем технической реализации. Для обеспечения операционной совместимости в масштабах страны, которая позволит получателям помощи использовать свои учетные данные в самых разных условиях, потребуется проведение значительной работы по поддержке и продвижению в гуманитарных организациях и в других секторах. Даже если гуманитарные организации смогут организовать необходимую кампанию по развитию операционной совместимости, это все равно потребует инноваций на техническом уровне. Действительно, попытки изменить практику регистрации данных в организациях с радикально различными информационными архитектурами будут сталкиваться со значительными препятствиями [#5] [#6]. Более того, правовые ограничения (включая разработку соглашений об интеллектуальной собственности и доверительных рамок «от точки к точке») представляют собой проблему для внедрения любого рода технологических изменений в гуманитарном секторе [#7]. Несмотря на значительный прогресс, достигнутый сообществом децентрализованной идентификации в разработке стандартов, в первую очередь W3C, еще многое предстоит сделать [14].

Таким образом, сближение стандартов в гуманитарном пространстве потребует активного продвижения к усилению как политической воли, так и технических ноу-хау. Внимание ученых, анализирующих политическую волю, в основном сосредоточено на четырех ключевых компонентах:

Тем не менее, поскольку как гуманитарные, так и негуманитарные организации стремятся предоставить получателям помощи высокофункциональные формы удостоверения личности, им придется развивать отраслевую и межсекторальную совместимость, чтобы обеспечить пригодность для использования удостоверений личности.

- большое число лиц, принимающих решения
- широкое и общее понимание проблемы и возможных решений
- широкая поддержка решения
- готовность к итерационному поиску эффективного решения.

Хотя каждая организация должна сама определить, как лучше всего воздействовать на эти четыре фактора политической воли, несколько первоначальных шагов включают в себя:

- вступление в соответствующие торговые и отраслевые организации для накопления
- внутреннего и внешнего опыта
- участие в соответствующих форумах
- участие в диалоге на внутреннем уровне, направленном на то, чтобы четко увязать
- ценность инновации с миссией или мандатом организации [18].

Вопрос

2

В настоящее время возрастает необходимость защиты данных получателей помощи, внедрения технологий самостоятельной идентификации, чтобы предоставить получателям помощи больше автономии в управлении и владении своими данными, а также уменьшения объемов конфиденциальных данных, хранящихся в централизованных базах данных. Ввиду перечисленного, как гуманитарные организации должны адаптировать свои системы и практику управления данными получателей помощи для обеспечения ответственной интеграции цифровых идентификационных решений?

На сегодняшний день гуманитарные организации, как правило, используют ряд систем управления и хранения данных для сбора и обработки информации о получателях помощи и программах. Действительно, экосистема решений по управлению данными, доступных гуманитарным организациям, является большой и сложной.

Одной из крупнейших систем управления данными в гуманитарном секторе является SCOPE ВПП ООН, в которой в настоящее время хранятся данные более 20 миллионов получателей помощи и которая лицензирована для других НПО. Другой пример – мобильное решение «Последняя миля» компании World Vision, которое используется более чем 20 НПО в 29 странах и содержит данные более 8 миллионов получателей помощи [19] [20]. Главный вопрос, с которым сталкиваются гуманитарные организации, изучающие возможность использования решений для цифровой идентификации, заключается в том, как управлять переходом от традиционных систем хранения и управления данными, таких как решения для управления информацией о получателях помощи, к решениям для цифровой идентификации.

Рекомендация 2А

Инвестировать ресурсы в целях продвижения изменения внутренней культуры для обеспечения долгосрочного успеха.

Несколько опрошенных использовали термин «вызов культуры» для описания трудностей перехода от одной парадигмы управления данными к другой [#5] [#7] [#8]. Для гуманитарных организаций важно создать общий язык для обучения сотрудников не только механизмам цифровой трансформации, но и ее причинам [#6] [#7] [#9]. Сотрудники должны участвовать в процессе перехода и воспринимать его как неотъемлемую часть выполнения своей работы. Гуманитарным организациям, которые так заинтересованы в распределении помощи для смягчения кризисов, часто бывает трудно оправдать инвестиции в то, что может рассматриваться как системы и процессы бэк-офиса. Тем не менее, как отметили несколько респондентов, именно функционирование (или нефункционирование) этих процессов часто определяет успех или неудачу программы [#6] [#7] [#9]. Поэтому лидеры цифровой трансформации в гуманитарных организациях должны воспринимать обучение и изменение внутренней культуры как часть своей роли. Изменение культуры – это медленный процесс, требующий изменения повседневных привычек и организационных процессов, а также значительных предварительных инвестиций.

Критически важным для изменения культуры является пересмотр существующих практик и протоколов управления данными. Несколько респондентов отметили, что переход от традиционных систем управления данными к решениям для цифровой идентификации часто является скорее вопросом изменения практики управления данными, чем технологическими изменениями. Наибольшая сложность при внедрении ответственных соглашений об обмене данными и протоколов управления заключается в обучении специалистов, занятых в сфере гуманитарной помощи: как и многие другие современные специалисты, они зачастую не имеют полного понимания, а тем более навыков управления своими собственными данными, а тем более их защиты.

Наибольшая сложность при внедрении ответственных соглашений об обмене данными и протоколов управления заключается в обучении специалистов, занятых в сфере гуманитарной помощи: как и многие другие современные специалисты, они зачастую не имеют полного понимания, а тем более навыков управления своими собственными данными, а тем более их защиты.

[#10] [#11]. Отсутствие понимания привело к случаям, когда организации доверяют чужим данным больше, чем своим собственным, потому что «мы знаем, какие оговорки и ограничения есть в наших данных, и предполагаем, что другие работают по более высоким стандартам, чем мы» [#8].

Эксперты отметили, что для перехода от управления данными о получателях помощи к системам цифровой идентификации необходимо решить существующие проблемы, связанные с управлением данными. Некоторые из этих проблем включают изменение исторически сложившегося отношения к обмену и защите данных. «Само собой разумеется», что большинство исторически не приемлет никакой вид обмена данными, учитывая, что часто какое-либо национальное государство или другой субъект стремится получить документ с конфиденциальной информацией, к которой имеет доступ сотрудник [#7]. Один из участников описал это как «постоянную игру в кошки-мышки, чтобы защитить данные, которые у нас есть», и в результате «обмен данными не является естественным для наших сотрудников» [#8]. Поскольку политика защиты данных возлагает бремя ответственности на организации, им необходимо перейти от слов «нет, это слишком конфиденциально, мы не можем этим делиться» к последовательному размышлению о том, как выглядит передовой опыт: цель и объем обмена, сроки доступа, хранения и удаления данных, а также дополнительные расходы, связанные с этими усилиями [#8].

Гуманитарные организации должны сделать значительные предварительные инвестиции в определение того, как должна измениться их практика управления данными, затем приступить к обеспечению внутренней поддержки для изменения культуры, а затем внедрить ее. Внедрение технологического перехода часто является самой простой частью организационных изменений, требующих широкой поддержки и принятия. Однако следует отметить, что путь к подлинному изменению культуры во многом зависит от особенностей конкретной организации. Однако, подобно выработке политической воли, шаги, которые организация может предпринять для более глубокого изменения культуры, могут включать в себя обязательное использование определенной технологии, если определенная программа имеет право на финансирование, вступление в соответствующие торговые и продвигающие организации и создание внутреннего диалога, тесно увязывающего инновации с программной миссией организации.

Рекомендация 2В

Заранее инвестируйте ресурсы в укрепление собственных технических знаний.

Центральное место в этом переходе занимает повышение технической грамотности имеющих сотрудников. Этот процесс может быть долгим и трудным, особенно когда у сотрудников множество конкурирующих приоритетов. Для одной организации потребовалось 2-3 года внедрения программ обучения и стратегических внутренних коммуникационных кампаний, прежде чем ей удалось добиться того, чтобы любая инициатива, касающаяся данных, была сформулирована на едином языке, знакомом и понятном всем. Представитель признал, что эта работа «никогда не будет закончена, но, по крайней мере, на уровне ключевых лиц, принимающих решения, мы уже добились результата, и я не слышу, чтобы много говорили о проблемах с определениями» [#7].

То же самое нельзя сказать о секторе в целом. Поставщики, ученые и практики утверждали, что несогласованность определений и терминологии является серьезным источником трений в партнерских отношениях. Йоханнес Эберт из Gravity был не единственным, кто утверждал, что поиск общего глоссария по цифровой идентификации в гуманитарном секторе – это далеко не проблема второго уровня, а вопрос, который он хотел бы видеть в качестве самого неотложного [#9]. Как показывает проблема с созданием общего глоссария терминов, повышение квалификации технического персонала в области активного технического развития может быть дорогостоящим и трудным процессом.

Тем не менее, некоторые методы повышения квалификации технических специалистов в гуманитарных организациях демонстрируют первые признаки успеха. Австралийский Красный Крест, в дополнение к таким поставщикам, как Тукп, взял на себя эту ответственность с решимостью оправдать доверие, оказанное организации, посредством внедрения гарантии конфиденциальности данных в дизайн их цифровых систем идентификации [#2].

Принцип, лежащий в основе этого подхода, заключается в облегчении задачи обучения получателей помощи, которая в противном случае легла бы на работников гуманитарного сектора. Вместо этого, даже если бы пользователи были готовы поделиться всеми своими данными, их никогда не попросили бы предоставить больше минимальной информации в силу того, как изначально была разработана система цифрового удостоверения личности. Цитируя Аманду Робинсон:

«Как организация, которая не относится к пользователям как к товару, мы просто должны придерживаться этого принципа и сделать его прозрачным для людей, которых мы обслуживаем» [#2]. Тактика, которую применяет другая организация, заключается в переходе от обмена данными к доступу к ним, который в идеале должен быть инициирован самим человеком с помощью биометрического ключа, а через несколько лет – с помощью суверенного идентификатора (SSI)² [#7]. Текущая стратегия заключается в добавлении временных ограничений в соглашения об обмене данными. Однако это противоречит мандату некоторых организаций, таких как УВКБ ООН, которые обязаны архивировать данные. Минимизация данных может быть особенно сложной задачей в контексте гуманитарного реагирования, когда крупная организация по оказанию помощи выполняет координационные функции, в результате чего множество партнеров зависят от данных, которые собирает эта организация – такой сценарий был назван «кошмарным» с точки зрения минимизации сбора и обмена данными [#7].

Поэтому чрезвычайно важно, чтобы гуманитарные организации инвестировали в развитие потенциала сотрудников и внутренней компетенции или находили решения, подобные описанным выше. Однако для небольших организаций нецелесообразно вкладывать значительные средства в развитие собственных технических знаний [#8]. В этом случае будет полезно обучить соответствующих сотрудников, используя широко доступные бесплатные инструменты, чтобы создать хотя бы базовый уровень понимания и знакомства. Хорошим ресурсом для поиска таких инструментов является Linux Foundation [22].

Вопрос

3 Организации по оказанию помощи располагают ограниченными ресурсами. Принятие новых технологий может повлечь за собой барьеры в плане затрат, навыков и ресурсов (обслуживание, поддержка и т.д.). Какие экономические стимулы и устойчивые бизнес-модели для использования технологии цифровых идентификаторов применимы к гуманитарным организациям?

Многим гуманитарным организациям постоянно приходится балансировать между сбором средств и выделением их на достойные программы, поэтому они постоянно сталкиваются с дилеммой финансирования. В этом сонме обязательств гуманитарным организациям часто бывает трудно обосновать инвестиции в технологии, которые в основном относятся к операциям бэк-офиса. Не имея прямой связи с распределением помощи получателям, гуманитарные организации с трудом привлекают необходимые средства для разработки таких систем, как решения для цифровой идентификации нового поколения. Верно и то, что переход на новые технологии часто требует дополнительных инвестиций в повышение квалификации персонала и разработку технологий обслуживания. Поэтому крайне важно, чтобы гуманитарные организации изучили весь спектр экономических стимулов и устойчивых бизнес-моделей в отношении решений для цифровой идентификации. Общие компоненты затрат на эксплуатацию системы цифровой идентификации включают расходы на человеческие ресурсы, удостоверение личности, центральную ИТ-инфраструктуру, физические помещения, ИТ-инфраструктуру регистрации, информацию, образование и коммуникацию [23].

2. SSI – это «цифровое движение, которое признает, что человек должен информация о собственной личности должна быть в руках самого человека и управление ей должно осуществляться без вмешательства административных органов. SSI позволяет людям взаимодействовать в цифровом мире с той же свободой и способностью к доверию, что и в автономном мире».[21].

Рекомендация 3А

Цифровые системы идентификации являются дорогостоящими и могут получить наилучшее финансирование за счет инвестиций благотворительных организаций и других финансирующих организаций государственного сектора.

Внедрение решений для цифровой идентификации требует больших затрат. Как и в случае со многими другими новыми технологиями, средства, которые необходимо вложить в предварительно затратить на исследования и разработки, а также на адаптацию к конкретным условиям использования, значительно увеличивают объем необходимых инвестиций в решения по цифровой идентификации. Помимо первоначальных затрат, существует также долгосрочная необходимость в инвестициях в наращивание внутреннего потенциала для обеспечения данного перехода [23]. Как сказал один из участников: «Вы обретаеете целый сонм огромных проблем, связанных с процессом, потому что политика разрабатывается на высоком уровне, а ее реализация всегда требует дополнительного рассмотрения, сроков, инвестиций и обсуждений, чтобы убедиться, что у вас есть все необходимые элементы для обеспечения безопасности. Нам потребовалось три года, чтобы перейти от политики защиты данных к практическим рекомендациям, и мы работали на полную мощность» [#7]. Многие участники подчеркнули необходимость инвестирования в изменение культуры и обучение на внутреннем уровне, поскольку функциональность любой политики, связанной с данными, в конечном итоге зависит не от используемой технологии, а от способностей людей, которые ее используют. Сотрудники должны «знать, как ее использовать и применять должным образом, и понимать риски, если они не будут применять ее должным образом» [#7]. Обучение тех, кто управляет системами цифровой идентификации, представляется серьезной проблемой, учитывая, насколько новыми и сложными для понимания являются эти системы даже для тех, кто работает в этой сфере уже много лет, и это постоянные инвестиции, учитывая темпы развития соответствующих технологий и практик.

