Introduction

The humanitarian response in Somalia operates with limited visibility from **fragmented data**. In an increasingly resource-constrained environment, the need for **interoperable systems** has become critical to ensure efficiency, accountability, and equity in assistance delivery. Through the network of Post-Distribution Aid Diversion (PDAD) Working Groups, a framework to enable **secure data exchange** and **better coordination** through interagency deduplication**,** referrals, and relevant situational awareness.

Plans for interagency data exchange rely on two core building blocks:

1. **Single Registration Form (SRF)** – a harmonized set of data fields for beneficiary registration, enabling common standards and targeting methodologies
2. **Federated Registration System (FRS)** – an integration-enabled model facilitating data analysis across multiple agency systems while preserving agency's system autonomy, data ownership, and privacy

This report reviews strategic vision**,** governance structures**,** sustainability, and feasibility for this interoperability model in Somalia, highlighting questions regarding data protection, deduplication, UID management, biometrics**,** and alignment with government systems. It reflects inputs from key partners, including IOM, SCC, and WFP (among others).

PDAD Task Teams

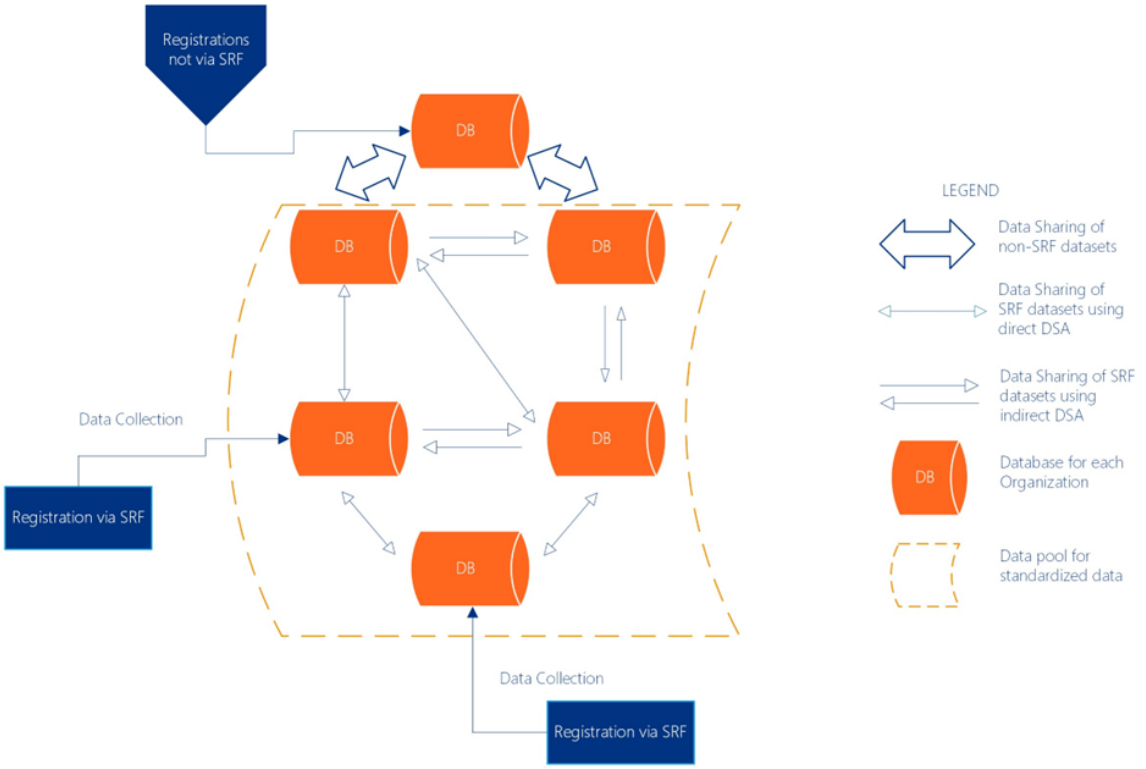
Throughout 2024, the Post-Distribution Aid Diversion (PDAD) Task Teams (TTs) made significant strides.[1] Specifically, the PDAD Registration and Targeting TTs built consensus around three commitments: 1) transitioning to vulnerability-based targeting, b) adopting a "single registration form" (SRF), and 3) adopting a federated configuration of digital registries, supported by a uniform registration process [SRF] and biometrics. (While non-biometric registration methods are included, biometrics are the noted preference.) The uniform registration process is still under discussion to build consensus around key steps within the processes, such as initial assessment (of eligibility), formal registration (eligible households), enrollment into an assistance programme, etc.

The Registration and Targeting TTs also kickstarted a policy paper now endorsed by the HCT, outlining both rationale and architecture supporting future-state data sharing and biometric identity management for humanitarian actors. As a first major step, the TTs developed the SRF, a single standardized survey intended for use by all actors conducting registration exercises on affected populations including IDPs, refugees and host communities.

[1] As of October 2025, the PDAD TTs have dissolved. Three (3) new HCT "Reset" Teams now continue

"Direction of Travel" Proposed

Single Registration Form (SRF)



Single Registration Form Flow Chart (Source: HCT-endorsed Policy Paper)

The SRF establishes a minimum standard dataset, capturing data fields (e.g. name, DOB) uniformly in ways that can be used standalone or alongside biometric data to better facilitate duplication checks, referrals, and analysis. Developed as a mobile data collection tool [in Kobo], actors are envisioned to adopt the SRF as a standardized entry point to enrol new potential aid recipients. (For latest iteration of the SRF, please refer to the draft RTT Policy Paper or Registration TT.)

The SRF is not a comprehensive vulnerability assessment, though does serve as a starting point of household-level data collection for more in depth follow-up for agencies that choose to do so. The digitized SRF is meant to generate a unique identifier (UID) for each form submission in order to manually support longitudinal data collection. Per SRF draft reviewed[2], the UID calculation is assigned per household based on a concatenation of timestamps and manual data entry:

- concat([**form-submission-timestamp**],'_', [**registrationDistrict**], [**organizationID**]

[2] *SRF – Question Bank and Indicators Rev.xlsx*

There is a goal, however, for ***fingerprint and facial biometrics to serve as the primary form of UID used by humanitarian actors***, captured through the SRF for all household members above the age of five (5).

Federation of Registration Systems (FRS)

Admittedly a more ambitious effort is the second component of the "direction of travel": developing a Federation of Registration Systems (FRS). This generally refers to "semi-autonomous" registration systems[3] connected through shared principles, common standards and/or interfaces to ensure security, interoperability and reliably high performance. Each contributing organization retains control and responsibility over its own data, systems, and workflows. For those with digital systems, this means maintaining their own systems while adhering to interoperability policies and frameworks set by a governing body.

Baseline Insights

In 2024, the Registration TT gathered insights from nearly 35 agencies regarding targeting methods, registration practices, data management, and data sharing more broadly. While informative, more direct inputs are needed from implicated agencies to better understand average capacity, experience (with digital), and more pointedly, willingness to adopt the SRF and/or FRS: as-is; with clarifications; with modifications; etc.

Some visibility was provided on data sharing agreements (DSAs) and data protection policies (DPP), with less understanding on how DSAs/DPPs are working in practice. To what extent DSAs and DPPs include clear communication, adjudication or conflict resolution frameworks to ensure digital accountability between participating organisations and towards affected people/ data subjects within them also requires further review.

Registration Systems Survey

- 13 total respondents, only 1 of which was a **local/national NGO or CSO** (LNGOs). UN agencies represented 69% of responses [9]. Local RC/RC societies were a notable absence; WHO (and health actors in general) were also not represented.
- Methods to verify a beneficiary included smartcards, tokens, and SMS confirmations to registered phone numbers
- 4 agencies recorded use of finger print biometrics, 3 of which are UN actors; the last agency, a LNGO, may serve as an implementing partner to a UN agency

Data Sharing Agreements Survey

[3] Registration systems can be comprised of multiple components, which may be hosted by different service providers. In this case, the 'federated' element pertains to the component where data is stored.

- Of 34 total respondents, 71% were **local/national NGOs or CSOs** (LNGOs). Almost all UN agencies were represented. UNICEF and Local RC/RC societies were a notable absence; WHO (and health actors in general) were also not represented.
- 35% (12) of respondents did not have a **data protection policy** in place, though of those the overwhelming majority were LNGOs (92%)
- **Deduplication rates** provided a more telling view onto the sensitization that will likely be required across actors in order to see SRF/FRS concepts take hold. As over half (65%) do not deduplicate.
- 26% (9) indicated having **no data protection policy or deduplication processes** in place. This represents a 'bottom tier' of capacity, where many other agencies may also sit. This tier serves as the lowest common denominator that all digital concepts, rollout plans, and otherwise must be sure to incorporate.
- For **biometrics,** 21% (7) use them in some form; no INGOs noted using biometrics. One agency did note using non-biometric digital verification, relying on mobile network operator (MNO) data.

Efforts to Operationalize

Single Registration Form (SRF)

While there are no indications of major disagreements on SRF content, more questions remain about its operationalization. SRF piloting has begun with several agencies, though parameters to record, evaluate, and compare experiences are still needed. IOM has setup dedicated technical support to onboard organizations and help them mitigate challenges operationalizing the tool within their own business processes. What is in need of greater clarification, however, is whether adopting these tools actually improves bottom line metrics of efficiency and effectiveness per agency: lowering costs, decreasing aid delivery timelines, and improving the general aid/service delivery experience for households receiving assistance.