Существует еще одна проблема, связанная с тем, что надежная защита конфиденциальности во многих системах цифровой идентификации затрудняет их масштабное внедрение. Организации в основном отвергают идею монетизации пользовательских данных, хотя некоторые из них признали, что к ним обращались за консультацией клиенты из частного сектора, чтобы рассмотреть такую возможность. Представители австралийского Красного Креста и генеральный директор компании Тукп признались, что их непоколебимое стремление защищать данные пользователей и даже не собирать их привело к потере возможностей развития бизнеса и партнерства [#2] [#3].

Большинство проектов по цифровой идентификации, с которыми проводились консультации, получали финансирование за счет грантов от крупных доноров или фондов поддержки инноваций. Однако эти источники финансирования могут создавать проблемы для организаций. Донорское финансирование может сопровождаться такими условиями, как запрос списков участников программы, что может поставить под угрозу обязательства организации по обеспечению защиты данных пользователей [#8]. Более того, некоторые респонденты отметили, что донорское финансирование таких инноваций, как цифровая идентификация, было недостаточным, поскольку они, как правило, финансировали только одну часть процесса, а не весь процесс. Как отметил один из членов Кенийского Красного Креста: «Если вы собираетесь финансировать инновации, то финансируйте весь процесс, чтобы мы могли получить работоспособное решение в результате его применения» [#12]. Далее респонденты отметили, что расходы на систему цифровой идентификации должны взять на себя доноры и субъекты частного сектора, которым выгодно ее создание, как это делают финансовые учреждения и операторы мобильной связи в любой ситуации, когда денежные средства поступают в систему.

Рекомендация 3В

Обратитесь к другим отраслям, чтобы оправдать первоначальные затраты на инвестиции в решения по цифровой идентификации с учетом долгосрочного повышения эффективности и сокращения расходов.

Существует также вероятность того, что повышение эффективности за счет масштабирования решений для цифровой идентификации в параллельных областях снизит затраты на их внедрение в таких секторах, как гуманитарный сектор, в долгосрочной перспективе. Интерес к применению решений для цифровой идентификации в целях решения традиционных задач управления идентификацией и доступом, а также нишевых вариантов использования, таких как вакцинация Covid-19 и тестирование удостоверений личности, может помочь снизить стоимость внедрения решений для цифровой идентификации [25]. Даже гуманитарные организации, которые в течение нескольких лет разрабатывали свои собственные системы цифровой идентификации, признали, что финансирование дальнейшего развития этих систем должно осуществляться из средств, не относящихся к гуманитарному сектору, поскольку создать самостоятельный бизнес в гуманитарной сфере непросто [#4].

В то время как дальнейшее развитие, скорее всего, будет проводиться на средства грантов на инновации или внедрение инноваций, продвижение стимулируют крупные донорские организации, более вероятно, что системы цифровой идентификации будут совершенствоваться субъектами частного сектора, вероятно, для различных областей применения. Многие участники интервью из гуманитарного сектора признали, что сейчас пришло время проявить терпение. Они отметили, что в конечном итоге они смогут адаптировать инструменты, разработанные частным сектором, к своим потребностям, а не пытаться создать свои собственные. Как отметил один из респондентов [№1]:

«Мы пытались занять ведущее место в разработке решения для цифровой идентификации и поняли, что, возможно, нам больше не следует занимать это место. Это позволяет по-другому взглянуть на то, как можно финансировать такую деятельность, даже если это означает, что вам, возможно, придется немного подождать, пока появится подходящее решение. Тем временем мы разобрались с финансированием для управления информацией, потому что мы просто используем набор документов с открытым исходным кодом, например, Open Data Kit для KoVo».

Рекомендация 3С

Там, где это возможно и целесообразно, используйте гранты на внедрение инновационных технологий в целях обеспечения финансирования для лицензирования программного обеспечения как услуги, а не единичные гранты на развитие инноваций.

Несколько респондентов посоветовали гуманитарным организациям финансировать разработку решений по цифровой идентификации за счет грантов на внедрение. Программные гранты, которые зачастую намного больше, чем бюджеты на инновации, и имеют больше возможностей для изменения бюджетов по мере необходимости, могут обеспечить объем, необходимый для разработки и внедрения решений по цифровой идентификации в масштабе [#4]. Более того, несколько источников отметили, что структурирование этих инвестиций в виде услуг может облегчить долгосрочные проблемы финансирования и внедрения решений в области цифровой идентификации. Пример такой возможности финансирования в виде программного обеспечения как услуги (SaaS) был приведен поставщиками и организациями по оказанию помощи [#7]. Австралийский Красный Крест рассматривает модель многоуровневой подписки, при которой другие некоммерческие организации платят за доступ к базе данных учетных данных волонтеров. Генеральный директор Тукп Джимми Снук также был воодушевлен потенциалом ценообразования SaaS, когда ценность, создаваемая при верификации людей, может быть использована внешними поставщиками услуг в том смысле, что поставщики финансовых услуг или мобильной связи будут оплачивать расходы на верификацию. Модель SaaS может принести тройную выгоду: поставщики услуг получают новую клиентскую базу, получатели помощи получают несколько более высокую степень социально-экономической интеграции, а организации по оказанию помощи могут использовать и расширять систему без необходимости покрывать расходы на исследования и разработки [#3].

Вопрос

4

Что представляет собой операционная совместимость между гуманитарными организациями, использующими цифровые идентификаторы? При ответе на этот вопрос следует изучить функциональную совместимость данных независимо от технологий, используемых для их сбора и хранения (например, цифровые удостоверения, выданные различными технологиями цифровых удостоверений личности, но использующие такие стандарты, как децентрализованные идентификаторы, проверяемые удостоверения и т.д.), а также процессы и готовность обмена данными между организациями для предотвращения дублирования.

Обеспечение операционного взаимодействия является критической задачей при разработке любой цифровой инфраструктуры. Корпорация MITRE, американская некоммерческая организация, управляющая центрами исследований и разработок, финансируемых из федерального бюджета, определяет операционное взаимодействие как «способность использовать ресурсы из разных источников так, как будто они были разработаны как части единой системы» [26]. Некоторые традиционные технологические системы, такие как электронная почта и https, способствуют созданию крупномасштабных открытых экосистем, в которых пользователи могут подключаться к различным провайдерам, сервисам и другим пользователям с помощью совместимого формата обмена данными и переносимости данных.

Переход к решениям цифровой идентификации осуществляется в нескольких отраслях, поскольку пользователи начинают требовать более совершенных форм управления данными, которые защитят их конфиденциальность и повысят безопасность их данных. Аналогичным образом, по мере того как организации видят сокращение затрат в результате внедрения решений для цифровой идентификации, все большее их число начинает инвестировать в разработку открытых стандартов и рамок для обеспечения совместимости. По мере того как экосистема сходит на моделях операционной совместимости, гуманитарные организации, инвестирующие в разработку решений для цифровой идентификации, начинают изучать вопрос о том, как они могут обеспечить операционную совместимость между гуманитарными организациями. Для гуманитарных организаций обеспечение эффективной технической совместимости может означать возможность расширения спектра услуг для получателей помощи, а также потенциальную возможность использования гуманитарных учетных данных для получения доступа к услугам в других секторах.

Исключительно важно, чтобы операционная совместимость в рамках гуманитарных организаций также распространялась на различные заинтересованные стороны, с которыми гуманитарные организации взаимодействуют в ходе реализации программ, включая, в частности, финансовые институты, поставщиков телекоммуникационных услуг, организации гражданского общества и общественные организации. Потребность в операционной совместимости в гуманитарном секторе стоит особенно остро. Несколько организаций могут одновременно испытывать потребность в одних и тех же данных о получателях помощи. Если единая регистрация позволит обмениваться данными о получателях помощи между гуманитарными организациями, это позволит сэкономить время и деньги организаций, избавив получателей помощи от потенциальных проблем [#2] [#13] (или просто затрат времени и сил), связанных с процессами регистрации.

Рекомендация 4А

Обратитесь к открытым стандартам операционной совместимости, обмена данными и переносимости данных, разрабатываемым в других секторах, чтобы перейти к созданию открытой, операционно совместимой экосистемы

Вполне вероятно, что по мере разработки моделей операционной совместимости за пределами гуманитарного сектора гуманитарные организации могут начать перенимать открытые форматы данных и шаблоны из других секторов. Однако стоит отметить, что существует несколько проблем, препятствующих обеспечению долгосрочной операционной совместимости в гуманитарном секторе. К ним относятся:

- финансовые стимулы и конкуренция, которые касаются различных потребностей гуманитарных организаций в плане доступа к информации о получателях помощи [#7][#8]
- необходимые культурные изменения
- общее недоверие к качеству данных
- сложности, связанные с доверием пользователей в условиях, когда им часто не хватает цифровой грамотности.

Рекомендация 4В

Укреплять политическую волю на уровне секторов для обеспечения эффективности операционной совместимости.

Достижение технологической операционной совместимости зачастую является скорее вопросом политической воли, чем технической осуществимости. Привлечение необходимого интереса к операционной совместимости среди ключевых заинтересованных сторон имеет большое значение для достижения серьезного уровня операционной совместимости в гуманитарном секторе. Кроме того, организациям требуются различные виды информации о получателях помощи, поэтому назначение одной организации для регистрации получателей помощи, которые будут получать услуги от нескольких организаций, потребует больших предварительных вложений времени и усилий для координации потребностей всех партнеров [#7] [#8].

Тем не менее, в долгосрочной перспективе операционная совместимость может дать гуманитарным организациям значительные преимущества. Решения в сфере цифровой идентификации помогут обеспечить операционную совместимость как в рамках деятельности одной гуманитарной организации, так и нескольких. Вместо того, чтобы дублировать данные по несколько раз для интеграции усилий нескольких организаций, системы цифровой идентификации могут обеспечить интегрированный доступ к данным и программным операциям в режиме реального времени. Такая интеграция значительно расширит возможности гуманитарных организаций по оказанию помощи и тем самым поможет им выполнить свою миссию.

Вопрос

5 Перспективы самостоятельной идентификации зависят от нескольких факторов: цифровой грамотности конечных пользователей, степени развитости инфраструктуры и доступности средств связи, таких как смартфон. Такие факторы являются барьерами в местах, где потенциальные получатели помощи могут быть одними из самых уязвимых групп населения. Как гуманитарные организации могут внедрять технологии цифрового удостоверения личности в условиях низкой доступности связи?

Одной из самых больших проблем при внедрении решений по цифровой идентификации в гуманитарных ситуациях является отсутствие надежной связи. Несмотря на то, что поставщики технологий в этой области предлагают несколько обходных путей, включая использование QR-кодов и бумажных удостоверений личности в качестве резервной копии цифровых систем [#3] [#9] [#14], некоторые ключевые функции, выполняемые решениями для цифровых удостоверений личности, все же требуют доступа к стабильному соединению. Например, для выполнения дедупликации многие решения для цифровых идентификаторов требуют доступа к стабильному интернет-соединению. Однако некоторые функции системы цифровой идентификации можно выполнять и без стабильного соединения [27].

Рекомендация 5А

В условиях низкого уровня охвата связью используйте аналоговые механизмы защиты от сбоев в целях облегчения аутентификации на местном уровне без устройств связи.

Получатели гуманитарной помощи часто не имеют доступа к устойчивой связи или техническому устройству, такому как смартфон, телефон или планшет. Во многих гуманитарных ситуациях получатели помощи, не имеющие стационарных телефонов, берут чужие телефоны, если им нужно связаться с кем-либо, в том числе с гуманитарными организациями. Несмотря на эти проблемы, гуманитарные организации могут внедрять системы цифровой идентификации в условиях низкого охвата связью. Некоторые поставщики исследуют частичные обходные пути решения проблемы отсутствия связи. Кэшируя данные на местном уровне и синхронизируя их с другими узлами хранения, когда локальное устройство подключается к стабильной среде, эти решения могут поддерживать функциональный и цикл идентификации при отсутствии полного и регулярного доступа к стабильной связи [#3] [#9] [#14].

Чтобы сохранить контроль над своей информацией в условиях низкого охвата связью, получатели помощи могут использовать общие цифровые кошельки [#3] [#9]. Храня несколько кошельков на одном общем устройстве с уникальными механизмами доступа для каждого пользователя, несколько пользователей могут получить удаленный доступ к своим учетным данным. Тем не менее, работа нескольких видов цифровых кошельков зависит от наличия смартфона, которого у многих получателей гуманитарной помощи нет. В этих случаях использование аналоговых механизмов аутентификации может поддержать цикл идентификации при отсутствии устройства связи. Например, штрих-код на бумаге может позволить получателю помощи идентифицировать свою личность в месте, где осуществляется взаимодействие, и получить доступ к своим учетным данным на локальном устройстве, находящемся в гуманитарной организации [#3] [#9].

Рекомендация 5В

В условиях низкого охвата услугам связи управление данными по доверенности может помочь в идентификации личности при отсутствии персональных устройств связи.