It is clear agencies not already using Kobo for data collection would need clear indications regarding what within current processes may shift and how many resources will it take to get there. From a data capture standpoint, this could be as easy as translating SRF form content from Kobo into another ODK-based tool. (This may be more difficult to do if non-ODK based data collection applications are in use.) For agencies using Kobo, the digital integration may not be as arduous, though internally, programme teams will still need to realign existing data collection practices to incorporate the SRF into already ongoing operations. While not impossible, this does require "diligent planning, collaboration, and an ongoing commitment to improving the system based on user feedback and changing community dynamics."[4] What that translates to in practice is dedicated resources to support digitally-led change management and in some cases, digital transformation (especially for agencies new to digital programme delivery all together).

While the SRF may overtly focus on standardizing a component of data collection, the quality of the data produced and the governance framework agreed on are foundational to the success of all components that follow after. Organizations will be incentivized to adopt the SRF not only because its purpose and content are clear, but more as a result of a clear, well-understood, and easy to implement process is laid forth.[5] Even if a form is well designed, if its rollout is not well managed, there is no uptake, and its use will not scale. Addressing this risk, IOM has continued to step up and provide relevant support for SRF rollout, training at least 80 participants from 32 organizations (both local and international), with district level trainings forthcoming. Though more comprehensive and sustainable support structures will need to be considered for the long-term – with other organizations also contributing resources to stand up a shared training support.

Despite being the more 'straightforward' piece of what is being proposed (relative to the FRS), **the SRF rollout does pose one of the first opportunities to help build positive trust between humanitarian actors beyond what has been agreed upon to date.** In many ways,

[4] Draft RTT PP
[5] Latest approach found in "SRF Dissemination & Monitoring Strategy"

a final definition "what" (in terms of system architectures) is less important now – as discussions are still being had – than organizations feeling as if they are consistently engaged and supported throughout the process of design, decision making, and development of any technical components. Without this hands-on support, the entire effort may be diminished as actors may not have the means or expertise to fulfil their commitments (i.e. to rollout a new digital form, adopt new technologies, update workflows, etc.).

Furthermore, the SRF presumably relies on convincing actors to use already trusted digital platforms. Its rollout will provide critical insight onto roadblocks to adoption, even when technologies are well known and trusted. As diverging internal policies, capacity and resource limitations, and distributed decision making will all need to be mitigated by lead agency/agencies leading SRF rollout and, at a later stage, management. If sequenced well, this experience will **greatly** inform if and how pushes towards biometrics may also play out, provided actors' relative unfamiliarity with biometric systems and may have internal restrictions that may need to be addressed.

As of September 2025, pilots of the SRF continue to expand in tandem with efforts to further detail FRS architecture. One critical decision is to articulate and represent where **unique identifier functions** sit within the overall ecosystem. Whether functions & oversight are embedded within Kobo form/SRF auspices or a standalone piece within the FRS, technicalities and governance around UID management should be well detailed as it is the most critical aspect needed for interagency data sharing to scale (sans biometrics).

Federation of Registration Systems (FRS)

The real challenge comes with data consolidation across myriad systems, even when data standards are agreed upon. This is especially important of digitally-prominent organizations who may not necessarily fall under implementing / consortium partner relationships, unless there is a clear decision made to tier organizations based on these relationships. Hence the introduction of the FRS concept. Based again off directions of travel indicated within the policy paper, the FRS is technically serves as a data exchange system (DES). The combination of the SRF and FRS are meant to encourage a more federated approach to implementation where partners may play different roles depending on their willingness and capacity. For example, partners who have biometric functions and operational capacity may serve as "registration partners," where others may enter IP-like relationships in order to collaborate with them. Other agencies may only serve as data consumers, pulling data (collected by other agencies) in order to provide assistance without actually needing to do household-level data collection or registration themselves.

Though this is dependent on how data from the SRF is ultimately intended to be used and managed. Without more consensus on the FRS **primary functions**, however, aspects of the FRS can be interpreted similar to digital components found in social protection systems (e.g. social registry, IBR, etc.). The FRS is presented as a "pass through" for data, not a primary host, though there have also been indications that the FRS will display unique IDs and other

data points in which organizations can review. While this idea is clear, its technical execution still requires the FRS to host data – even if temporarily as a pass through. The data will still enter and exit FRS architecture. This is an important point to consider with technical and legal experts, as the FRS will technically host data even if not in a traditional manner like a data registry.

Regardless of final designs, the FRS is dependent on the existence of trustworthy digital data and in some interpretations, well-functioning information management systems (IMS). This includes in-house systems as well as third-party platforms. Active IMS in Somalia include platforms like SCOPE and HOPE, while Red Rose is a commonly known platform primarily contracted by INGOs. On the development side, digital public good (DPG) IMS like OpenCRVS and OpenSPP are in early stages of discussion, development, and/or rollout in conjunction with the Government of Somalia and its partners. Needless to say, however, the majority of actors do not have sophisticated IMS, relying on some combination of mobile data collection platforms (e.g. Kobo) and data management applications (e.g. Excel) to support their work.

As of September 2025, FRS design discussions are well underway, with a related workshop scheduled for 16 September 2025. While system diagrams and architecture are slowly being proposed, a clear outline of current (or "very soon to be") business process and data flows is not yet publicly shared. This includes where and how agencies beyond the 5-6 listed (UN+SCC) fit into overall processes and systems.

Identified Gaps & Risks

Metrics

As indicated from other consultancy reports,[6] there is a need to build trust and transparency amongst actors at all levels in order to provide foundation for digitally-reinforced data sharing and governance. Inclusivity is key even in the earliest stages of design and conceptualization; hosting inclusive conversations proactively sharing survey results or concepts as they iterate will be an important step for those spearheading or facilitating SRF/FRS discussions on behalf of the humanitarian community.

In an effort to help establish **baseline metrics**, two (2) rapid surveys are open for completion. The goal is to diversify and widen perspectives, regardless of whether multiple responses come from a single agency.

1. Rapid Survey: Biometrics
2. Rapid Survey: Digital Stock take

[6] Meraki Labs consultancy report (2025)

In addition to establishing consistent feedback loops with organizations piloting and/or scaling adoption of the SRF, FRS, or biometrics, organizations can also be encouraged to track certain metrics while they pilot and rollout new digital components. Below are some example metrics, with note some may not be applicable to all stakeholders depending on their tier of engagement or entry point to the FRS (more below). These metrics should be considered in addition to those outlined in the "Interoperable Registration System Implementation, Dissemination and Monitoring Strategy" (January 2025).

Performance

- **Data Submission Rates**: % of expected submissions actually received – SRF form, data to FRS, biometric data
- **Timeliness**: How quickly data is submitted & processed (i.e. shareable) after collection
- **Enumerator Performance**: Number of forms submitted per enumerator; error rates per enumerator
- **Efficiency:** time spent completing X operational phase (e.g. registration) decreases

Effectiveness

- **Data Sharing**: How often is data successful shared (into the FRS) and received (from the FRS)
- **Coverage**: Geographic or demographic coverage of "interoperable data" expands
- **Referrals**: Number of successfully made referrals (using SRF/FRS tools) increases
- **Duplicates**: Number of duplicates identified (through the FRS) decreases

User Engagement & Trainings

- **Training Completion**: % of enumerators trained successfully on: SRF, FRS, biometrics
- **Active Users**: % of registered users [organizations] who submitted /requested data in the last X days
- **Support Requests**: Number of field complaints logged, addressed
- **User Satisfaction**: Survey feedback on app/platform usability.

Scalability & Sustainability (Long-term)

- **Cost per User or Beneficiary**
- **Integration with Government Systems**
- **Diversified Usage**: are tools used beyond the initial scope?
- **Adoption by Local Stakeholders**: number of local organizations taking over system components

Purpose-driven Interoperability

Simply put, the majority of humanitarian data is hosted by a small percentage of actors: four UN agencies (FAO, IOM, UNHCR, WFP) and one consortium (SCC/Concern). This data is generated and "owned" by myriad other actors (dictated by implementing/consortium

partnership agreements), though digital data is overarchingly managed by these major agencies.

This thus raises the question as to whether the final design of the FRS is driven by the largest data holders or system owners, or whether it is designed inclusive of all humanitarian systems and capacities – including international and national organizations that are not contractually bound to one (of the five) largest actors, and/or potentially not using digital tools within their programmes. Noting that there is no right or wrong method, rather just a need to confirm a clear strategy help actors better understand why they may (or may not be) as engaged in the moment on seemingly large data reforms.

It is a significant technical achievement to realize the FRS even with a small pool of IMS, though achieving this with a small pool of organizations does not necessarily achieve overarching goals of interoperability. Essentially because the "rules of federation [would] inform interoperability standards." This suggests some version of *de facto interoperability*, whether intentional or not.[7] As "interoperability by design" requires far more consolidation of efforts and consensus building across actors in order to develop shared principles, common standards and systems collectively;[8] the Digital Convergence Initiative's (DCI) interoperability efforts provide a relevant proxy to consider what this effort can entail.[9] De facto interoperability is not inherently bad, though does require those implicated to be aware of and agree to the approach and its governance. Otherwise, it may sow distrust among certain actors, especially those without 'large data systems' to substantiate any level of influence on discussion.