В условиях низкого охвата услугами связи помочь могут также управление данными по доверенности и кошельки, размещенные по доверенности. Управление данными по доверенности - это процесс, при котором один пользователь берет на себя ответственность за управление учетными данными другого пользователя [#3]. Например: пожилой или молодой человек или человек, не имеющий собственного телефона или временно потерявший SIM-карту, может поручить управление своими данными доверенному лицу-посреднику, например, члену семьи. Разнообразные технологические подходы могут обеспечить ориентированную на пользователя управление информацией по доверенности. Например, биометрические данные или голосовая аутентификация могут быть использованы для предоставления пользователю контроля над его информацией на устройстве доверенного лица в момент взаимодействия [#3] [#9] [#14]. Другие механизмы облегчения ориентированного на пользователя опекуинства включают использование разделенных ключей [#1] [#9]. Разделив ключ между тремя или более получателями, а затем восстановив единый ключ в момент взаимодействия, получатель помощи может контролировать свои данные на различных устройствах, принадлежащих другим людям.

Вопрос

6 Существует противоречие между желанием отдельных лиц сохранить контроль над собственными данными (децентрализация хранения данных и контроля получателям помощи над ними) и желанием организации использовать данные отдельных лиц в целях координации (чтобы избежать дублирования и мошенничества) и подотчетности перед донорскими организациями (чтобы продемонстрировать, что помощь оказывается реальным людям). Каковы компромиссы, связанные с разрешением этого противоречия? Как можно найти баланс? Каких подводных камней следует избегать?

Возможно, основным противоречием при внедрении решений по цифровой идентификации является противоречие между индивидуальным и организационным контролем. Концепция самодостаточной идентичности основана на вере в независимость личности при обеспечении контроля над своей информацией. Цифровой мир далек от независимости. Интернет основан на федеративной модели владения данными, в которой пользователи подтверждают свою личность через посредника. Концепция независимой самоидентификации призвана перевернуть эту парадигму, передав контроль над личной информацией в руки человека. В то время как многие потребители требуют более ориентированных на пользователя моделей управления данными, организации продолжают утверждать, что для предоставления эффективных, оптимизированных услуг они должны обрабатывать данные частных лиц. Основное противоречие движения за независимость цифровой идентичности является в этом смысле основным противоречием цифровых технологий в целом.

Рекомендация 6А

Гуманитарные организации должны признать, что правильно внедренные решения по цифровой идентификации могут улучшить организационные процессы, одновременно предоставляя получателям помощи возможность усиленного контроля над своей их информацией.

В Цифровые решения по идентификации личности могут обеспечить гуманитарным организациям доступ к стандартизированным и проверенным идентификационным данным и возможность осуществлять программные операции в нескольких различных организациях. Возможно, что более важно, цифровые решения для идентификации личности могут также упорядочить процедуру регистрацию внутри организации и повысить ее эффективность.

Однако эти преимущества могут быть реализованы только путем переговоров относительно других организационных приоритетов и соображений, таких как предоставление получателям помощи доступа и контроля над их данными. В настоящее время получатели помощи имеют лишь минимальный контроль над своей информацией, если вообще его имеют. Один из экспертов Красного Креста по экспериментальному использованию инструментов цифровой идентификации отметил, что несмотря на то, что получатели помощи могут сами вводить свои данные, они не могут определить, какая информация о них будет передана тем или иным организациям [#12].

Таким образом, решения по цифровой идентификации могут облегчить организационные процессы, одновременно повышая качество индивидуального опыта получателей помощи.

Рекомендация 6В

Обучение как получателей помощи, так и гуманитарных организаций в целях достижения согласия и повышения эффективности систем.

Однако, будут ли применены на практике вышеуказанные преимущества зависит от того, будут ли согласны получатели гуманитарной помощи использовать инструменты цифровой идентификации. В программах, применяющих новые технологии, такие как цифровые идентификационные решения, заручиться подлинным согласием получателей может быть трудно или даже невозможно. Несколько респондентов отметили, что, помимо того, что многие получатели гуманитарной помощи не обладают базовой цифровой грамотностью, отмечается также неравномерность с точки зрения распределения власти между теми, кто оказывает и получает помощь, что во многих случаях осложняет взаимодействие [#6] [#9] [#12]. Несколько респондентов отметили, что гуманитарные организации обязаны встроить в разработку систем цифровой идентификации механизмы защиты, чтобы они по своей сути минимизировали и защищали информацию пользователей, чтобы в случае согласия пользователей на использование цифровой идентификации их информация была максимально защищена [#2] [#10].

Как отмечается в документе, опубликованном Mozilla Foundation, «инструменты цифровой идентификации должны быть разработаны с самого начала, чтобы предотвратить их использование в качестве инструмента для обеспечения и усиления отслеживания со стороны государства и частных лиц. Страны должны критически изучить вопрос о том, нужно ли вообще регистрировать запросы на аутентификацию, и, безусловно, ввести в действие законы, ограничивающие хранение, доступ и обмен записями, фиксирующими процесса идентификации [28].

Для того чтобы получатели не только понимали, на что они соглашаются, но и были заинтересованы в успехе программы, необходимо сделать решения по цифровой идентификации полезными для них. Документально подтверждено, что беженцы и перемещенные лица прибегают к стратегиям сопротивления и игры в рамках процедур и категорий, связанных с оказанием помощи, которые их окружают. Пол Керрион предупреждает, что решения по цифровой идентификации могут устранить многие из этих стратегий сопротивления и усложнить, а не упростить их применение для получателей помощи [#6]. По мнению одного из экспертов по правам и данным, необходимо как минимум обеспечить наличие каналов, которыми затронутые люди действительно могли воспользоваться, чтобы получатели помощи могли претендовать на то, чтобы их рассматривали как законных, равных людей, наделенных равными правами.

В случае применения цифровой идентификации или форм контроля за информацией данные получателей помощи становятся «сферой, в которую можно погружаться, чтобы создавать и собирать информацию ad libitum» [#15]. Это было признано поставщиком Tynk, который утверждал, что пользователи должны иметь возможность с самого начала отказаться от использования решений для цифровой идентификации и сохранять возможность и право удалить свои данные из системы даже после того, как они присоединились к данной системе [#3].

Вопрос

7 Какое обучение грамотности в области данных требуется получателям цифровых идентификаторов для того, чтобы они могли безопасно ими пользоваться? В чем различия этих требований для пользователей смартфонов и телефонов?

Одним из наиболее сложных элементов внедрения решения по цифровой идентификации является обучение пользователей. Для внедрения решения по цифровой идентификации, которое будет полезным для получателей помощи и эффективным для гуманитарных организаций, крайне важно проводить широкие кампании по повышению цифровой грамотности и обучению получателей помощи.

Рекомендация 7А

Рассматривать обучение цифровой грамотности и образование как итеративный, двусторонний процесс.

Цифровые идентификационные решения одновременно являются и бременем, и привилегией для пользователей. Несмотря на то, что они позволяют пользователям управлять своей информацией, они также налагают на них ответственность за контроль собственной информации – не каждый человек, например, сможет принимать обоснованные решения о последствиях передачи своих данных различным типам организаций. Цифровая идентификация также предполагает базовый уровень цифровой, лингвистической и арифметической грамотности, который может не быть широко распространен в гуманитарных контекстах и контекстах развития.

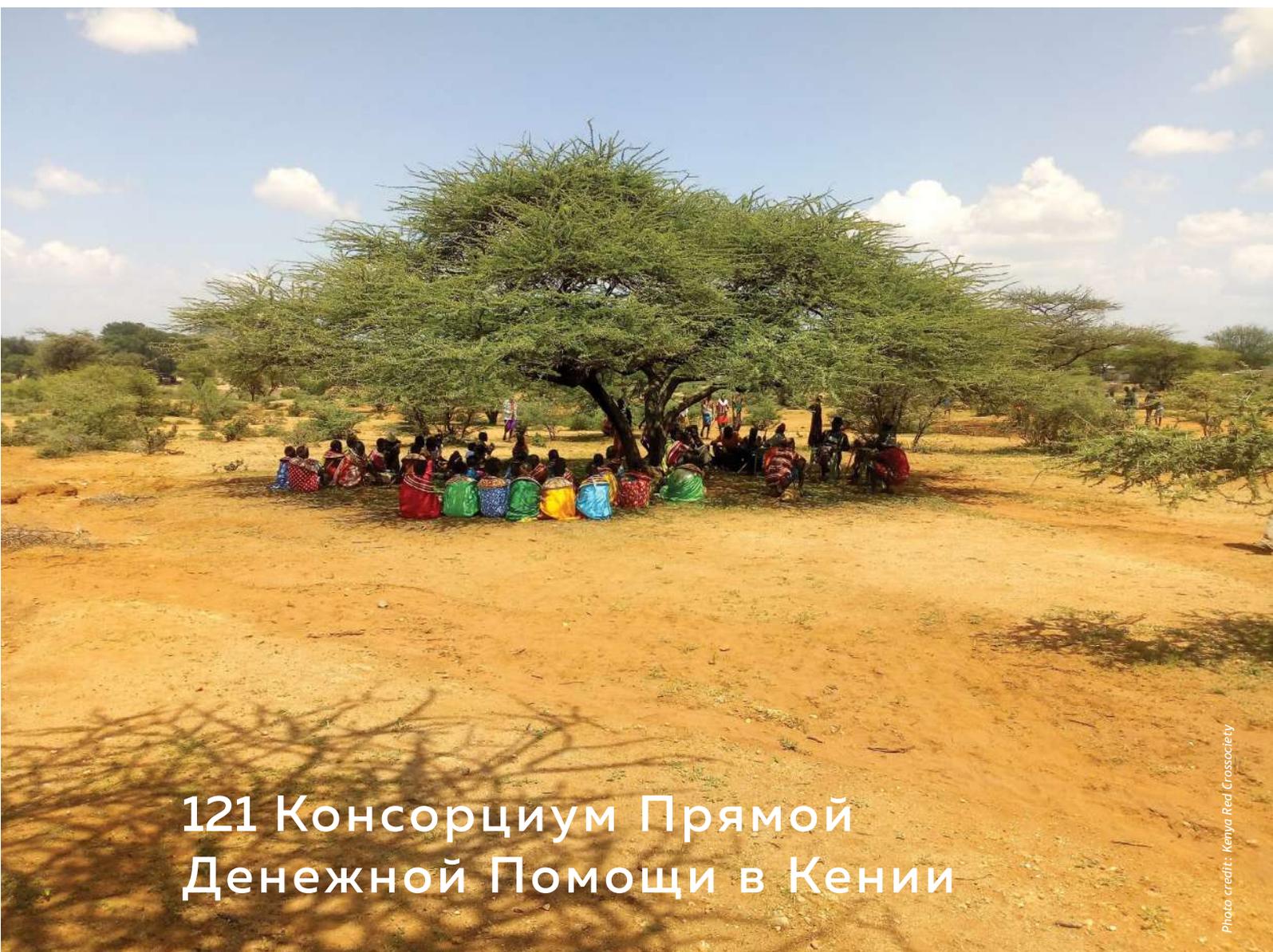
Крайне важно, чтобы обучение было проведено на начальном этапе внедрения цифровой идентификации. Оно должно рассматриваться как двусторонний процесс, в ходе которого пользователи повышают свою цифровую грамотность, а организации узнают, как лучше предоставлять услуги получателям помощи. Вкладывая средства в проектирование, ориентированное на пользователя, поставщики решений могут усовершенствовать и оптимизировать свои решения для местных условий. Например, поставщики Gravity и Tynk используют голосовую аутентификацию вместо трудоемкой аутентификации на основе пароля, чтобы лучше удовлетворить потребности получателей помощи [#3] [#9] [#14]. Аналогичным образом, Нидерландский Красный Крест последовал предложению пожилой женщины из Сен-Мартена, которая пожаловалась на то, что системы управления данными, которой она пользовалась, не был интуитивно понятен. В ответ на это был разработан механизм самостоятельной оценки уязвимости в стиле чата в WhatsApp, в ходе которой получатели представляют необходимую информацию, отвечая на вопросы чат-ботов. Адаптируя свои решения к потребностям получателей, поставщики услуг могут способствовать внедрению и, следовательно, успеху своих технологий в долгосрочной перспективе. Однако следует отметить, что цифровая грамотность зачастую может являться прикрытием для предоставления услуг. Несколько респондентов предупредили, что предположение о том, что получатели помощи не понимают важность и не озабочены защитой конфиденциальности

своих данных может отражать неокOLONиальную политику [#10] [#11]. По их мнению, гуманитарные организации должны признать, что они обязаны помочь людям понять, что происходит с их данными в случае применения решения по цифровой идентификации. Большинство организаций признают настоятельную необходимость приложить больше сил для просвещения своих сотрудников и пострадавших сообществ. Действительно, есть разница между информированием как процессом, в ходе которого респонденты галочкой заполняют анкеты и созданием у человека ощущения, что он действительно проинформирован. Как отметил один из респондентов: «Я могу сказать, что проинформировал кого-то, но это не значит, что он это понял». В этом заключается разница между информированием и пониманием» [#8].

Рекомендация 7B

Требовать от поставщиков включения процесса обучения в их дорожные карты развития.