Integrations

To date, preliminary diagrams of the FRS indicate an integration-based approach. While integrations offer a technically viable way to exchange data across identified systems, this 1-to-1 or 1-to-many approach can hinder inclusiveness and scalability if not designed properly. This approach also brings complexity to data sharing agreements (DSAs), especially if bilateral DSAs are required vis-à-vis system design. Integration-based approaches also require clear and consistent stewards, while also denoting what the single source of truth amongst datasets actually is. Integrations across an evolving network of data systems requires constant level of customized effort, negotiation, and maintenance which may not be feasible or cost effective in the long run.

---

[7] *De facto interoperability* occurs when there is a dominant market actor whose product—as result of overwhelming market share—dictates standards for all other market actors; a simple example is Microsoft Excel (i.e. XLS and XML formats). The challenge with this approach to interoperability is that the product owner can choose to accept or ignore any future standards set by a community of actors, as their product ultimately sets a *de facto* standard through its sheer dominance over the market. (Source: Nogueira, E., Moreira, A., Lucrédio, D. et al. Issues on developing interoperable cloud applications: definitions, concepts, approaches, requirements, characteristics and evaluation models. J Softw Eng Res Dev 4, 7 (2016).)

[8] BASIC Yemen research - forthcoming

[9] DCI: https://spdci.org/interfaces/

Proprietary Solutions: Deduplication
Multiple service providers have focused on "de-duplication" offerings within their existing "Software as a Service" (SaaS) platforms. The majority of these platforms focus on supporting teams with restricted and unrestricted cash programmes, whether transferring vouchers, tokens, or fiat currency to individuals. Many of these service providers rely on blockchain and re-imagined data partitions in order to support autonomous data management and data principles. Though the sophistication of features (validated or not) is not in question. The challenge comes in terms of voluntary adoption strategies, especially in absence of HCT mandating the use of an identified product (which they themselves do not manage a contract or service agreement for). As such, key considerations for private sector service providers include validated experience leading:

- Multitenant contract management *(beyond consortiums, which have clear mandates and strong governance, unlike a 300+ actor response)*
- Operations at comparable scale to Somalia response *(v. pilots or early-stage projects)*
- Business experience and continuity *(>3 years with myriad clients from all tiers – UN, INGO, local)*

Middleware: Working Examples from Social Protection– Chile & Uganda[10]
Chile and Uganda present two indicative models and approaches to multi-actor data exchange. In 2008, Chile launched the *Sistema Integrado de Información Social (SIIS)* [Integrated Social Information System]; while aspects of the system were in use as early as 2002, the SIIS was officially codified and ratified in 2008. Uganda's Social Protection MIS (SPMIS) was launched over a decade later in 2021 with support from DFID/FCDO, Unicef, and the World Bank (among others). Uganda's SPMIS followed the development and implementation of the National Single Registry (NSR) in 2020, which integrated various MIS with the National Identification & Registration Authority's (NIRA) national ID registry.

Chile's SIIS enables **automated, real-time data exchange** between various government databases (health, education, labor, social services) to assess and update individuals' eligibility for social programs. The SIIS acts as an **interoperability layer** [middleware] between sectoral databases and the *Registro Social de Hogares* (RSH), the national social registry. It is managed by the Ministry of Social Development, with each participating agency retaining its own data while also complying with shared standards and API protocols coordinated through the middleware. Importantly, data is not centralized. Middleware instead **queries original databases on demand** to provide the latest data received in support of eligibility assessments and other coordination. The SIIS does not update information; it simply provides a secure way for various departments to safely access verified data from disparate sources.

[10] World Bank. (2021). Sistema Integrado de Información Social (SIIS), Ministerio de Desarrollo Social de Chile: Diagnóstico rápido y recomendaciones (Report No. 265291614755039574).

Uganda's SPMIS, on the other hand, connects systems from various ministries (i.e. Gender, Labour & Social Development), local governments, and the national ID registry (NIRA). SPMIS acts as an **integration layer** for *identity verification, payment tracking,* and general *case management*. This means data hosting is mixed, with some data stored centrally and other data accessed via integrations with external systems. It also means that the SPMIS's different components directly support different phases of implementation. Its core components include: **(1)** Registration, **(2)** National Identification and Registration Authority (NIRA) – national ID, **(3)** National Single Registry (NSR), **(4)** Payments, **(5)** Monitoring & Evaluation Tools, and **(6)** Middleware layer supporting integrations.

Where Chile's system provides autonomy to participating ministries' ways of working, Uganda's model presumes last mile activities are funneled through a single system, the SPMIS – where payments, M&E, and other activities are initiated from; different tools feed registration data to the SPMIS (1), which then interfaces with the NIRA through middleware to verify an individual's identity while also assigning a unique ID within the SPMIS system (2, 6). Relevant records are stored within the NSR, where middleware supports standardization and deduplication of new data submissions before being stored (3, 6); the NSR serves as the **single source of truth** for beneficiary data that support future targeting, payments, and M&E. The NSR thus sends payment instructions to various payment providers, all connected again through the middleware layer (3,4,6). Finally, follow-up M&E is conducted by teams who query the NSR and connected payment systems through the SPMIS. Uganda's **middleware** thus acts as a translator and router, routing form data to verification systems, querying biometric matches (NIRA), consolidating records (NSR), sending secure payment instructions, and aggregating data for comprehensive M&E.

	Chile – SIIS & RSH	**Uganda – SPMIS**
Middleware Role	Real-time query bridge between sectoral databases and social registry	Integration layer connecting registration, ID verification, and payment systems
Main Use	Dynamic eligibility assessment and service coordination	Registration, ID validation, benefit delivery, and monitoring
Data Location	Data stays with original agencies (decentralized); middleware pulls when needed	Mixed: some data stored centrally; others accessed via links to external systems
Interoperability Focus	Health, education, labor, civil registry, municipal services	NIRA (ID system), MoGLSD, local governments, payment providers
Governance	Ministry of Social Development (MDSF); API rules and access controlled by law	Ministry of Gender, Labour and Social Development (MoGLSD); donor-supported transition to national ownership
ID Integration	Yes – integrates with national ID (RUN – civil register ID)	Yes – integrates with NIRA (biometric national ID)
Data Protection	Strong legal frameworks and layered access controls	Emerging frameworks; guided by donor and national privacy policies
Modularity	High – agencies connect via APIs; no need for new platforms	High – designed as modular components (registration, payments, etc.)

It is important to note that in both models, respective Ministries of Social Development/Labour are the single entity accountable to maintaining and governing respective middleware layers. So while the design and development of middleware is critical, it is equally important to reach consensus around who will ultimately host, manage, and maintain FRS-related middleware on behalf of humanitarian agencies.

Data Sharing Agreements (DSA)

Terms of DSAs codify real-life data exchange processes, increasingly informed by digital architecture underpinning them. As such, it is difficult to draft future-proofed DSAs while so many technical details of the FRS remain undetermined. DSAs and other governing documents will be greatly informed by whatever model of middleware is chosen. As such, the need for myriad bespoke and/or bilateral DSAs may become less critical. There is a distinction between bilateral DSAs and one that could cover FRS middleware alone. Essentially by entering a DSA **with the FRS** [whether the FRS is hosted by a single entity or interagency body mandated to oversee it], the same rules and expectations to comply apply to all signatories. Whether employing a query-based model [Chile's SIIS] or integration layer [Uganda's SPMIS], data sharing can be governed by a single overarching "DSA" rather than customized DSAs per agency. In practice, data sharing terms would look more similar to an End User License Agreement (EULA) than bespoke DSA. This of course only covers data accessed via the FRS; any data shared *outside* of FRS architecture or governance structures would still need bilateral DSAs.