Поставщикам технологий следует разрабатывать решения для цифровой идентификации, в которых в интерфейс будут включены приложения для обучения и для получателей помощи. Например, в приложениях должны быть четко объяснены различия в типах данных, если пользователи захотят «узнать больше». Когда от пользователей требуется подтвердить свое согласие, необходимо, чтобы у них была возможность сначала прочитать, что выбор варианта «не делиться данными» будет на практике отражаться на их возможности получения доступа к услугам [#10]. Независимо от того, склонятся ли пользователи к тому, чтобы подтвердить свое согласие или нет, им будет представлено еще одно краткое заявление о последствиях выбранного варианта, и их снова попросят подтвердить свой выбор. Цель этих шагов заключается в том, чтобы в рамках интерфейса донести до пользователя, почему необходимо предпринять какое-то действие. Понятие «информирование/обучение, заложенное в дизайне инструмента» было также поддержано Нидерландским Красным Крестом. По мнению НКК, было бы особенно полезно, если бы самостоятельной регистрации для получения помощи сопутствовала интуитивная ясность административных процессов [#6]. Например, анкеты можно было бы заполнять в формате чата с ботом в WhatsApp. На каждом этапе процесса интерфейс – текстовый или звуковой – должен объяснять, почему от пользователя требуется предоставить конкретную информацию. Действительно, от поставщиков следует требовать, чтобы они включали в свои дорожные карты развития задачу сделать свои решения более интуитивно понятными для получателя помощи.



121 Консорциум Прямой Денежной Помощи в Кении

Photo credit: Kenya Red Cross Society

Обзор

Платформа 121 – это система предоставления прямой денежной помощи, инициированная командой 510 Нидерландского Красного Креста (НКК). Консорциум запустил два пилотных проекта для тестирования платформы: один в Кении, другой – в Нидерландах. В декабре 2020 г. при поддержке GSMA и Фонда ИКЕА был успешно завершён пилотный проект в Кении [29].

Результаты пилотного проекта дают важное представление о вопросах, связанных с использованием цифровых идентификационных систем в условиях низкой доступности связи (особенно в отношении проблем цифровой грамотности и коммуникации с получателями помощи), о недостатках внедрения самостоятельной идентификации (СИ) в гуманитарной сфере, а также о проблемах, связанных с операционной совместимостью и ответственным использованием данных в данном секторе.

Пилотируемая система состоит из двух компонентов: создание цифрового инструмента идентификации и распределение денежных средств. Цель состоит в том, чтобы благодаря цифровой идентификации, которую получатели помощи создают сами, у них была возможность идентифицировать себя в многочисленных гуманитарных организациях. Для достижения этой цели проект был разделен на два направления, одно из которых сосредоточено на дизайне, ориентированном на человека (ДОЧ), а другое – на технологической поддержке.

Технологическое направление включало в себя создание цифрового инструмента идентификации, а также распределение денежной помощи. Были протестированы следующие основные концепции: самостоятельная регистрация, СИ, автоматизированная односторонняя связь через СМС, управление программой распределения денежной помощи и интеграция платформы с М-Pesa. Подготовка началась в апреле 2019 г. и была ориентирована на планируемый запуск пилотного проекта в ноябре 2020 г.

Роли

Партнерские организации поддерживали различные аспекты пилотного проекта. Направление ДОЧ возглавлял НКК /510 при содействии Красного Креста Кении. В рамках этого направления проводились семинары по совместному проектированию с участием пострадавших людей, сотрудников Кенийского и Британского Красного Креста, а также представителей компании Safaricom. В рамках технологического направления было организовано партнерство между НКК/510 и Туqn. Туqn разработала бэкэнд для компонента СИ, а НКК/510 разработал все остальные бэкэнд-системы, фронт-энд и управлял работой по интеграции обеих систем. Disberse была выбрана для поддержки разработки внутренней системы организации денежных потоков, в результате изменений сроков реализации проекта, вызванных глобальной пандемией Covid-19, ИТ-отделы NLRC/510 и Красного Креста Кении вместо этого стали сотрудничать с местным поставщиком финансовых услуг, компанией Africa's Talking [30] в целях распределения денежной помощи. Заинтересованными сторонами в распределении помощи были Кенийский Красный Крест и М-Pesa. Услуги обмена сообщениями были частично интегрированы с Twilio. Для проведения платежей в рамках пилотного проекта была успешно реализована интеграция с М-Pesa посредством привлечения услуг компании Africa's Talking.

Технологии

Структуры, основанные на участии получателей помощи

В ходе пилотного проекта в Кении некоторые пострадавшие имели телефоны, а оборудование Кенийского Красного Креста включало планшеты с динамиками, а также смартфоны. Помощь распределялась через М-Pesa SMS или через их представителей. Технологические компоненты включали самостоятельную регистрацию, связь и SSI. Пользователи могли зарегистрироваться через веб-приложение с низкой пропускной способностью. Благодаря системе в стиле чата WhatsApp пользователи регистрировались и получали информацию о программе помощи на выбранном ими языке. Обращение к пользователям было написано совместно командой по ДОЧ и волонтерами, волонтерами Кенийского Красного Креста и профессиональным копирайтером-специалистом по работе с пользователями (РП). Регистрацию также можно было пройти, прослушав озвученный интерфейс для пользователя; голос интерфейса был записан через сообщение WhatsApp местными волонтерами. Копия всего текста хранилась на платформе Transifex, чтобы его можно было легко перевести, а затем загрузить обратно в систему НКК/510. Это облегчило местным волонтерам задачу по оказанию помощи конечным пользователям в переводе дополнительных аспектов. Изменения РП были внесены в ответ на сообщения о трудностях, с которыми столкнулись пользователи в связи с особенностями дизайна кнопок в интерфейсе – получатели чаще удерживали кнопки после нажатия вместо того, чтобы отпустить их после краткого нажатия.



Source: 121 Product Roadmap, December 2020, p.13



Source: 121 Product Roadmap, December 2020, p. 16

3. В настоящее время переведены на языки туркана, самбуру, арабский и тигринья, планируется перевод на голландский, французский и суахили.

Тукп и ККН/510 заключили техническое партнерство для продвижения программы SSI в гуманитарном секторе путем разработки и интеграции технологии в более широкую платформу 121. Техническая инфраструктура была функциональной, но она не стала более ценной для пострадавших, отчасти из-за ограничений, связанных с низким уровнем распространения смартфонов среди населения и плохого качества подключения к Интернету. В результате возникших трудностей сотрудники платформы 121 пришли к выводу, что Sovrin и SSI в настоящее время не представляют ценности для платформы 121. Цифровые кошельки получателей помощи хранились централизованно, поскольку команда не продолжила разработку децентрализованного хранилища. Использование облачного сервера остается возможным рабочим вариантом, как и использование независимого python-сервера и Sovrin. Тем не менее, было установлено, что ценность SSI состоит в том, что этот инструмент способствует продвижению конфиденциальности и ответственного использования данных, а также способствует введению самостоятельной регистрации, что может значительно сократить время на регистрацию, хотя этот результат не очевиден и зависит от качества инструкций, длительности процесса регистрации и т.д.

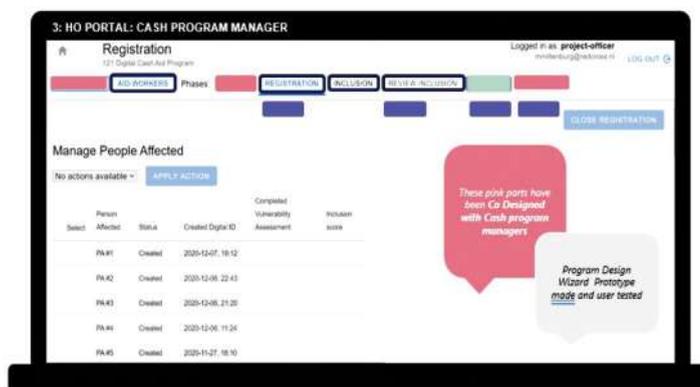
Системы для гуманитарных организаций

Портал для управления информацией о денежных потоках был разработан для обработки массовых регистраций и поддержки работы с конфиденциальными данными. Портал для гуманитарных организаций представляет собой программное решение, доступное через любой браузер. Он позволяет управлять программой помощи наличными от начала до конца, включая общение посредством СМС и WhatsApp и проведение платежей через цифровые ваучеры и M-Pesa.

Платежи можно осуществлять одним нажатием кнопки, хотя обеспечение полной технической регистрации у поставщиков финансовых услуг является сложной задачей. Данная сложность не связана с требованием кодирования или интеграцией интерфейса прикладного программирования (ИПП). Скорее, сложность представляет внедрение процесса обеспечения доступа к контактам и изменения процессов в гуманитарной организации. Аналогичным образом, команда пришла к выводу, что важно иметь возможность распределять наличные деньги в физической форме в тех случаях, когда работа с цифровыми ваучерами или наличными проблематична. Достижение лучшего понимания объема рынка технической интеграции поставщиков финансовых услуг с гуманитарной практикой является ключевым приоритетом на ближайшее будущее.



Source: 121 Product Roadmap, December 2020, p.20



Source: 121 Product Roadmap, December 2020, p.27

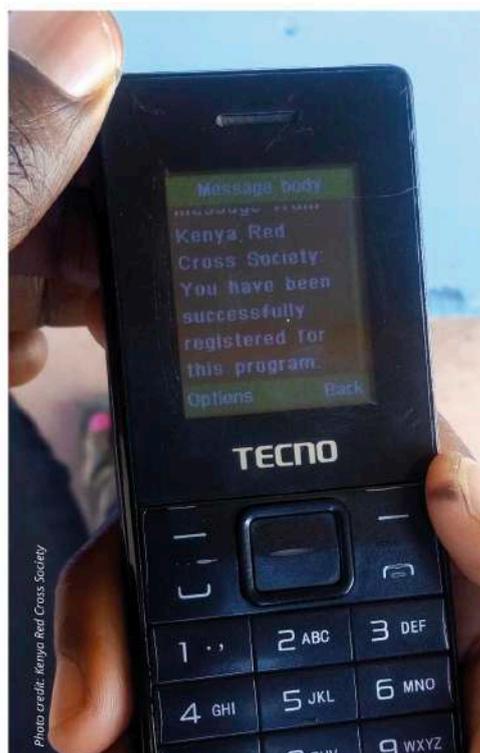
Анализ

На примере Кении показан ряд важных проблем, возникающих в связи с обеспечением операционной совместимости и ответственного подхода к работе с данными в гуманитарной сфере, а также несовместимости систем самостоятельной идентификации и способов преодоления барьеров, возникающих при низком уровне доступности связи.

Многие моменты, затронутые в данном анализе, соответствуют результатам интервью, проведенных с ключевыми заинтересованными сторонами, которые неоднократно подчеркивали, что мощным сдерживающим фактором для внедрения цифровых инструментов идентификации в гуманитарном секторе являются особенностями культуры работы гуманитарных организаций и отсутствие у них цифровой грамотности несмотря на значительные достижения и успехи, достигнутые в развертывании необходимой технической инфраструктуры.

Операционная совместимость и взаимодействие

По результатам работы над различными пилотными проектами НКК/510 заключил, что нельзя сделать вывод о том, что все организации стремятся к цифровой совместимости. Согласно отчету о перспективах НКК/510 на 2021 г., «трудно проверить, захотят ли организации стандартизировать сбор данных в рамках всего сектора». Необходимо также повысить операционную совместимость с поставщиками финансовых услуг, возможно, путем предоставления ими открытых услуг через программируемые интерфейсы. Самой сложной задачей является завоевание доверия. Гуманитарные организации должны принять подтвержденные идентификационные атрибуты, созданные партнерскими организациями. Несмотря на то, что с технологической точки зрения это возможно, организации должны скоординировать свои действия, чтобы операционная совместимость эффективно работала на практике. Как подтвердили участники интервью, значительным препятствием является отсутствие опыта взаимодействия между гуманитарными организациями. Координация необходима не только в отношении регистрации, но и в отношении критериев отбора, объема помощи и так далее. НКК/510 считает, что такие механизмы координации должны быть организованы централизованно и что некоторые функциональные возможности могут быть включены в платформу 121 для поддержки этих механизмов координации. Например, можно было бы обязать получателя помощи предоставить свои записи о получении помощи при регистрации. Это может как снизить вероятность дублирования, так и улучшить координацию и повысить осведомленность организации о предыдущих программах. Такой функционал еще не разработан, поэтому борьба с дублированием данных с помощью СИ является не такой простой задачей. Более того, даже если такой функционал будет разработан, внедрение технологических инструментов не решит всех проблем координации. Организациям все равно придется доверять этой системе, и она будет работать только после того, как будет достигнут сетевой эффект. Как и в случае большинства проблем, связанных с использованием систем цифровых идентификаторов в гуманитарной сфере, социально-политические и технологические проблемы взаимосвязаны.



From 121 project implemented by Kenya Red Cross Society, 510, British Red Cross and Funded by GSMA.

На данный момент СИ не представляет ценности для платформы 121

В конце 2020 года NLRC/510 пришел к выводу, что СИ в настоящее время не представляет ценности для платформы 121. СИ было слишком сложно внедрить, учитывая отсутствие практики ответственного отношения к данным, ограничения, связанные с низкими параметрами связи, и проблемы нормативно-правового регулирования. В ходе ряда пилотных проектов было отмечено, что гуманитарные организации хотят работать с партнерами, знакомыми с пострадавшим населением, или с человеком, который хорошо осведомлен о положении дел, а не принимать идентификационные данные получателей помощи в цифровом формате. Для работы с СИ организациям также придется повысить уровень внутренней цифровой грамотности. Сложно проверить, обладают ли организации, участвующие в той или иной программе, основанной на СИ, достаточной цифровой грамотностью, что порождает неопределенность и подрывает доверие. Это указывает на более широкую проблему цифровой трансформации в секторе, которая отражается в проблемах, связанных с отсутствием практики обеспечения безопасности данных. В настоящее время не существует способа предотвратить сбор и оцифровку избыточных данных. Более того, юридические причины и требования доноров могут вынуждать организации хранить личную информацию в течение определенного срока. Как и другие респонденты, ГКК/510 сообщил о том, что сталкивается с просьбами предоставить гуманитарным организациям доступ к личной информации и даже право на ее скачивание.