Foundational

Governance – as with most discussions related to interoperability, governance structures can be seen as a north star for any eventual digital development efforts. This not only regards responsibilities associated with data hosting or sharing, but also more practical aspects of procurement, adaptation, maintenance, and support. Step one to all of this is a ***policy framework*****,** providing an overarching mandate for the interoperability effort; HCT endorsement on various Policy Papers can be considered as such. Governance informs systems designs, but also requires deputizing decision makers. This is difficult to do in decentralized humanitarian contexts, though identifying **neutral hosts** or stewards is the first step. This does not necessarily mean one agency controls all, but rather inclusive bodies or steering committees are established to start defining and make consensus-based decisions on topics[11] such as:

- **Standards/Processes:** shared implementation principles; modifications (i.e. updates to SRF); data structures and formats [based off SRF]; identity management and data sharing standards; process flows
- **Data:** quality assurance; legal basis (e.g. consent) / ethical considerations; data ownership and access rights – who can access what, under what circumstances; adjudication and conflict resolution; data lifecycle management – when to update, retain and erase what type of data.
- **Legal:** data sharing frameworks (templates); regulatory compliance / jurisdiction; hosting expectations for shared infrastructure (to inform technical requirements)
- **Digital Components*:** developing and maintaining digital systems (e.g. middleware, interoperability gateways); documenting technical standards, security and data standards; scoping and addressing new technical needs as they arise
- **Support*:** rollouts, troubleshooting / escalation plans, onboarding and system(s) maintenance

***Digital components + support function hand-in-hand, only separated here to emphasize equal importance and distinctions in expertise each area needs.*

Suggested Roles: Stakeholder alignment is one of biggest challenges digitalization efforts face. The sooner clear forums for collaboration are established, the sooner governance roles (per above areas) can be defined. Though considering current funding climates, many organizations are not in a position to responsibly commit resources to such efforts. To date, OCHA has been identified as one option to lead discussions regarding interagency data governance; they are also identified as a prime candidate to also host resulting digital / interoperability systems. Though recent aid funding cuts have impacted all organizational outlooks – including those of major UN agencies. As organizations continue grappling with forced restructures and consolidations, agency-specific options to host the FRS may be less reliable than initially assumed. As such, suggested governance roles and responsibilities

[11] This is an indicative, non-exhaustive list

are outlined below with indications of membership composition or personnel, knowing the exact capacity and availability of resources within each agency is still being determined. Some roles may also lend themselves to consolidation.

Trust building, however, is also key to the success of interoperability efforts. One way to foster this is to incorporate checks-and-balances within governance frameworks, where no single agency is perceived to be singularly driving decision making by sheer nature of housing appropriate expertise. This may take form as instituting co-leads for areas, or ensuring there is strong trust built in the composition of an inclusive and participatory Data Governance Steering Committee who approves personnel per role.

1. **Data Governance Steering Committee**, whose role is to provide strategic oversight and serve as a final decision-making body on matters. Members to include senior leaders from participating agencies (supported by technical advisors): all major MIS hosts; 1-2 local agencies to represent IP perspective; 1-2 international agencies to represent non-IP/consortium perspective. ***Suggested responsibilities*** to include:
    a. Setting governance vision and principles
    b. Approve overarching data sharing agreements (DSA) and policies regarding participation in FRS (not to approve bilateral DSAs)
    c. Resolve interagency issues
    d. Ensure alignment with national or donor policies

2. **Data Governance Lead** (rotational or non-implementing agency), whose role is to provide executive leadership for data governance and liaise with Steering Committee; this can mirror other hosted roles, such as Consortium Directors or cluster coordinators, who are meant to represent the perspective of multiple agencies equally. This can be assigned to an agency, though ideally an individual (within assigned agency) is still presented and approved to play this role. ***Suggested responsibilities*** to include:
    a. Driving strategy, policy, and compliance (subject to Steering Committee approval)
    b. Coordinating cross-agency initiatives (e.g. FRS piloting; feedback sessions)
    c. Liaising with stakeholders and funders
    d. Ensuring complementarity with sector-wide data frameworks (incl. emerging national systems)

3. **Data Stewards / Sector Data Leads** identified per participating agency as well as deputized within sector-specific clusters/working groups, whose role is to ensure the quality and integrity of data within a specific agency and across sector. ***Suggested responsibilities*** to include**:**
    a. Maintaining metadata and data dictionaries [response/sector-specific]
    b. Enforcing data standards and definitions [agency level]
    c. Managing data lifecycles (entry, storage, retention) [agency level]
    d. Coordinate data validation and cleaning [agency level]

4. **Interoperability Architect (Technical Lead)**, whose role is to ensure all participating systems can exchange and use shared data. Similar to the CDO, this role can be hosted by an agency, but a specific individual should be identified and approved in order to foster transparency and agreement around this individual's remit. This role would be accountable to work directly with contracted service providers, whether for-profits/third-parties or teams housed within specific agencies (e.g. BraVeX team). ***Suggested responsibilities*** to include:
    a. Designing APIs, standards, and integration protocols
    b. Supporting implementation of interoperability frameworks vis-à-vis set data standards (e.g. informed by SRF)
    c. Assessing existing systems for compatibility, confirming what technical changes are needed
    d. Developing documentation and technical materials to support interoperability implementation across various MIS
    e. Resolving technical issues with data exchange
    f. Monitoring performance and security of integrations

5. **Data Privacy & Security Officer** (rotational), whose role is to safeguard sensitive data across shared systems (i.e. FRS). Many agencies already have these officers in place for internal data management, including oversight on data privacy within systems used to operationalize the SRF and/or integrate with the FRS. This role while similar in practice would be accountable to data exchanged through the FRS and any resulting data that may be temporarily or permanently hosted within it, even if non-sensitive (i.e. unique ID numbers). This role may require standalone level of effort, or be combined under other roles - depending on final remit. ***Suggested responsibilities*** to include:
    a. Enforcing data protection policies vis-à-vis shared architecture (e.g. GDPR)
    b. Conduct risk assessments and audits, including interagency data privacy impact assessments (DPIA); support agencies who may not have capacity to conduct internal DPIA upon their request
    c. Monitor compliance with privacy regulations
    d. Handle breach notifications and mitigation

6. **Legal & Policy Advisor** (rotational, seconded by agency), whose role is to provide legal guidance for data sharing agreements, service contracts, and other binding commitments related to shared architecture. ***Suggested responsibilities*** to include:
    a. Draft/review any *interagency* data sharing DSAs, memorandums of understanding (MoUs), service level agreements (SLAs) - not bilateral
    b. Ensure alignment with local and international laws
    c. Advise on intellectual property and data ownership

7. **Technical Reference Group,** comprised of programmatic representatives nominated by participating agencies. Agency representation can mirror membership of Steering Committee or remain distinct. This group's role would be to represent the needs and constraints of each type of partner agency (including those not formally represented). ***Suggested responsibilities*** to include:
    a. Communicate agency-specific requirements and constraints, ensuring a diversity of needs are represented
    b. Ensure internal / operational compliance with interagency agreements
    c. Report issues and updates to the steering committee vis-à-vis FRS/SRF use (see Metrics)

8. **Capacity Building / Training Coordinator**, who support trainings-of-trainers for agencies in order to improve digital literacy and operational capacities to support FRS/SRF adherence. This role is currently being fulfilled by IOM, where the support team is (among other tasks):
    a. Creating and managing trainings for identified staff
    b. Supporting onboarding of new stakeholders
    c. Building sustainable local capacity for data governance

Additional supporting roles may also include an interagency ***data analyst*** (for interagency reporting and insights, likely covered by expanded remit of OCHA IM), and a ***change manager*** (to guide cultural and operational changes required to adopt FRS/SRF); this role could be subsumed under the expectations of a technical reference group or as a temporary support position providing ad hoc advisory throughout, at request of various agencies.

Costs and resources – especially for agencies that neither have digital systems in place nor have the resources to do so. Considering biometrics standalone: assuming 75% of recorded implementing organizations commit to the use of biometrics, that still consists of over 200 organizations to include within a rollout. Based off quite conservative estimates regarding fit-for-purpose biometric hardware, software platforms, rollout, and support at scale – the rollout of each device purchased can fall around US$1000 each (inclusive of hardware).[12] One could imagine a well-resourced agency taking on procurement on behalf of the response, distributing / licensing out devices as such.

- ***Nb.*** *Considering the variety of models of biometrics available, it is important – as with any new introduction of technology – to appreciate the operational context in which the tool will be used. For Somalia, this includes options that comply with customs regulations/procedures, work "offline first" and ideally, are opensource to support integrations more readily.*

[12] Based off 200 total organizations x 10 devices**:**
- **US$400** per mobile biometric device (US$1m total - with 5% annual replacement);
- **$10,000 per org** (US$200,000 total) setup and training cost;
- **US$5,000 per month** (US$60k annually) software & data hosting fees, shared across organizations; **US$3000 per month** (US$36k annually) service provision: technical support, onboarding, troubleshooting – estimated minimum **US$500 per month** ($6,000-12,000 annually), per organization

Cost Sustainability – in-house / agency-hosted digital solutions and infrastructure are exposed to unique funding risks. As opposed to third-party platforms (e.g. for-profit DPGs) or government-funded digital systems, digital solutions within the humanitarian sector are primarily reliant on project grants and/or time bound donor investments. Cost recovery models are also not always clear. With recent funding freezes and budgets, new considerations come to light. Will actors trust that a "humanitarian hosted" system will stay online despite policy shifts within donors? What ensures business continuity of humanitarian "digital public goods"? Perceived unreliability is as detrimental to early adoption as actual system failures, so cost considerations must be built in to decision making in order to ensure resulting systems are in fact viable beyond grant cycles. As a first step, Total Cost of Ownership (TCO) should be well outlined as solution designs and/or service providers emerge. This includes any components that may be hosted by humanitarian agencies. Any actor playing the role of a technology service provider should be considered as such, regardless of whether they are for-profit, non-profit, or hybrid vendor.

Complexity of rollout – related to cost and resources is the complexity of a large-scale rollout that for some agencies requires adoption of multiple new tools at once. It is comparable to an enterprise-level / organization-wide rollout of new processes and multiple systems. Heavy investment is required, specialized expertise is needed, and rollout timelines can be long (even if actual development / integration timelines are not). While rollout would happen in a staggered manner, it still requires willingness and significant, ongoing effort by the entire humanitarian community and/or participating organizations. The procurement effort and logistics for the biometric component alone would be challenging enough. Community engagement and buy-in is also be key, and may take time to establish given the stage of concept development.

Capacity – having, for example, a local organization transition from no digital data collection tools to adopting full-fledged biometric systems is both risky and somewhat unreasonable to expect. A sizeable portion of organizations will fall into this category, again reiterating the need for a thoughtful capacity building/strengthening plan and peer-to-peer support to ensure proper sensitization occurs, uptake takes place and appropriate safeguards are put in place. Embedded monitoring mechanisms are also key in order to ensure performance enhancements while also catching and mitigating community-based challenges as they arise.

Scope and purpose – as noted during the Inception Report, it becomes difficult to fully realize a digital concept without clear driver(s) and purpose(s) articulated and prioritized. For example, "deduplication of _____" (e.g. MPCA recipients), or "referrals for _____," which requires major referral actors inputs across all sectors. Scope and purpose definition is also needed for tools like the SRF. For example, is it to be used for a particular caseload (e.g. new arrivals), during specific times (e.g. emergencies) and for specific purpose(s) (e.g. identity management for humanitarian assistance). Some lines will ultimately need to be

drawn in terms of which beneficiaries' data is included under the FRS and under what circumstances – including regular quality checks on legacy data.

Trust – trust frameworks bolster interoperability efforts. In non-humanitarian settings, trust is built among actors through certifications, compliance audits, and transparent policies. This often translates into technical mechanisms used for authentication, authorization, and secure data sharing. In humanitarian settings, trust frameworks are not as easily defined, especially if distrust exists across different levels and actors of the response. As noted before, one way to incrementally build trust around the interoperability effort is to be as inclusive and transparent with proceedings as possible. This includes when designing rollout plans, like for the SRF. Over time, actors and affected populations will gain confidence and trust in the methods and processes being proposed, with opportunity to help shape them.

- ***Nb.*** *Introducing biometrics with an over purpose to prevent fraud may cause challenges. Without* ***transparent evidence to substantiate,*** *nor* ***benefits clearly articulated to communities*** *– the introduction of biometrics may be met with resistance, especially without support from community leaders, as already shown in other countries.*[13]

Technical

Technical variability as organizations' digital systems vary greatly in capabilities and sophistication. To avoid exacerbating this "digital divide," funding and technical support will be needed for organizations lagging on pre-requisites for interoperability (e.g. quality digital data, MIS), to ensure quality performance and avoid exclusion. In a protracted crisis like Somalia, operating with a partial view on humanitarians' digital landscape is difficult, however, despite knowing major data holders' systems and their purpose definition. Despite the number of agencies to be included, it is important to develop a comprehensive data ecosystem map to better appreciate the magnitude and complexity of proposed efforts. As it is clear both the SRF and FRS presume a baseline level of digitalization, and in the case of the FRS, a functional programmes MIS.

Operational variability. Registration practices (and even definitions of) also vary across different actors. Some provide assistance or service delivery at the household level, others rely on centre-based / centralized distributions. This means large efficiency gains to "speed up verification" (as example) do not extend equally to all actors, depending on whether they conduct activities house-to-house or not. As with any digital effort, establishing **common operational indicators** will be important in order to monitor whether digital tools are in fact improving bottom lines of beneficiary satisfaction and timely aid delivery. This will also help maintain objectivity in operational reviews of systems, without relying solely on service providers' reports.

[13] Ethiopia, Bangladesh, and Yemen to name some.

Absence of case management. There is a potential leap of logic, moving from systems with no UID generation to the application of biometrics. Case management systems may be a middle ground or 'intermediary' step for some organizations. Mirroring mobile data collection tools, case management tools additionally assign a globally unique identifier (GUID) to each registered 'case,' which is used to link data together over time. Whether capturing information on a person, household, or camp site. Case management systems also provide a backbone to many social protection systems – which the SRF / FRS concept seemingly mirrors. If strictly looking at ways to improve UID management, case management platforms can be a helpful bridge to move beyond "manual" UID generation through one-way survey tools like Kobo.

While the SRF/FRS concept promotes the concept of a unique identifier, the non-biometric form suggested is not based off personally identifiable information (PII). The household ID is instead a combination of a form submission timestamp and preassigned codes (for the location of registration and registering organization).[14] As Kobo is a one-way data collection tool,[15] it is not immediately evident how UIDs are issued for to members within a household, nor how overlaps in household members are identified sans biometrics when conducting follow-ups either by the same user account that registered or especially when another user account is conducting follow-up (even if based in the same agency).

Absence of Unique IDs. Functional unique IDs form the backbone of interagency interoperability efforts.[16] Unique IDs help protect PII, while also facilitating efficient, low-bandwidth deduplication with basic digital architecture. Based off preliminary designs for the FRS, interagency / system relevant unique IDs need far more technical solidification. Some key considerations are whether **all agencies registering households** will either connect their independent data systems to a consolidated, shared UID generator (to ensure consistency and uniformity from a single source) or whether each agency will be trusted to autonomously generate and assign UIDs in a consistent manner, pooling UIDs on a periodic basis for deduplication checks. In either case, PII data is stored nor needs to be shared. There are myriad designs and workflows that can facilitate efficient UID assignment and management. Considering the fact that static UIDs will be in use by majority of agencies for some time (as opposed to biometrics), it is critical for whatever approach and/or digital aides supporting UID prioritize **ease of adoption** and avoid **vendor lock-in**.

Identity Management. Unique ID generation and "functional" ID management is not the same as identity management. Identity management requires free and well-informed consent by individuals, especially when capturing sensitive biometric data. (It also typically

[14] form-submission-timestamp_registration-district+organization-ID
[15] This means data recall is not readily supported; mobile users effectively send their data to a server without ability to 'recall' or 'add to' that information from their mobile accounts on follow-up visits.
[16] For more information regarding the difference between **functional** and **foundational** IDs, see here.

assumes there is an ultimate authority to issue legal identity.) In Somalia, biometrics are considered sensitive, requiring informed consent by law.[17]

In practice, capturing biometrics of all household members – that in some interpretations of the SRF/FRS, may still be *potentially* eligible beneficiaries – blurs lines with the Somali Government's own digital identity initiative. Regardless of whether data or systems are shared between humanitarian and GoS actors, the two stakeholder groups' biometric ambitions still mirror one another operationally. Though with one group (i.e. GoS) relying on biometrics to support the issuance of legal digital identities, to ***verify*** whether a person is who they claim to be by validating identities against trusted sources; this is a one-time process reliant on access to other formal datasets. The other group (i.e. humanitarians) using biometrics as a form of unique identifier to primarily help ***authenticate*** individuals over time, confirming that someone is the same person who was originally verified. This distinction seems slight, but does raise questions that need further clarification:

1. Will all agencies – large or small, international or local – have the authority and/or technical ability to **verify** individuals' identities? This means having "trusted data sources" identified and solutions in place to validate information against them to ensure the person is who they claim to be.
    a. Relatedly, where does identity verification sit within an agency's implementation cycle – before or after a household is deemed eligible for assistance and therefore ready for "official" enrolment or registration into a system as an active recipient of aid or services? (This harkens back to whether biometrics are collected on all potential beneficiaries, during needs assessments, or only from households deemed eligible for assistance.)
2. If not all agencies are sanctioned to formally "verify" beneficiaries, what is the cost justification of biometric systems for actors who may only use the tool to **authenticate** already enrolled beneficiaries on the spot (e.g. during a distribution)? Are other forms of authentication, like issuing one-time-pins (OTP) or cross-referencing non-biometric data (e.g. SIM cards) more relevant or cost effective for this tier of implementers?

If the SRF/FRS systems aim to first **verify identities** (rather than support ongoing authentication relying on biometric unique identifiers), it should be detailed as such to flag the necessary safeguards that must be embedded, likely mirroring those put in place by