Самое главное, неясно, существует ли необходимость в многократной цифровой идентификации. Гуманитарные организации упоминали о преимуществах перехода от функциональных цифровых идентификаторов к более фундаментальным формам идентификации или даже к созданию поведенческих маршрутов для использования в качестве альтернативных форм кредитного скоринга или оценки рисков, чтобы помочь бенефициарам в долгосрочной перспективе, но в настоящее время это не более, чем надежды, поскольку нормативная среда еще не адаптирована для реализации этой цели. Это лишает оснований аргументы в пользу СИ, основанные на понимании ценности многократного цифрового идентификатора. NLRC/510 подтвердил, что для того, чтобы движение за обеспечение конфиденциальности, компонентом которого является стремление к СИ, стало катализатором любых изменений, правительства должны в первую очередь определить обеспечение конфиденциальности данных как свой приоритет и принять соответствующие меры.

Наконец, СИ – инструмент непрактичный, поскольку требует от пользователей хорошего подключения к интернету и (для полного функционала) смартфонов, а также высокой цифровой грамотности – все это маловероятно в условиях, в которых работает большинство гуманитарных организаций. Кроме того, разработка SSI требует значительных ресурсов, а сектор помощи отличается консервативностью. ГКК/510 взял на себя обязательство прекратить работу над СИ, удалив компоненты СИ из существующих систем, и двигаться в сторону централизованного хранения данных и более простых, менее ресурсоемких решений.

Цифровая идентификация в условиях низкого охвата связью и низкого уровня цифровой грамотности

Дизайнерские решения, принятые в рамках проекта, отвечали ограничениям, связанным с низким уровнем подключения. Одним из примеров является система связи в стиле WhatsApp для регистрации и поддержки пользователей. Этот компонент был добавлен специально для ситуаций с высоким уровнем цифровых технологий, но низким уровнем физического доступа, таких как:

- нелегальные мигранты в Нидерландах
- люди, пострадавшие от конфликта в Украине
- люди, пострадавшие после урагана на острове Сен-Мартен.

Другой пример – использование аудиоинтерфейса. Ограниченные возможности подключения к Интернету и низкий уровень проникновения смартфонов также заставили команду отказаться от решения на основе SSI. Партнеры по технологическому треку даже подали заявку на финансирование для разработки решения для мобильных телефонов, но она не увенчалась успехом.

В рамках пилотного проекта в Кении удалось сделать важные выводы о том, как лучше общаться с получателями помощи, не знакомыми с цифровым интерфейсом. Был проведен семинар для того, чтобы помочь пользователям создать и запомнить свои пароли. Понятие пароля может оказаться сложным, а его запоминание может быть особенно трудным для людей, переживших травму.

Среди компонентов интерфейса, которые оказались сложными, были: кнопки в целом (трудно использовать), кнопки "о" в частности (абоненты не используют или плохо понимают функцию кнопки), набор текста, понятия учетных записей и конфиденциальности данных.



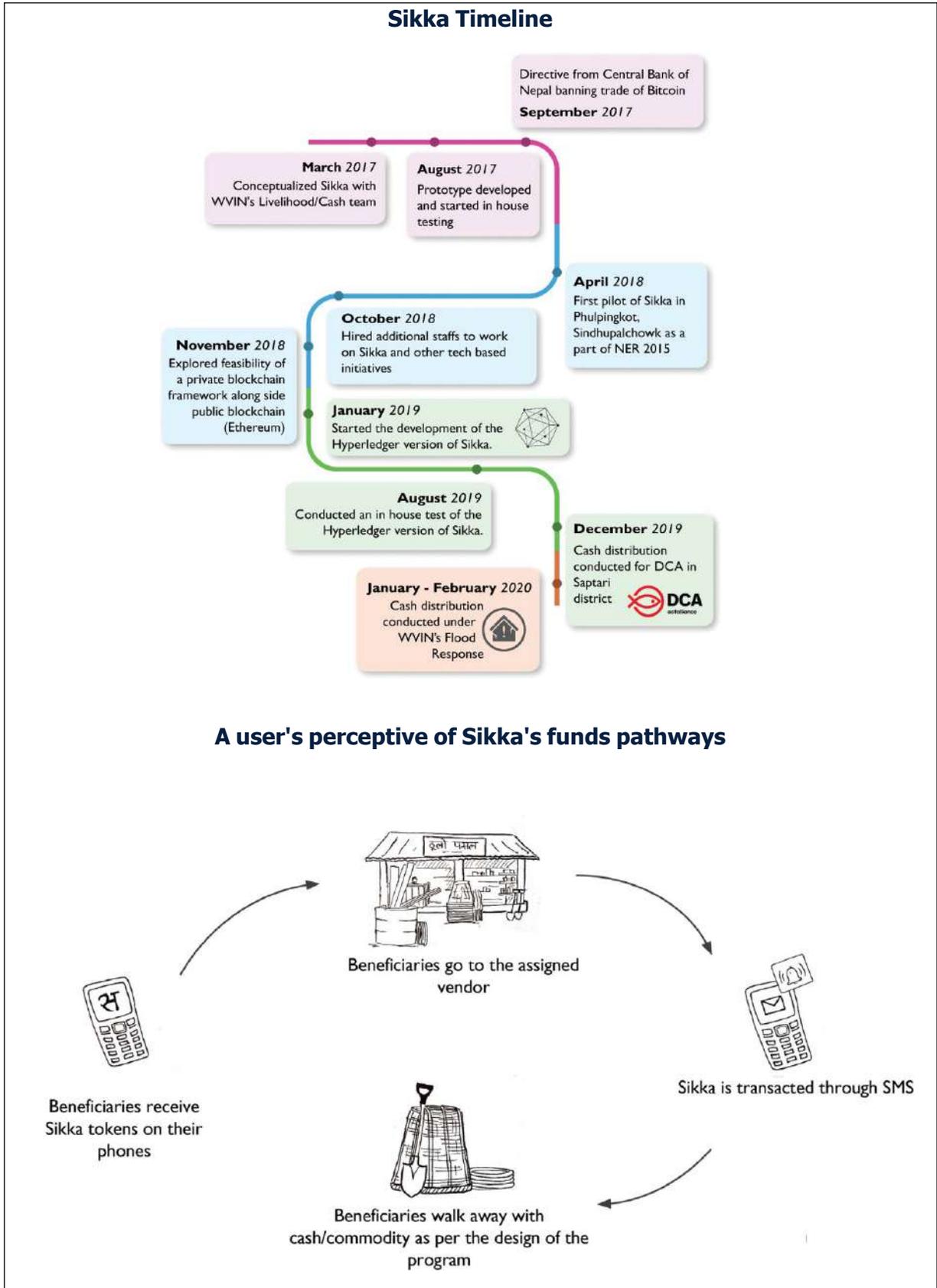
Photo credit: World Vision International

Платформа по передаче цифровых активов компании Sikka на основе Ledger-технологий

Обзор

Sikka, что в переводе с непальского означает «монета», является платформой для передачи цифровых активов. Она была разработана, профинансирована и внедрена непальской инновационной лабораторией World Vision International в Катманду. Платформа решает проблему доступа к финансовой помощи в виде обеспечения наличных денег во время кризисов с опорой на технологию блокчейн и цифровые токены. В ситуациях реагирования на стихийные бедствия применение мануальных процессов перевода наличных денег приводят к логистическим осложнениям, операционным расходам и не являются полностью прозрачными. Эти проблемы усугубляются отсутствием инфраструктуры и услуг в сельских районах. Технология блокчейн позволяет осуществлять цифровые транзакции с использованием токенов через сотовые сети. Пользователи могут безопасно получать доступ к наличным деньгам или товарам через цифровые кошельки, которые они получают при регистрации. Кошельки привязаны к номеру мобильного телефона, который служит идентификатором пользователя в блокчейне Ethereum (который имеет один узел и одну контролируемую организацию). Sikka не внедряет собственную систему управления идентификацией. Данное решение носит местный характер, основано на принципе дизайна, ориентированного на человека, и разработано с учетом имеющихся знаний конечного пользователя и доступных технологий:

SMS-функционал, совместимый с любым базовым функциональным телефоном и сценарием с низким уровнем подключения. В дополнение к таким ценностям, как доступность и устойчивость сети, Sikka делает акцент на подотчетности, поскольку каждый перевод между получателями помощи, поставщиками услуг и кооперативами происходит через неизменные журналы транзакций. Приведенные ниже рисунки иллюстрируют, на каком уровне развития находится Sikka и как она работает. С 2020 г. решение Sikka было предложено в ответ на пандемию Covid-19 [31]. Будущие разработки включают в себя изучение возможности создания нового стандарта токенов, версии Sikka для гиперлэджера и внедрение существующего процесса проверки личности на основе блокчейна.



Роли

Функционал Sikka встроен в экосистему участников процесса оказания помощи. Система описывается как сеть передачи цифровых активов, поскольку токены могут представлять права доступа к различным товарам. Токен будет иметь ценность только в рамках взаимодействия между организацией, оказывающей помощь, получателями помощи, поставщиками услуг и/или финансовыми кооперативами, и эти участники отвечают за определение стоимости токена. Очень важно, что Sikka сотрудничает с местными поставщиками услуг и поставщиками финансовых услуг, чтобы уменьшить хлопоты в случаях, когда получателям услуг приходится преодолевать большие расстояния, чтобы получить поддержку. Для регистрации и управления идентификационными данными получателей помощи Sikka опирается на партнерские НПО, которые используют свои собственные существующие процессы. Между разработкой и финансированием системы через World Vision International, передачей этих процессов на исполнение третьим лицам, партнерством с местными финансовыми организациями, развертыванием своего токен-контракта в основной сети Ethereum и запуском системы через смс и, таким образом, через операторов мобильной связи, для функционирования системы Sikka не требуется никакой дополнительной внешней поддержки. Тем не менее, Sikka работает с финансовыми кооперативами в Непале, чтобы помочь им решить проблему высокого риска ликвидности, который часто мешает им работать с гуманитарными или благотворительными организациями. Как объяснил координатор проекта Суджанья Ачарья, «отслеживая активы посредством применения книги бухгалтерского учета, Sikka обеспечивает основу, на базе которой могут быть реализованы некоторые основные функции банковского программного обеспечения для оцифровки процессов и записей, что [способствует укреплению доверия между сторонами]». Sikka также изучает возможность использования инфраструктуры Infura в качестве альтернативы поддержанию собственного узла. Что касается финансирования, Sikka «полностью принадлежит World Vision International и проводит собственный сбор средств традиционными методами в соответствии с установленными правилами и политикой организации» [32]; по этим причинам она никогда не будет работать на основе первичного размещения монет (ПРМ).

Технологии

На основе Ethereum

Sikka работает через единую контролируемую организацию в основной сети Ethereum в целях управления созданием, распределением и подтверждением транзакций в рамках программы помощи. Токен представляет собой контракт ERC20 (Ethereum Request for Comments 20). Поскольку токены могут представлять права доступа к различным товарам, Sikka может использоваться для представления любой валюты или цифрового актива, привязанного к товарам (таким как литр масла, мешок риса или строительные материалы), отвечающим потребностям, определенным организациями по оказанию помощи, получателями помощи, поставщиками услуг или финансовыми кооперативами, принимающими участие в данной ситуации. Токены не являются криптовалютой; их стоимость определяется экосистемой участников. Пользователи проводят операции через свои кошельки Sikka, которые привязаны к номерам мобильных телефонов и получены при регистрации. Номера мобильных телефонов служат идентификатором пользователя в блокчейне. Затем токены Sikka отправляются по SMS для покупки товаров, услуг или обмена токенов в виде электронных ваучеров на наличные или в местном финансовом кооперативе. Каждый раз, когда пользователь совершает транзакцию по смс-сообщению, в блокчейне запускается транзакция. После завершения транзакции пользователь получает подтверждение в смс.



Функционал цифрового удостоверения личности

Не имея собственной системы управления идентификацией, Sikka полагается на партнерские НПО для регистрации и учета своих получателей помощи. Это решение основано на сложном и деликатном характере внедрения решения по цифровой идентификации. В ближайшее время Sikka может работать с существующим решением, которое «может включать процесс удостоверения личности на основе блокчейна» [32]. В 2018 г. был разработан ППИ, позволяющий существующим системам управления данными получателей помощи напрямую подключить Sikka к такой системе. Цель данного функционала – позволить агентствам по оказанию помощи включить Sikka в качестве варианта оплаты «последней мили» в существующую систему управления идентификацией. ППИ работает с 2019 г., поддерживая выдачу токенов и получение данных о транзакциях.

Безопасность

Sikka пользуется решениями для обеспечения безопасности хешрейта Ethereum и поэтому не нуждается в создании собственной сети защиты конфиденциальности. Токены на блокчейне пользуются преимуществами криптографической безопасности, включая устойчивость к подделке и элемент прозрачности и проверяемости транзакций [33]. Цифровые кошельки хранятся на серверах Sikka и связаны с SIM-картой пользователя таким образом, что доступ к средствам возможен только через поставщиков сети или утвержденные финансовые кооперативы. Команда обязуется следовать отраслевым стандартам безопасности для веб-приложений, постоянно пересматривать их и внедрять обновления. Данные резервируются; с самого начала Sikka следует принципу минимизации данных, так что никакая ненужная идентифицируемая личная информация пользователя не хранится на их серверах или где-либо на блокчейне [34]. Практика обмена данными с системами партнеров отражает эту цель: список телефонных номеров получателей помощи передаются вместе с необязательным уникальным идентификатором для облегчения создания отчетов.