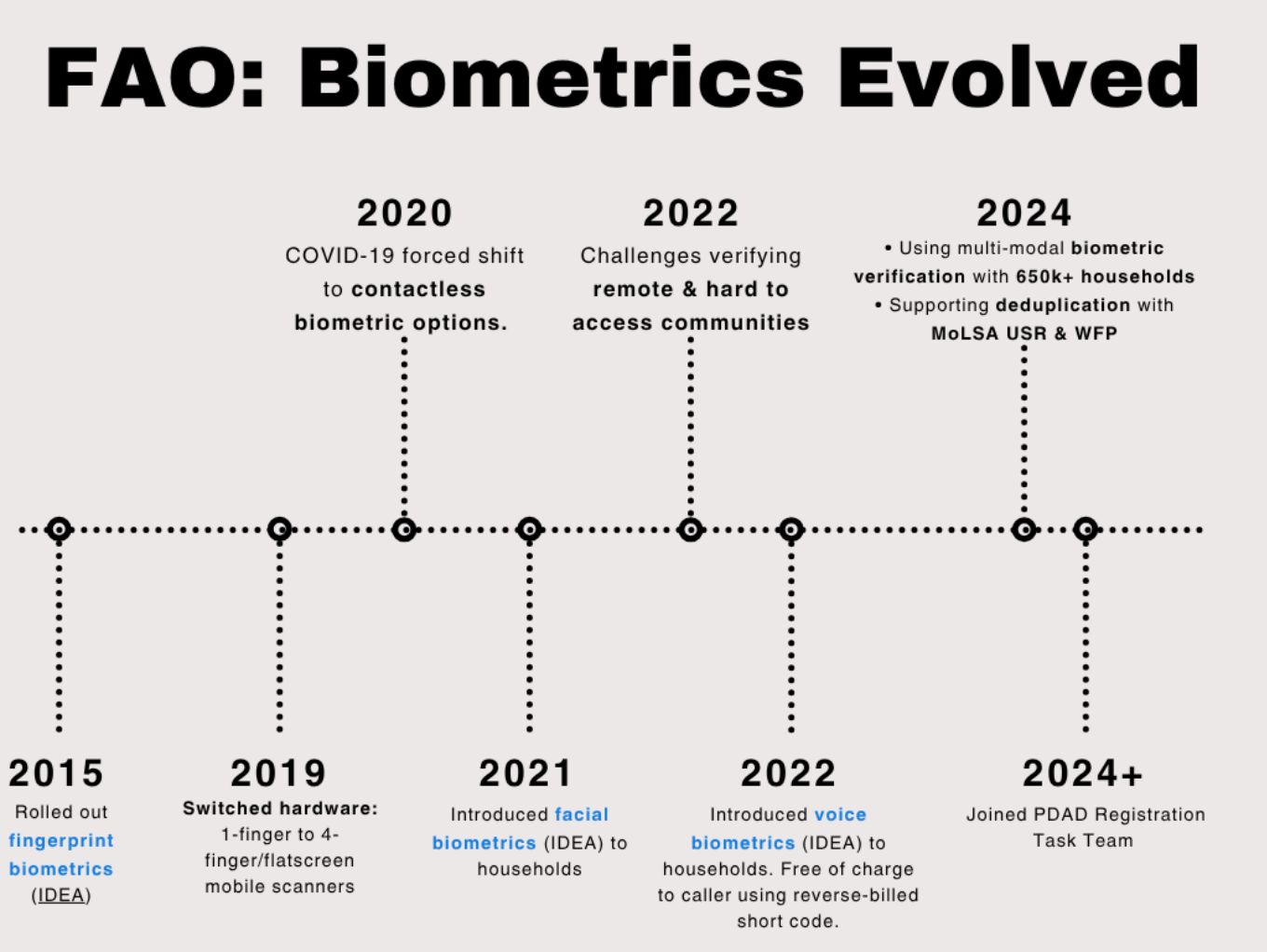
[17] "*In many legal systems, biometric information is considered "Sensitive Data". Consequently, special, detailed requirements apply to the Processing of this type of data, directly affecting the lawfulness of the Processing in the event that they are not met… However, biometric data are considered to be Sensitive Data, and therefore Data Controllers should obtain the Data Subjects' Consent. In addition, given that biometric information may only be collected directly from the individuals concerned, and in contrast to some other methods of data collection and Processing, it is generally feasible for Humanitarian Organizations to obtain Consent to use biometric data. However, it will not always be possible for Humanitarian Organizations to collect unambiguous, free, informed and documented Consent for the Processing of biometric data…"*
(ICRC Data Protection Handbook, 2024)

government ID authorities.[18] There may be need to clearly distinguish between a set of agencies empowered to officially verify identities on behalf of all humanitarian actors (similar to a "single" authority having mandate to issue a government-sanctioned ID), versus those who must simply authenticate whether the right person is receiving the aid or services they are enrolled to receive.

Authentication (v. Verification). Well-designed identity *authentication* supports different ways to confirm an individual is who they say they are – based on previously provided information. This can include cross-referencing a combination of biometrics, certified documents, device serial numbers, or SIM card data. In short, biometrics are one of many forms of "trusted data" that can be used to continually authenticate an individual's already verified identity. More importantly, inclusive designs allow beneficiaries / users to choose their preferred form(s) of authentication, with some options (e.g. OTP) requiring more secondary verifications than others (e.g. biometrics). Biometrics systems are also not full proof and have several data protection implications. Some form of 'secondary' or backup verification option will be needed when system malfunctions or devices malfunction. It is important to think through how the implementation cycle can continue if a technical component (like biometrics) is removed from the equation. In some cases, continuation will not be possible – though these instances should be limited especially while using technologies within communities.

[18] See DPI Safeguards Framework and DPI Map on Digital ID systems for relevant models to adapt.

Biometrics Spotlight: FAO's Evolution



Approach

Inclusive Cost/Benefit. (See next page.) As elements of the SRF and FRS are better defined, it is important to consider each component through a cost/benefit analysis that includes all stakeholder groups, including beneficiaries. For knowns, such as biometrics, this will be supplemented with surveys and targeted consultations. For less clear concepts, like the FRS, a common reference will need to first be agreed upon in order to host comparative conversations. As the concept itself is complex with few existing models to share as an example.[19] More pointedly, it is important to consider trade-offs between *speed* (regarding decision making, digital development, or rollouts) and *trust building* (including establishing safeguards). This potential trade-off will be elaborated upon in the final report alongside others, as also informed by survey results and follow-up consultations.

[19] Closest approximations would be government-led examples of middleware or DPI; see page 10.

Sensitization. Biometrics are undoubtedly sensitive and many agencies will have hesitations to adopt these systems, whether due to high cost, low capacity, lack of accountability, or otherwise. Even transitioning from one mobile data collection tool to another may meet resistance. The more agencies are nudged to engage in early-stage design discussions, the more fears and concerns can be raised and ameliorated. Where perceived risks (borne from lack of information) can also be separated from actual challenges actors need to resolve.

Incentives. There are still fundamental gaps to address across actors that ultimately influence their ability to voluntarily adopt what is being proposed by donors or "bigger agencies." Without addressing this imbalance of incentive structures, donors will likely be put in a position to mandate adoption of pre-determined solution designs some agencies had little part in deciding upon, even to point of making funding contingent on accepting these terms. As noted above, incentives for adopting the SRF and FRS primarily rely on improving performance et al. metrics per agency. The adoption of biometrics, however, is more sensitive and thus requires targeted incentivization strategies if it is indeed expected to serve as the primary form of UID management.

Solution hunting. There are a variety of options that can facilitate secure, scalable data exchange between myriad organizations. Each presents different benefits (and constraints), whether architectural or business. With nearly all "humanitarian validated" solutions focusing primarily on deduplication alone. It is important to note, that these solutions **do not** typically support unique ID generation and/or management. Rather, they rely on externally-provided UIDs (e.g. tax ID) to ensure uniqueness across entries. It is important to note, many of these "deduplication" solutions—in their current forms—do not work without being provided an externally generated UID. While the systems themselves

Example Cost/Benefit: Biometrics[20]

Requirement	Expected Benefit	Who Benefits	Activity	Output	Outcome	Indicators	Notes & Purpose
Donor Requirement - Use Biometrics to prevent fraud	Reduction in aid diversion	• Donor - accountability of spend • Implementers- comply with donor *If verifiable through baseline studies and/or quality monitoring, it can also be assumed:* • Aid recipients - receive expected aid	Biometric registration added; biometric verification added to distributions/follow-up; staff appropriately trained; risk mitigation plan developed / updated; sensitization plans developed and run	Rollout plan + procurement/ logistics strategy + rollout + maintenance (incl. updates, troubleshooting, etc.)	Programme objectives are met with confidence - X distributed to Y people	• % of records with biometric UID rises from X% to Y% by Year 2, 3, 5 • Reported instances of fraud drops from X per year to Y* • Recipients report a high level of satisfaction with a programme - increase from X to Y	• Requires accurate baseline statistics re. deduplication ratio and risk-benefit analysis (DPIAs etc.) • Requires constant monitoring of satisfaction levels among communities • Requires constant costs/ resources for maintenance purposes
Biometrics for de-duplication purposes (interagency)	Reduction of unintentional overlaps in assistance provision	• Donor – best use of resources • Implementers - more effective use of resources	Whole-of-response agreement + plans for biometric adoption; Biometric registration added; biometric verification added to distributions/followups; staff appropriately trained; risk mitigation plan developed / updated; sensitisation plans developed and run	Interagency commitment + Rollout plan + rollout	Program objectives are met with confidence, with best use of resources	• % of records with biometric UID rises from X% to Y% by Year 2, 3, 5 • Reported instances of unintentional overlap from X per year to Y* • Recipients report a high level of satisfaction with assistance - increase from X to Y • Organizations report better use of resources - increase from X to Y	• Requires accurate baseline statistics re. unintentional overlap • Requires constant monitoring of satisfaction levels among communities • Requires an adjudication strategy

[20] Adapted from Simprints

Requirement	Expected Benefit	Who Benefits	Activity	Output	Outcome	Indicators	Notes & Purpose
Donor Requirement - Use Biometrics to prevent fraud	Reduction in aid diversion	• Donor - accountability of spend • Aid Recipients - receive expected good	Biometric registration added; biometric verification added to distributions/follow-up; staff appropriately trained; risk mitigation plan developed / updated; sensitization plans developed and run	Rollout plan + procurement strategy + rollout	Program objectives are met with confidence - X distributed to Y people	• % of records with biometric UID rises from X% to Y% by Year 2, 3, 5 • Reported instances of fraud drops from X per year to Y* • Recipients report a high level of satisfaction with a program - increase from X to Y	• Requires accurate baseline statistics re. incidents of fraud • Requires constant monitoring of satisfaction levels among communities
Biometrics for de-duplication (interagency)	Reduction of unintentional overlaps in assistance provision	• Donor – best use of resources • Implementers - more effective use of resources	Whole-of-response agreement + plans for biometric adoption; Biometric registration added; biometric verification added to distributions/followups; staff appropriately trained; risk mitigation plan developed / updated; sensitisation plans developed and run	Interagency commitment + Rollout plan + rollout	Program objectives are met with confidence, with best use of resources	• % of records with biometric UID rises from X% to Y% by Year 2, 3, 5 • Reported instances of unintentional overlap from X per year to Y* • Recipients report a high level of satisfaction with assistance - increase from X to Y • Organizations report better use of resources - increase from X to Y	• Requires accurate baseline statistics re. unintentional overlap • Requires constant monitoring of satisfaction levels among communities

Lessons from the Field: Inclusive Selection Processes

The **Ukraine Cash Working Group (CWG)** used a multi-step **review and assessment methodology** to review its existing deduplication system.[1] A similar process was used in Gaza (2025), in an effort to facilitate a transparent and inclusive decision making process before any one system was deployed or reinforced by donors.

Purpose and Context. Ukraine's reassessment was mandated by the **CWG's MPC Deduplication SOPs (Oct 2024)**, requiring **bi-annual system reviews**. The review updated the 2022 assessment to reflect expanded scope (beyond MPC), new tools, and legal/technological changes.

Process for System Evaluation.
The assessment followed a **seven-step methodology**:

1. **Identified needs and challenges:** user feedback and operational challenges related to deduplication and data management were gathered
2. **Agreed on minimum requirements:** the CWG collectively defined baseline standards deduplication systems must meet
3. **Assessed systems against these requirements:** technical and functional assessments were done per system
4. **Evaluated governance models:** each system's data ownership, access control, and compliance with legal frameworks was revived
5. **Organized provider briefings:** system providers were invited to present functionalities and compliance details. This included UN, INGO, and private sector vendors.
6. **Analyzed resource implications:** financial and staffing requirements for sustainable implementation were assessed
7. **Produced comparative summary and recommendations:** a scoring and narrative comparison led to prioritized recommendations.

Minimum Evaluation Criteria. Systems were tested across four thematic areas:

I. **Functionality & Features:** Deduplication capability (for assistance and registration), referral capacity, user interface in Ukrainian
II. **Governance:** Joint ownership potential, member participation equality, follow-up processes, interoperability, and data subject rights
III. **Analysis:** Access to aggregated statistics and data analytics
IV. **Data Protection & Security:** Compliance with **GDPR and Ukrainian law**, adherence to **data minimization principles**, **encryption**, and **open-source verifiability**.

Scoring Methodology. Each system was rated against **12 minimum requirements**, using a **3-point scale**.[1] Evaluations included resource mapping (setup, maintenance, support, staffing).

Neutral and Expert Oversight
The **OCHA Centre for Humanitarian Data** supported the process end-to-end, ensuring global alignment with humanitarian data responsibility standards and comparability with other CWG exercises (e.g. in Gaza). OCHA also served as a neutral, non-operational broker—a critical non-negotiable to ensure objectivity throughout the review process. The Ukraine CWG's deduplication system review is a prime example of a standardized, evidence-based, and collaborative process combining technical evaluation, governance analysis, data protection review, and sustainability planning**.** While an emerging approach, it is one that should be strongly considered by the Somalia response and adapted as part of discussions finalizing final directions of travel regarding the FRS.

Interoperability with Social Protection

Digital Public Infrastructure (DPI). Humanitarian actors should expect Government DPI efforts to pursue the use of digital public goods (DPGs) and even adopt emerging data standards set by groups such as the Digital Convergence Initiative (DCI), GovStack, and others. While these efforts may not match humanitarians' development timelines or needs, it is crucial for those supporting technical standards or digital components on behalf of humanitarian actors to engage with those doing similar on the Government side. This includes engaging with service providers and standards committees - that some agencies are already a part of (WFP). This is particularly important as biometrics and other identity management tools are being considered concurrently by humanitarian actors and the Government of Somalia. Without this cross-communication, already expensive systems run the risk of needing substantial retrofitting[21] in the future, especially as Somalia's national ID programme expands.

Next Steps

A **phased approach** prioritizes incremental adoption**,** strong governance**,** and evidence-based scale-up to minimize risks and maximize operational value in the eyes of target adopters.

Phased Roadmap

Phase	Key Activities	Expected Outputs
Preparatory (Current) *Q1–Q2 2025*	• Finalize **Single Registration Form (SRF)** tool and onboarding materials. • Launch additional SRF pilots with M&E framework. • Endorse **governance structure** and roles. • Define **Federated Registration System (FRS)** architecture options.	• Approved SRF onboarding package. • Baseline pilot reports. • Draft FRS functional design. • Endorsed governance TORs.
Phase 1: Foundation *Q3–Q4 2025*	• Continue SRF onboarding with adoption targets. • Draft **Data Sharing Agreements (DSA)** and legal templates. • Initiate FRS technical design. • Conduct cost-benefit analysis for FRS adoption.	• SRF systematically adopted by core partners. • Finalized legal templates. • Initial FRS architecture blueprint.

[21] Especially if biometrics standards (ISO) do not coincide with NIRA's selected biometric system.

Phase	Key Activities	Expected Outputs
Phase 2: Prototyping & Testing *Q1–Q3 2026*	• Scale SRF implementation. • Develop and test **FRS prototype** with selected agencies. • Train partner staff on interoperability workflows. • Run interoperability proof-of-concept using lightweight tools (e.g., HotPot).	• Expanded SRF adoption. • Tested FRS prototype. • Operational governance and legal processes.
Phase 3: Integration & Biometric Readiness *Q4 2026–Q2 2027*	• Validate biometric integration options and develop safeguards. • Launch **consent framework** and data protection guidelines. • Pilot biometric deduplication (optional, small scale). • Expand FRS to additional agencies.	• Approved biometric use policy. • Pilot results on UID and deduplication. • Updated FRS technical design.
Phase 4: Scale & Sustainability *Q3 2027–Q4 2028*	• Full FRS rollout with secure middleware. • Capacity building for local actors. • Integration with **government systems** where feasible. • Finalize **cost-sharing and hosting model** for sustainability.	• Fully functional FRS. • Sustainability plan with cost allocation. • Established interoperability pathways with national systems.

Governance and Compliance Priorities

Based off the latest iteration of HCT Task Teams (TT) focused on (1) Accountability, (2) Effective & Prioritized Response, and (3) Common Enablers, FRS/SRF efforts will remain cross-cutting. Regardless of which TT assumes ultimately oversight authority over FRS software development, there are multiple conversations around FRS/SRF governance that need prioritization prior to. **Data governance** is a present and ongoing discussion, while system designs are being formalized, where legal frameworks and data protection standard procedures are also covered by TTs. While SRF/**FRS project governance** exists, it mirrors traditional humanitarian task teams' ways of working rather than a multi-actor product/software development effort. Weak project management and oversight will hamper any software development effort. In order to better formalize this piece of the work, a qualified (potentially temporary) TT should at minimum establish a clear statement of work (SOW) for the Technical Lead, mirroring governance documents normally used when working with a technology service provider. This means tapping IT and/or procurement expertise in order to adapt "traditional" service provider management tools for this unique scenario of an appointed service provider.

A strong SOW typically includes clearly outlined digital outputs,[22] expected service provisions (e.g. trainings), monitoring processes, and a general roadmap / milestone dates. The Technical Lead (who is also the "service provider" in this case) ideally does not draft their own SOW. Rather, a representative body can draft a SOW—with inputs from a Technical Lead—to ensure everyone lands on the same page around the purpose, design, and rollout stages of the resulting software(s).

- **Legal Frameworks:** establish a multilateral MoU with embedded DSA clauses to define roles, responsibilities, and data rights
- **Data Protection:** continue implementing Data Protection Impact Assessments (DPIAs) for all participating agencies; draft template SOPs for data sharing policy
- **UID & Semantic Standards:** adopt a minimum data set aligned with the SRF and maintain a shared data dictionary**;** see efforts in Yemen, Gaza

Technical Clarity

- Finalize the **SRF tool and onboarding package** for humanitarian partners, including pilot results and reflections
- Confirm the **FRS architectural approach** (federated vs centralized); this should also be reviewed by governance technical leads; designs underway [IOM]
- Confirm comprehensive approach to **unique ID generation** that ensures uniqueness and usability across all humanitarian actors; feasibility to adopt and sustain new technologies / UID processes is the critical metric, not digital sophistication
- Design **cost-benefit analysis and risk assessment** for early adopters of SRF and/or integration with FRS

Conclusion

The SRF and FRS represent significant and ambitious steps towards enhancing coordination, efficiency, and accountability within humanitarian response systems in Somalia. Across multiple consultations, surveys, and policy developments, it is evident that there is both momentum and widespread recognition of the need to modernize and harmonize registration and data-sharing practices. Success, however, hinges not only on technical execution, but also equitable inclusion, clear governance, and sustained trust-building among all actors.