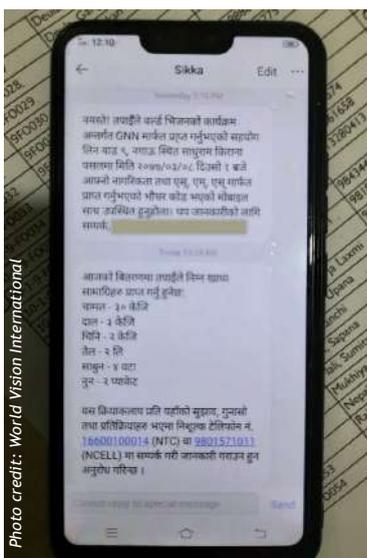


Рис. 1: Сообщения с отчетностью о гуманитарной деятельности



Рис. 2: Код ваучера, направленный в смс Sikka по телефону с необходимым функционалом



Рис. 3: Получатель помощи читает сообщение sikka с подробной информацией о распределении помощи

Нет Дарр или ICO

Sikka не является приложением (Dapp), и команда не стремится к этому в будущем, поскольку не считает это актуальным, учитывая текущую постановку задачи. Аналитик по поддержке блокчейна UNOPS Джеф Дэвис также подтвердил, что Sikka никогда не будет проводить ICO, поскольку этот процесс предназначен для того, чтобы инвесторы могли получить прибыль от стоимости токена, используемого в приложении. Токены Sikka сами по себе не являются рыночными товарами, и нет необходимости в таких токенах для удовлетворения потребностей, решению которых служит Sikka.

Технологические характеристики в стадии разработки

Команда Sikka изучает процесс проверки личности на основе блокчейна, внедряет новый стандарт токенов, изучает альтернативную инфраструктуру вместо поддержания собственного узла, а также разрабатывает версию Sikka для hyperledger. Новый стандарт токенов определен в ERC865 и поможет снизить транзакционные издержки для токенов Sikka. Этот стандарт позволяет третьей стороне осуществлять транзакции от имени отправителя, что означает отсутствие необходимости предоставлять кошельки получателей с Ethereum для осуществления отдельных транзакций. Снижение затрат также возможно, если Sikka будет использовать инфраструктуру Infura; это позволит сократить расходы, связанные с обслуживанием собственного узла и сервера. Хотя снижение затрат может быть отдельной целью, Sikka удалось сократить расходы на одного получателя помощи на 78.5% в ходе пилотного проекта 2019 г.. Также в стадии разработки находится версия Sikka для hyperledger, которая будет работать в тандеме с текущей версией Ethereum; это должно позволить учреждениям открыто использовать систему ваучеров Sikka при работе в странах, где существует строгая политика в отношении блокчейна и криптовалют. Хотя токены Sikka не являются криптовалютой, «газ-сборы», связанные с их использованием, потребуют проведения платежей в Ethereum, что может заблокировать возможность использовать Sikka как вариант для агентств по оказанию помощи, работающих в нормативно-правовой среде, которая не поддерживает транзакции на основе блокчейна или криптовалюты.

Анализ

Sikka является интересным примером использования цифрового идентификатора, поскольку он представляет собой высокотехнологичный проект, который с течением времени демонстрирует высокую эффективность в различных контекстах, с различными партнерами, в том числе в низкотехнологичных условиях. Кроме того, первое поколение системы оказалось достаточно гибким, чтобы стимулировать внедрение дальнейших инноваций в плане технологических достижений, таких как итерация hyperledger, а также адаптацию к более широкому спектру случаев использования. Проблемы, выявленные Sikka, также информативны.

Решения по проектированию и внедрению основаны на стремлении удовлетворить потребности пользователей. Интерфейс и инфраструктура соответствуют потребностям и навыкам конечных пользователей. Аналогичным образом, местный дизайн является краеугольным камнем проекта; управление командой, разработка и поддержание кода осуществляются гражданами Непала в Непале. По этим причинам решение Sikka полностью основано на знаниях, которыми обладают конечные пользователи. Например, Sikka использует текстовые сообщения, потому что это то, с чем большинство пользователей уже знакомы. Кроме того, для функционирования Sikka организациям не требуется распространять какое-либо дополнительное оборудование или материалы (например, дебетовые карты) среди получателей помощи. Как и многие другие современные программы гуманитарной помощи на основе цифровых идентификаторов, команда рассматривает возможность внедрения услуг интерактивного голосового ответа для повышения доступности.



5 В исследовании на местах 2018 г. затраты на одного получателя помощи составили 6,972 доллара США. В 2019 г. этот показатель составил 1,54 доллара США (1,42 швейцарских франка / 1,29 евро). 583 000 непальских рупий (5 500 долларов США) были распределены среди 73 получателей помощи; а затраты на Ethereum и SMS составили менее 0,50 доллара США на получателя помощи.

Несмотря на этот преднамеренный выбор дизайна, Sikka столкнулась с рядом проблем со стороны регулирующих органов и конечных пользователей. Одним из основных препятствий является необходимость повышения информированности регулирующих органов о том, как работает блокчейн. Технология блокчейн часто окутана неверными представлениями и предположениями, связанными с незаконной деятельностью. Это не просто маркетинговая или брендинговая трудность, это также фактор, влияющий на регуляторную среду. Например, в 2017 г. компания Sikka была готова к проведению первого пилотного проекта, но Непал Растра Банк запретил любую деятельность, связанную с переводом криптовалют. Хотя Sikka и не развернула криптовалютную деятельность, она сделала шаг назад, чтобы пересмотреть структуру дизайна, чтобы исключить возможность восприятия Sikka как криптовалютной торговой платформы. Нынешнее решение Sikka изучить версию hyperledger является ответом на ту же самую проблему, связанную с регулированием. Получатели помощи также столкнулись с проблемами. Те, кто подписался на услуги небольших операторов мобильной связи, испытывали трудности с отправкой и получением смс, в то время как другие не умели пользоваться телефоном достаточно хорошо, чтобы погасить токены без посторонней помощи. Введение нового стандарта токенов помогло решить данную проблему, так что Sikka может по-прежнему работать в тех случаях, когда требуется дополнительная помощь людям с плохим зрением или не имеющим возможности подключения к сети, не обладающим достаточным уровнем технического понимания, грамотности или не имеющим телефонов.

Sikka может быть использована в трех неисследованных случаях. Во-первых, она может помочь укрепить микрофинансовые услуги, если мы установим адекватные нормативные и этические границы, согласно платформе Convergences [35]. Во-вторых, HumanityX использовала Sikka в качестве примера в своем дереве решений, чтобы помочь взвесить преимущества и риски использования блокчейна для предоставления гуманитарной помощи; Sikka продемонстрировала, как введение токенов помогает избежать волатильности и регулирования криптовалют и повышает прозрачность [36]. В-третьих, команда Sikka считает, что Sikka может выступать в качестве суррогатной системы для обеспечения доступа к другим жизненно важным услугам во время стихийных бедствий (например, выплата наличных денег во время реагирования, восстановления и реконструкции), что может повысить функционал сообществ, у которых уже имеются партнеры по финансовым услугам [33].





Программа усиления эффекта реализации Целей устойчивого развития в Турции

Photo credit: Gravity

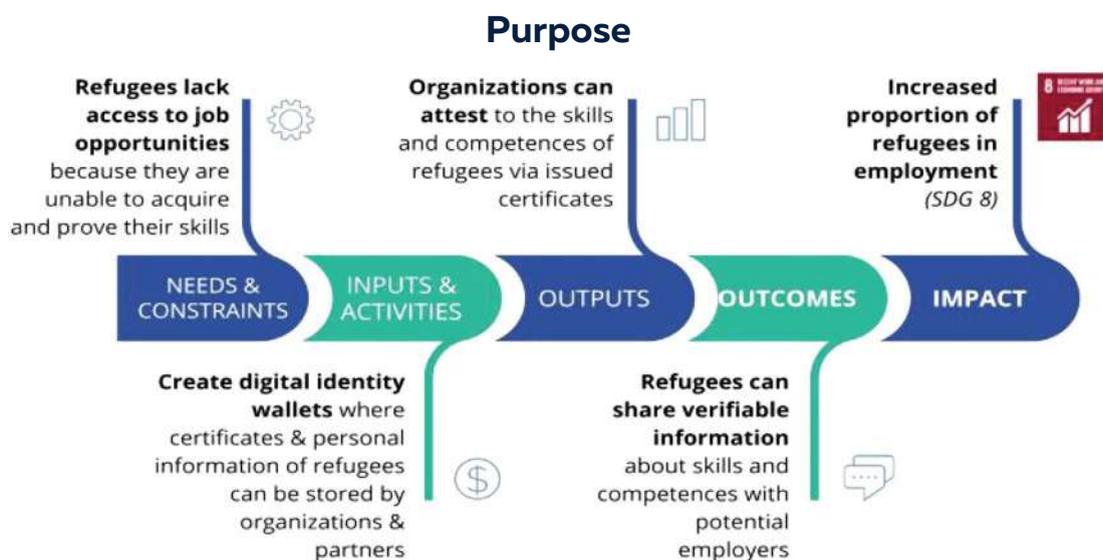
Обзор

Программа усиления эффекта реализации Целей устойчивого развития (SDGia) была разработана Министерством иностранных дел Турции и ПРООН для создания инноваций, способствующих развитию рынка для беженцев и населения наименее развитых стран [37]. Первый вариант программы «Accelerator Bootcamp» был запущен в июле 2019 г. в Стамбуле и Анкаре. Один из стартапов, участвующих в программе, является влиятельным технологическим партнером гуманитарных проектов цифровой идентификации: Gravity. Хотя вниманию были представлены и другие решения по цифровой идентификации, в том числе от Тукп, технологического партнера консорциума 121, работа Gravity выбрана в качестве примера, потому что в этом решении с самого начала было включено тесное сотрудничество с четырьмя другими организациями. Таким образом, это решение является наглядным примером проблем совместимости, связанных с системами цифровой идентификации, а также того, как эти же системы могут быть использованы для преодоления существующих проблем координации. Более того, Gravity обеспечила широкую доступность более подробной документации по этому проекту.

Свою децентрализованную платформу идентификации для улучшения качества «гуманитарной координации» Gravity продвигает с помощью цифрового кошелька для документов об образовании [38]. Получателями помощи в рамках этого проекта являются перемещенные лица, прошедшие профессиональное обучение и курсы турецкого языка в Промышленной палате Газиантепа и Палате ремесленников и мастеров Газиантепа. После того, как проект был представлен, его реализация осуществлялась в течение шести месяцев (июль-декабрь 2020 г.).

Было отмечено, что беженцам необходимо преодолеть значительные барьеры, чтобы максимально повысить свои шансы на трудоустройство, и что существует слишком много организаций, предоставляющих возможности для обучения, при отсутствии механизма координации. В результате этого получатели помощи проходили случайные курсы, а не те, которые были необходимы для развития конкретных навыков. Организации, предоставляющие гуманитарную помощь, не могли выявить ненадежные курсы-дубликаты качественных.

Решение заключалось в использовании децентрализованной платформы идентификации Gravity для создания цифровых кошельков для получателей помощи. Получатели помощи хранят свои сертификаты об обучении в цифровом кошельке. Затем руководители программ могут целенаправленно обращаться к определенным слоям населения, исходя из искомым навыков или демографических характеристик. Донорские организации могут отслеживать анонимные траектории движения людей через систему вплоть до трудоустройства, чтобы оценить эффективность программы помощи. Система обеспечивает полную конфиденциальность, поскольку от получателей помощи ни на каком этапе не требуется хранить или раскрывать конфиденциальные личные данные. Конечный продукт повышает шансы беженцев на трудоустройство и усиливает подотчетность организаций, распределяющих помощь, перед донорскими организациями.



Source: Thakur, January 2020 via Medium

Роли

В целях создания совместной платформы Gravity сотрудничала с партнерами по консорциуму, компаниями Sertifier и Mark Labs, а также с двумя ветвями местных органов власти, Промышленной палатой Газиантепа (GSO) и Палатой ремесленников и мастеров Газиантепа (GESOB), которые обеспечивают языковое и профессиональное обучение для перемещенных лиц. На втором этапе пилотного проекта в нем также приняли участие местные работодатели.

Sertifier [39] является партнером по реализации; сертификаты об обучении получателям помощи, выданные через интерфейс Sertifier, приходят непосредственно на их цифровые кошельки. Mark Labs предоставляет возможность создания экосистемы данных для отслеживания и оптимизации воздействия [40]. С GSO и GESOB были проведены консультации для анализа статус-кво сбора и управления данными о получателях помощи, а также для понимания пути получателей помощи от прохождения обучающего курса до трудоустройства. В своих отзывах о пилотном проекте GSO и GESOB сообщили, что считают децентрализованную платформу обмена данными полезной с точки зрения координации и соблюдения конфиденциальности данных получателей помощи [41]. Благодаря тому, что основное внимание в вопросах обмена данными было уделено именно получателям помощи, удалось уменьшить трения, с которыми местные партнеры могли бы столкнуться при взаимодействии как с получателями помощи, так и с работодателями. На этапе разработки продукта в рамках пилотного проекта Gravity разработала новый функционал для того, чтобы получатели помощи могли делиться своими учетными данными с любым контрагентом, даже если они находятся за пределами экосистемы Gravity. В настоящее время получатели помощи могут обмениваться сертификатами с семью предприятиями в различных отраслях - от производства оборудования и машиностроения до информационных технологий и косметики. Этим работодателям, в свою очередь, доступна возможность просмотра историй пройденного обучения в GSO и GESOB и проверки их происхождения и подлинности данных. Ранее в рамках этого процесса представители GSO и GESOB представляли получателей помощи работодателям, посещая их лично.

Технологии

Gravity использует децентрализованную идентификацию таким образом, что каждый получатель помощи может получать, хранить и обмениваться данными на цифровом кошельке, доступ к которому есть только у него. Пользователи контролируют, какая информация передается тем или иным организациям, так что ни одна организация не может получить доступ к этим данным без их согласия. Участники получают инструкции по созданию и использованию своих кошельков с помощью информационного видеоролика и личной помощи. В ходе пилотного проекта было отмечено незначительное количество трудностей при регистрации, а те трудности, которые возникли, были изучены, а соответствующие функции и технологические процессы для последующих итераций были направлены на доработку. Веб-приложение Gravity доступно на турецком и арабском языках, что дает возможность легко пользоваться платформой сотрудникам GSO и GESOB, а также потенциальным работодателям.

Для сертификации цифровых учетных данных потребовалась интеграция между Gravity и Sertifier. Дополнительный функционал был создан для того, чтобы пользователи могли поделиться учетными данными с любым заинтересованным работодателем или третьей стороной, а те, в свою очередь, могли проверить, действительно ли учетные данные были выданы ГСО или ГЕСОБ через портал проверки на основе браузера. Ниже приведены примеры интеграции Gravity and Sertifier и портала верификации данных для работодателей.



Источник: Thakur, Январь 2020г. via Medium

Анализ

Опыт Gravity в Газиантепе демонстрирует ценность государственно-частного партнерства, а также то, как можно добиться значительной операционной совместимости без ущерба для конфиденциальности данных или контроля отдельных лиц над своими собственными данными. Этот пример также демонстрирует, как цифровые идентификационные системы могут помочь мигрантам на протяжении всего их пути. Цифровые идентификационные системы обычно внедряются для поддержки мер реагирования на кризисные ситуации или оказания немедленной гуманитарной помощи, включая первоначальную регистрацию для получения помощи, а также краткосрочную помощь, будь то в виде продуктов питания или денежных переводов. Работа Gravity способствует следующему жизненно важному шагу: помогает беженцам получить и подтвердить свое образование и профессиональную подготовку, чтобы они могли повысить свой уровень социально-экономической интеграции. Важно, что решение Gravity способно помочь всем заинтересованным сторонам: получателям помощи, организациям по оказанию помощи и обучению, а также работодателям.

О сильном потенциале цифровых идентификационных систем для создания долгосрочной ценности для мигрантов в их пути говорят в своих интервью представители команды Gravity. Многие представители Gravity с энтузиазмом говорили о том, что системы цифровой идентификации могут помочь получателям помощи создать альтернативный кредитный след, при котором их благонадежность будет определяться данными о взаимодействии с поставщиками услуг обучения, работодателями и даже финансовыми учреждениями. В идеале это могло бы помочь повысить качество их взаимодействия с официальными финансовыми структурами и поддержать их дальнейшую социально-экономическую интеграцию.

6 Проблемы, с которыми столкнулись около 5 процентов получателей помощи во время регистрации, были следующими: отсутствие активной SIM-карты (необходимой для получения одноразового пароля) и трудности с загрузкой файла криптографического ключа (особенно это касается пользователей iPhone).

Необходимо решить проблемы, связанные с этой моделью. Неясно, как можно обеспечить более устойчивое финансирование проекта вне зависимости от грантов SDGiA. Другой вопрос заключается в том, как при использовании программы можно избежать дальнейшего исключения, основанного на неравенстве доступа к мобильным телефонам и цифровой грамотности, которые заметны даже среди недавно переселившихся мигрантов, живущих в Газиантепе. Этот вопрос особенно актуален, поскольку зачастую модели исключения часто ставят в более уязвимое положение женщин.



ВЫВОДЫ

Возможность подтвердить свою личность становится все более важной в нашем взаимосвязанном цифровом мире. Для обеспечения равного для всех доступа к услугам, будь то услуги здравоохранения, финансовые услуги или государственные субсидии, возможность идентифицировать свою личность является жизненно важным фактором. Более чем один миллиард людей во всем мире, не имеющих признанного удостоверения личности, ощущают сегодня эту реальность особенно остро. Учитывая то, что гуманитарные организации обслуживают многие из наиболее уязвимых групп населения в мире, особенно важно ознакомить их с новыми решениями и обсуждениями о цифровой идентификации. В то время как процесс идентификации традиционно облегчалось наличие бумажных удостоверений личности, сегодня процессы идентификации все больше зависят от цифровых технологий [1]. Для гуманитарных организаций данные вопросы не новы. Многие из них занимались ими на протяжении десятилетий с помощью систем управления данным о получателях помощи и информацией. И все же в настоящее время самые разные организации, включая поставщиков телекоммуникационных услуг, финансовые учреждения, правительства и другие организации, начинают предпринимать новые усилия по цифровизации, чтобы адаптироваться к новым разработкам в сфере управления идентификацией и доступом и децентрализованной идентификации [2]. Поэтому очень важно, чтобы гуманитарные организации продолжали участвовать в этих дискуссиях для дальнейшего развития своих стратегий цифровизации.

Несмотря на рост консенсуса относительно ценности цифровой идентификации в сфере предоставления цифровых услуг, вопрос о том, стоит ли отдельной организации инвестировать в эту технологию, остается открытым. Потенциал цифровой идентификации для расширения доступа к социальной, политической и экономической интеграции делает ее потенциальным путем к выполнению миссии многих гуманитарных организаций и агентств развития. Тем не менее, эти технологии также поднимают важные вопросы о получении значимого согласия от получателей помощи, на которые пока нет ответа. Важно не ожидать, что технологии смогут решить эти проблемы, а в некоторых случаях их применение может усугубить асимметрию власти. Вместо того чтобы вкладывать средства в разработку системы цифровой идентификации на ранних этапах, гуманитарным организациям, возможно, целесообразно работать | с поставщиками решений, которые уже разработали продукт, который затем может быть адаптирован к потребностям организации. Это может сэкономить значительное время и финансовые ресурсы. Несколько организаций, с которыми проводились интервью, отметили, что в связи с необходимостью вложения первоначальных ресурсов для достижения цифровой трансформации программы цифрового удостоверения личности становятся непомерно дорогими. Тем не менее, возможность плодотворного участия зависит от возможности накапливать опыт в этой растущей области инноваций. Продолжая учиться, гуманитарные организации могут гарантировать, что их участие в развитии сферы цифровой идентификации будет активным.

Как показано в данном отчете, существует ряд сложностей, которые гуманитарная организация должна учитывать в процессе взаимодействия с системами цифровой идентификации. Операционная совместимость и способы ее эффективного достижения как внутри гуманитарного сектора, так и за его пределами остаются важнейшими и пока еще нерешенными вопросами. Стремясь достичь прогресса в этой области, гуманитарные организации могут обратиться к альтернативным вариантам финансирования и механизмам финансирования. Используя такие модели, как программное обеспечение как услуга, гуманитарные организации могут оптимизировать финансирование инноваций, повышая вероятность успешного долгосрочного взаимодействия с новыми технологиями. Кроме того, гуманитарные организации не должны действовать в вакууме. Напротив, сотрудничая с соответствующими отраслевыми организациями и развивая межсекторальное сотрудничество, гуманитарные организации могут извлечь преимущества из прогресса, достигнутого в соответствующих внешних областях.

Несмотря на то, что гуманитарные организации сталкиваются с целым рядом проблем при внедрении решений по цифровой идентификации, таких как низкий уровень охвата мобильной связью, инновации в других секторах (например, снижение стоимости смартфонов) могут значительно расширить возможности гуманитарных организаций по снижению этих рисков, одновременно реализуя преимущества новых технологий. В конечном итоге, технологии цифровой идентификации могут стать полезными как для организаций, так и для получателей помощи, но только в том случае, если они будут внедряться с тщательным учетом местных особенностей и с соблюдением необходимых мер предосторожности для обеспечения безопасности и эффективности.

СПИСОК ИСТОЧНИКОВ

(All URLs last accessed on 8 February 2021)

1. Financial Action Task Force/OECD. (2020). "Guidance on Digital Identity: Executive Summary." Available at <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-Executive-Summary.pdf>
2. Slavin, A. (2019). "Distributed ledger identity systems in the humanitarian sector." Available at <https://sovrin.org/wp-content/uploads/14A-Report.pdf>
3. PR Newswire. (2020). "Digital ID Solutions Industry Projections, 2020-2024: Increased Adoption of the Cloud-Based Digital Identity Solutions, Wide Adoption of Authentication Across Verticals." Available at <https://www.prnewswire.com/news-releases/digital-identity-solutions- industry-projections-2020-2024---increased-adoption-of-the-cloud-based-digital-identity- solutions-wide-adoption-of-authentication-across-verticals-301020601.html>
4. Bostrom, N. and Sandberg, A. (2011). "The Future of Identity." Report commissioned by UK Government Office for Science. Available at <https://nickbostrom.com/views/identity.pdf>
5. Mastercard. (2019). "Digital Identity: Restoring Trust in a Digital World." Available at <https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf>
6. Microsoft. "Own your digital identity." Available at www.microsoft.com/en-us/security/business/identity/own-your-identity
7. Crunchbase. "Okta". Available at www.crunchbase.com/organization/okta
8. White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M., and Sperling, O. (2019). "Digital identification, a key to inclusive growth." Available at www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#
9. Humanitarian Innovation Platform. "Dignified Identities (Digid) in Cash Programming" Available at <https://hiplatform.org/digid>
10. GSM Association. (2018). "Using Mobile Technology to provide Functional Identities." Available at www.gsma.com/mobilefordevelopment/blog_2/using_mobile_technology_provide_functional_identities
11. ICRC. (2019). "Do No Harm in the Digital Era." Event on 29 August 2019 at Marriott Hotel, Kigali, Rwanda. Available at <https://www.icrc.org/en/event/do-no-harm-digital-era>
12. UNHCR. (2013). "The mandate of the High Commissioner for Refugees and his Office." Available at www.unhcr.org/uk/protection/basic/526a22cb6/mandate-high-commissioner-refugees-office.html
13. World Bank. "ID4D Practitioner's Guide: Levels of assurance (LOAs)". Available at <https://id4d.worldbank.org/guide/levels-assurance-loas>
14. World Wide Web Consortium. "Verifiable Credentials Data Model 1.0". Available at <https://www.w3.org/TR/vc-data-model/>
15. World Bank. "ID4D Practitioner's Guide: Interoperability". Available at <https://id4d.worldbank.org/guide/interoperability>

16. Health Level Seven International "FHIR Overview". Available at <https://www.hl7.org/fhir/overview.html>
17. Financial Action Task Force. (2020). "Guidance on Digital Identity." Available at <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf>
18. Post, L., Raile, A., and Raile, E. (2010). "Defining Political Will." *Politics & Policy*. Vol.38(4):653-676. Available at: <https://doi.org/10.1111/j.1747-1346.2010.00253.x>
19. WFP. (2014). "SCOPE In Five Minutes." Available at <https://documents.wfp.org/stellent/groups/public/documents/communications/wfp272586.pdf>
20. World Vision International. "How LMMS works." Available at <https://www.wvi.org/disaster-management/how-lmms-works>
21. Sovrin Foundation (2018). What is Self-Sovereign Identity? Available at <https://sovrin.org/faq/what-is-self-sovereign-identity>
22. Rodriguez, K. (2020). "Linux Foundation Training Announces a Free Online Course-Developing Blockchain-Based Identity Applications." Available at <https://linuxfoundation.org/press-release/linux-foundation-training-announces-a-free-online-course-developing-blockchain-based-identity-applications/>
23. World Bank. (2018). "Understanding Cost Drivers of Identification Systems." Available at <http://documents1.worldbank.org/curated/en/702641544730830097/pdf/Understanding-Cost-Drivers-of-Identification-Systems.pdf>
24. Safaricom. "M-Pesa". Available at www.safaricom.co.ke/personal/m-pesa
25. Hawkins, L. (2020). "Secure digital ID verifying Covid vaccine status to launch." Available at www.healthcareglobal.com/digital-healthcare/secure-digital-id-verifying-covid-vaccine-status-launch
26. Bollinger, T. (2000). "A Guide to Understanding Emerging Interoperability Technologies." Available at http://www.mitre.org/sites/default/files/pdf/bollinger_interop.pdf
27. UNHCR. (2019). "Global Virtual Summit on Digital Identity for Refugees, Concluding Workshop: Summary Conclusions and Recommendations." Available at www.unhcr.org/idecosystem/wp-content/uploads/sites/69/2019/12/Conclusions_and_Recommendations.pdf
28. Kak, A., Ben-Avie, J., Munyua, A., and Tiwari, U. (2020). "Bringing Openness to Identity." Available at <https://blog.mozilla.org/netpolicy/files/2020/01/Mozilla-Digital-ID-White-Paper.pdf>
29. The Netherlands Red Cross. (2021). "GSMA Consortium Pilots 121 in Kenya". Available at <https://www.121.global/gsma-consortium-pilots-121-in-kenya/>
30. Africa's Talking. "Homepage." Available at <https://africastalking.com/>
31. World Vision International Nepal. (2020). "Nepal COVER Project". Available at <https://reliefweb.int/sites/reliefweb.int/files/resources/Nepal%20COVER%20Project%20SitRep%2011%20%28Updated%208%20July%202020%29.pdf>
32. Davis, J. (2018). "Sikka: Working at the intersection of blockchain and humanitarian innovation." Available at <https://medium.com/@davisjef/sikka-working-at-the-intersection-of-blockchain-and-humanitarian-innovation-2c752332c616>
33. World Vision International Nepal Innovation Lab. (2018). "Sikka: A digital asset transfer platform designed for the financially marginalized." Available at www.sikka.me/docs/SikkaConceptPaper.pdf

34. Acharya, S. and Pandey, S. (2019). "Sikka: One Year Later, Lessons Learnt and Recent Developments." Available at <https://medium.com/@saujanyaacharya/sikka-lessons-learned-and-recent-developments-8fda5b1b83cf>
35. Coppi, G. (2018). "Blockchain and microfinance: hype or promise?" Available at <https://www.convergences.org/en/blockchain-and-microfinance-hype-or-promise/>
36. Dodgson, K. (2018). "Blockchain for Humanitarian Aid Decision Tree." Available at <https://blockchain.humanityx.nl/uploads/toolkit/Blockchain-decision-tree-offline-toolkit-v2.pdf>
37. SDG Impact Accelerator. "About." Available at <https://www.sdgia.org/about-sdgia/>
38. SDG Impact Accelerator. (2019). "Live from #SDGIA Demo Day in Istanbul - 13 Sept 2019". YouTube livestream on 13 September 2019. Available at www.youtube.com/watch?v=nimVxveZ5Kg
39. Sertifier. "Homepage." Available at <https://sertifier.com/en/>
40. Mark Labs. "Homepage." Available at <https://www.marklabs.co/>
41. Thakur, S. (2019). "Results from the field: Improving livelihood prospects for refugees through decentralized identity in Gaziantep, Turkey." Available at <https://medium.com/gravity-earth/results-from-the-field-improving-livelihood-prospects-for-displaced-persons-through-digital-5786587308f8>

СПИСОК ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ, ИСПОЛЬЗОВАННЫХ В ДАННОМ ОТЧЕТЕ

Coppi, G. and Fast, L. (2019). "Blockchain and distributed ledger technologies in the humanitarian sector." Available at <https://odi.org/en/publications/blockchain-and-distributed-ledger-technologies-in-the-humanitarian-sector/>

Ebert, J. (2019). "Learnings from the SDG Impact Accelerator." Available at <https://medium.com/gravity-earth/learnings-from-the-sdg-impact-accelerator-90abe6c13669>

eSatya. (2020). "Blockchain and Sustainable Development." Available at <https://esatya.io/collection/blockchain-and-sustainable-development/>

Humanitarian Innovation Platform (2020). "Layering Digital ID on top of Traditional Data Management." Available at <https://hiplatform.org/blog/2020/5/20/layering-digital-id-on-top-of-traditional-data-management>

Innovasjon Norge. (2021). "Dignified identities in cash programming II (DIGID II)." Available at www.innovasjon Norge.no/no/subsites/hipnorway/innovation-projects2/dignified-identities-in-cash-programming-ii-digid-ii/

Intersolve. "Homepage." Available at <https://intersolve.nl/>

Myler, J. (2019). "Sikka: The Blockchain-Based Application Putting Money in the Hands of Nepal's Rural Communities." Available at <https://medium.com/@asiap3hub/sikka-the-blockchain-based-application-putting-money-in-the-hands-of-nepals-rural-communities-81ab9067a309>

UNDP Turkey, and Gravity. (2021). "Improving livelihood prospects for displaced persons through digital identity in Turkey." Available at https://drive.google.com/file/d/1jKn4oz_vUODUcen98c90P7jjCJnP343_/view?usp=sharing

ПРИЛОЖЕНИЯ

Приложение I: Вопросы интервью

Вопрос 1: В каких случаях могут применяться решения по цифровой идентификации, и что делает их подходящими? Каковы ограничения их применимости?

Вопрос 2: В настоящее время возрастает необходимость защиты данных получателей помощи, внедрения технологий самостоятельной идентификации, чтобы предоставить получателям помощи больше автономии в управлении и владении своими данными, а также уменьшения объемов конфиденциальных данных, хранящихся в централизованных базах данных. Ввиду перечисленного, как гуманитарные организации должны адаптировать свои системы и практику управления данными получателей помощи для обеспечения ответственной интеграции цифровых идентификационных решений?

Вопрос 3: Организации по оказанию помощи располагают ограниченными ресурсами. Принятие новых технологий может повлечь за собой барьеры в плане затрат, навыков и ресурсов (обслуживание, поддержка и т.д.). Какие экономические стимулы и устойчивые бизнес-модели для использования технологии цифровых идентификаторов применимы к гуманитарным организациям?

Вопрос 4: Что представляет собой операционная совместимость между гуманитарными организациями, использующими цифровые идентификаторы? При ответе на этот вопрос следует изучить функциональную совместимость данных независимо от технологий, используемых для их сбора и хранения (например, цифровые удостоверения, выданные различными технологиями цифровых удостоверений личности, но использующие такие стандарты, как децентрализованные идентификаторы, проверяемые удостоверения и т.д.), а также процессы и готовность обмена данными между организациями для предотвращения дублирования.

Вопрос 5: Перспективы самостоятельной идентификации зависят от нескольких факторов: цифровой грамотности конечных пользователей, степени развитости инфраструктуры и доступности средств связи, таких как смартфоны. Такие факторы являются барьерами в местах, где потенциальные получатели помощи могут быть одними из самых уязвимых групп населения. Как гуманитарные организации могут внедрять технологии цифрового удостоверения личности в условиях низкой доступности связи?

Вопрос 6: Существует противоречие между желанием отдельных лиц сохранить контроль над собственными данными (децентрализация хранения данных и контроля получателям помощи над ними) и желанием организаций использовать данные отдельных лиц в целях координации (чтобы избежать дублирования и мошенничества) и подотчетности перед донорскими организациями (чтобы продемонстрировать, что помощь оказывается реальным людям). Каковы компромиссы, связанные с разрешением этого противоречия? Как можно найти баланс? Каких подводных камней следует избегать?

Вопрос 7: Какое обучение грамотности в области данных требуется получателям цифровых идентификаторов для того, чтобы они могли безопасно ими пользоваться? В чем различия этих требований для пользователей смартфонов и телефонов?

Приложение II: Респонденты

Индивидуальные интервью:

Номер	Имя	Должность и место работы
#1	Анонимный F1	Проектная группа Цифровой Идентификации, организация помощи
#2	Amanda Robinson	Глава направления «Социальные инновации и технологии в гуманитарном секторе», Красный Крест Австралии
#3	Jimmy Snoek	Исполнительный директор, Tynk
#4	Anonymous F3	Проектная группа Цифровой Идентификации, организация гуманитарной помощи
#5	Anonymous A	Менеджер программ, организация гуманитарной помощи ООН
#6	Paul Currion	Директор по операциям, Disberse
#7	Anonymous D	Руководитель службы данных, организация гуманитарной помощи ООН
#8	Анонимный B	Менеджер проекта, крупная гуманитарная организация
#9	Johannes Ebert	Исполнительный директор, Gravity
#10	Sharanya Thakur	Менеджер проекта, Gravity
#11	Alexandros Yiannopoulos	н/п
#12	Safia Verjee	Менеджер инновационных программ, Красный Крест Кении
#13	Natalie Brinham	Специалист по разработке программ, Институт по проблемам лиц без гражданства и инклюзии
#14	Andrew Tobin	Управляющий директор (ЕБВА) & и Руководитель направления по продуктам для клиентов, Evernum
#15	Анонимный C	Исследователь в области прав человека, организация по вопросам адвокации
n/a	Jennifer Gilbertson	Координатор инновационных программ в гуманитарном секторе, Норвежский Красный Крест
n/a	Анонимный F2	Проектная группа Цифровой Идентификации, организация гуманитарной помощи

Фокус группа:

ФИ	Должность и место работы
Margie Cheesman	Д-р наук в области прав мигрантов на защиту данных, институт интернета г. Оксфорд
Emrys Schoemaker	Специалист по цифровым данным, Caribou Digital
Amos Doornbos	Директор по разработке стратегий и систем в сфере реагирования на катастрофы, WorldVision International
Vincent Graf Narbel	Стратегический советник по технологиям, МФКК
Giulio Coppi	Специалист по глобальным цифровым данным, Красный Крест Норвегии
Hakan Büyükbayrak	Директор, RedRose
Christine Leong	Руководитель глобальной группы, Идентификация личности и биометрические данные в работе с блокчейном, Accenture

ПРИЛОЖЕНИЕ III: Подробное описание методологии

Интервью

Интервью с ключевыми заинтересованными сторонами из гуманитарного сектора поддержали кабинетное исследование и анализ конкретных примеров. Исследовательская группа совместно с МФОККиКП работала над определением приоритетов и обращением к ключевым участникам. В общей сложности были проведены консультации с 24 людьми. Они представляли основных доноров развития, гуманитарные организации, которые в настоящее время внедряют системы цифровых идентификаторов, активистов за права на гуманитарные данные, экспертов по конфиденциальности данных из МФОККиКП и УВКБ ООН, представителей частного сектора, таких как Accenture, поставщиков технологий и исследователей из крупных академических институтов. Список всех участников интервью приведен в Приложении II.

Большинство интервью проводилось индивидуально в период с 3 декабря 2020 года по 15 января 2021 года. Семь участников приняли участие в виртуальной сессии фокус-группы, организованной 16 декабря 2020 года при поддержке Оксфордского центра технологий и менеджмента в целях развития. Все интервью проводились на английском языке с использованием Microsoft Teams. Один участник предоставил ответы по электронной почте.

Индивидуальные интервью проходили в полуструктурированном формате. Участники заранее получили список из семи ключевых вопросов, использованных в данной работе. Microsoft Teams была выбрана из-за функций безопасности платформы, включенных в лицензионное соглашение с Оксфордским университетом, к которому исследовательская группа имела доступ. Чтобы повысить шансы на сохранение стабильного интернет-соединения, участников не просили использовать видео. В начале разговора было выделено время, чтобы установить контакт и ответить на любые вопросы участников; это помогло создать личную атмосферу и установить доверие, необходимое для того, чтобы участники чувствовали себя достаточно комфортно, чтобы открыто поделиться своими мыслями.

Фокус-группа проходила в более строгом формате. Участникам заранее был выслан список ключевых вопросов, и им было предложено выбрать три из них для ответа, при этом было выделено время для ответов и открытой дискуссии в ответ на каждое выступление. В отличие от индивидуальных интервью, в фокус-группе поощрялось использование видео, чтобы создать атмосферу круглого стола.

Интервью и беседы фокус-группы записывались с помощью приложения Voice Memos на айфонах исследовательской группы для облегчения процесса расшифровки. Записи были немедленно загружены на зашифрованный жесткий диск и расшифрованы с помощью программы Nvivo. В начале каждого разговора опрашиваемых просили дать устное согласие на участие в исследовании. Участников также спрашивали, желают ли они сохранить анонимность. Несколько участников выбрали этот вариант; их имена и институциональная принадлежность не указаны, чтобы избежать риска идентификации. Высказанные ими соображения все же легли в основу результатов исследования. Участники сохранили за собой право запросить копию своей записи или попросить удалить ее в любой момент в период с ноября 2020 года по март 2021 года. На момент написания статьи (апрель 2021 года) записи были удалены. Всем участникам была предоставлена возможность ознакомиться с окончательным вариантом проекта отчета об исследовании и попросить внести в него изменения.

ОСНОВОПОЛАГАЮЩИЕ ПРИНЦИПЫ МЕЖДУНАРОДНОГО ДВИЖЕНИЯ КРАСНОГО КРЕСТА И КРАСНОГО ПОЛУМЕСЯЦА

Гуманность

Международное движение Красного Креста и Красного Полумесяца, порожденное стремлением оказывать помощь всем раненым на поле боя без исключения или предпочтения, старается при любых обстоятельствах как на международном, так и на национальном уровне предотвращать или облегчать страдания человека. Движение призвано защищать жизнь и здоровье людей и обеспечивать уважение к человеческой личности во всех случаях. Оно способствует достижению взаимопонимания, дружбы, сотрудничества.

Беспристрастность

Движение не проводит никакой дискриминации по признаку расы, религии, класса или политических убеждений. Оно лишь стремится облегчать страдания людей, и в первую очередь тех, кто больше всего в этом нуждается.

Нейтральность

Чтобы сохранить всеобщее доверие, Движение не может принимать чью-либо сторону в вооруженных конфликтах и вступать в споры политического, расового, религиозного или идеологического характера.

Независимость

Движение независимо. Национальные общества, оказывая своим правительствам помощь в их гуманитарной деятельности и подчиняясь законам своей страны, должны тем не менее всегда сохранять автономию, чтобы иметь возможность действовать в соответствии с принципами Красного Креста.

Добровольность

В своей добровольной деятельности по оказанию помощи Движение ни в коей мере не руководствуется стремлением к получению выгоды.

Единство

В стране может быть только одно Национальное общество Красного Креста или Красного Полумесяца. Оно должно быть открыто для всех и осуществлять свою гуманитарную деятельность на всей территории страны.

Универсальность

Движение является всемирным. Все Национальные общества пользуются равными правами и обязаны оказывать помощь друг другу.



Международная федерация обществ Красного Креста и Красного Полумесяца (МФОККиКП) – крупнейшая в мире гуманитарная сеть, объединяющая 192 национальных общества Красного Креста и Красного Полумесяца и около 14 миллионов волонтеров. Наши волонтеры присутствуют в населенных пунктах до, во время и после кризиса или бедствия. Мы работаем в самых труднодоступных и сложных условиях в мире, спасая жизни и отстаивая человеческое достоинство. Мы помогаем сообществам обрести большую силу и устойчивость и стать местом, где люди могут жить безопасной и здоровой жизнью и иметь возможности для процветания.

Информация о нас доступна по ссылкам:

www.ifrc.org | twitter.com/ifrc | facebook.com/ifrc | instagram.com/ifrc | youtube.com/user/ifrc | tiktok.com/@ifrc