The SRF offers a tangible first step, standardizing registration inputs and providing a critical opportunity to foster collaboration through common data collection practices. Yet its utility will depend on thoughtful operationalization, accessible training, and support mechanisms that accommodate the varying capacities and digital maturity levels across actors. The FRS,

[22] Where each components' relevant business processes, data flows, user needs are clearly outlined.

while promising in scope, requires further articulation regarding governance structures, data flows, and core use cases before its full potential can be realized. While indications show that IOM / BraveX will supply critical pieces of digital architecture to actually FRS functionalities, this needs further clarification within the larger ecosystem of data management. More pointedly, actors will need clear articulation as to whether the FRS is meant to intentionally reinforce tiers of data management (per large MIS hosts) – or whether it is intended to include / meet the needs of a wider audience who may also already be using digital data tools. Biometric integration further complicates the landscape, demanding robust safeguards, informed consent mechanisms, and community-level sensitization to ensure ethical deployment. While its benefits in reducing duplication and supporting identity verification are evident, its application must be carefully scoped to avoid unintended consequences or erosion of trust—especially among vulnerable populations. More so, if there are limited agencies who will actually be able to adopt and apply biometrics – more attention needs to be made for non-biometric UID options. In short, the default for most actors is likely *non-biometric* UIDs, so processes and technical solutions should focus on ensuring these UIDs are well designed and implemented.

Key gaps remain in terms of legal clarity, cost sustainability, system integration, and stakeholder alignment. Importantly, any future-state architecture must reflect not only the technological ambitions of a few but the practical realities and needs of many—especially national and local actors without existing digital infrastructure. The balance between advancing innovation and reinforcing inclusion will define the credibility and long-term viability of this effort. As the humanitarian ecosystem in Somalia navigates this digital transition, coordinated investment in governance, capacity-building, and open dialogue will be essential. Only through collective ownership and mutual accountability can the vision of an interoperable, inclusive, and secure humanitarian data ecosystem be achieved.

Annex 1

System Landscape: Humanitarian-hosted UID/Deduplication

Three primary systems used by humanitarians in recent responses. Open source and/or humanitarian-hosted solutions are prioritized. While a variety of relevant proprietary systems exist, the likelihood one of these systems will be adopted by certain actors at scale is low unless a donor (or group of donors) mandates use of a private sector product. This would also require very clear procurement guidelines and up front alignment across hundreds of actors.

Feature	WFP Building Blocks	IOM BraVe	HotPot
Primary Function	Blockchain-based platform for deduplication of beneficiaries & transfers	Biometric and demographic deduplication & verification	Lightweight, rapid deduplication tool for CWG partners
Hosting / Ownership	WFP (global platform)	IOM-hosted	Open license, developed by CCD
Core Technology	Blockchain ledger + integration APIs	Biometric matching engine + integrated MIS	Web app with secure upload & matching algorithm
Strengths	• Strong audit trail • Integrated with WFP payment systems	• High biometric accuracy • Strong fraud prevention	• Quick to deploy • Minimal data fields required
Limitations	• Complex onboarding for non-WFP actors • Requires blockchain familiarity	• Requires biometric equipment & consent • High infrastructure cost	• Not a full MIS • Limited to deduplication

Considerations:

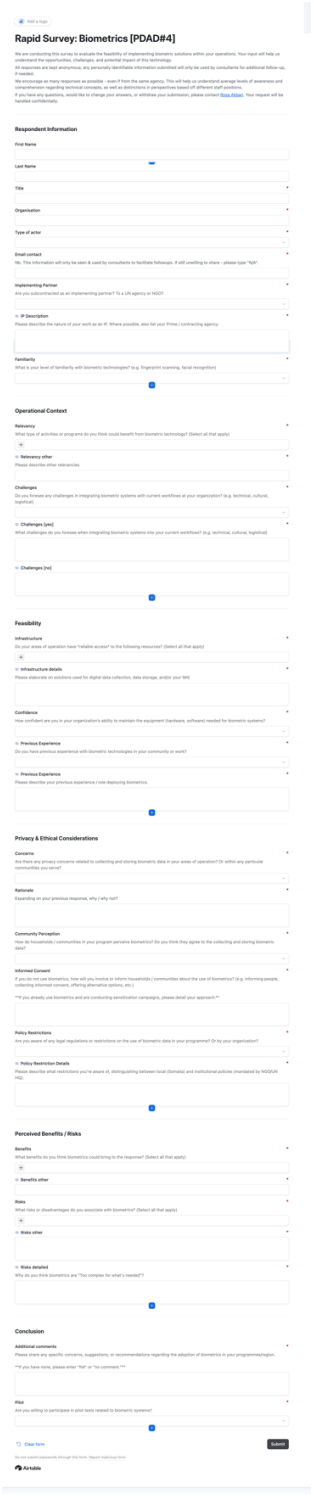
- **HotPot or similar lightweight interoperability tools** can be used for early-stage deduplication pilots and/or basic validation of governance or SOPs, while more robust solutions can be phased in at later date once configured and tested properly
- **API-based integration** between major MIS, supported by some combination of systems like Building Blocks or BraVe needs significant investment and technical commitment
- There may be practical scenario where all three (3) options can coincide, each targeting different capacity levels while still feeding information into the predesignated single source of truth (SSoT) / primary system
- Biometric-based matching is technical challenge. Before investing, important for agencies to also agree discuss governance, consent, and legal safeguards; certain agencies may have constraints which may limit effectiveness of using as primary or preferred form of UID

Annex 2

[LINK TO LIVE FORM]

some follow-up questions hidden due to display conditions

Sample Survey: Biometrics



Rapid Survey: Biometrics [PDAD#4]

We are conducting this survey to evaluate the feasibility of implementing biometric solutions within your operations. Your input will help us understand the opportunities, challenges, and potential impact of this technology.
All responses are kept anonymous; any personally identifiable information submitted will only be used by consultants for additional follow-up, if needed.
We encourage as many responses as possible - even if from the same agency. This will help us understand average levels of awareness and comprehension regarding technical concepts, as well as distinctions in perspectives based off different staff positions.
If you have any questions, would like to change your answers, or withdraw your submission, please contact Rosa Aldasi. Your request will be handled confidentially.

Respondent Information

First Name

Last Name

Title *

Organisation *

Type of actor *

Email contact *
NB. This information will only be seen & used by consultants to facilitate followups. If still unwilling to share - please type "N/A"

Implementing Partner *
Are you subcontracted as an implementing partner? To a UN agency or NGO?

IP Description *
Please describe the nature of your work as an IP. Where possible, also list your Prime / contracting agency.

Familiarity *
What is your level of familiarity with biometric technologies? (e.g. fingerprint scanning, facial recognition)

Operational Context

Relevancy *
What type of activities or programs do you think could benefit from biometric technology? (Select all that apply)

Relevancy other *
Please describe other relevancies

Challenges *
Do you foresee any challenges in integrating biometric systems with current workflows at your organization? (e.g. technical, cultural, logistical)

Challenges [yes] *
What challenges do you foresee when integrating biometric systems into your current workflows? (e.g. technical, cultural, logistical)

Challenges [no]

Feasibility

Infrastructure *
Do your areas of operation have "reliable access" to the following resources? (Select all that apply)

Infrastructure details *
Please elaborate on solutions used for digital data collection, data storage, and/or your IMS

Confidence *
How confident are you in your organization's ability to maintain the equipment (hardware, software) needed for biometric systems?

Previous Experience *
Do you have previous experience with biometric technologies in your community or work?

Previous Experience *
Please describe your previous experience / role deploying biometrics.

Privacy & Ethical Considerations

Concerns *
Are there any privacy concerns related to collecting and storing biometric data in your areas of operation? Or within any particular communities you serve?

Rationale *
Expanding on your previous response, why / why not?

Community Perception *
How do households / communities in your program perceive biometrics? Do you think they agree to the collecting and storing biometric data?

Informed Consent *
If you do not use biometrics, how will you involve or inform households / communities about the use of biometrics? (e.g. informing people, collecting informed consent, offering alternative options, etc.)

If you already use biometrics and are conducting sensitization campaigns, please detail your approach:

Policy Restrictions *
Are you aware of any legal regulations or restrictions on the use of biometric data in your programme? Or by your organization?

Policy Restriction Details *
Please describe what restrictions you're aware of, distinguishing between local (Somalia) and institutional policies (mandated by NGO/UN HQ).

Perceived Benefits / Risks

Benefits *
What benefits do you think biometrics could bring to the response? (Select all that apply)

Benefits other *

Risks *
What risks or disadvantages do you associate with biometrics? (Select all that apply)

Risks other *

Risks detailed *
Why do you think biometrics are "Too complex for what's needed"?

Conclusion

Additional comments *
Please share any specific concerns, suggestions, or recommendations regarding the adoption of biometrics in your programmes/region.

If you have none, please enter "N/A" or "no comment."

Pilot *
Are you willing to participate in pilot tests related to biometric systems?

Clear form

Submit

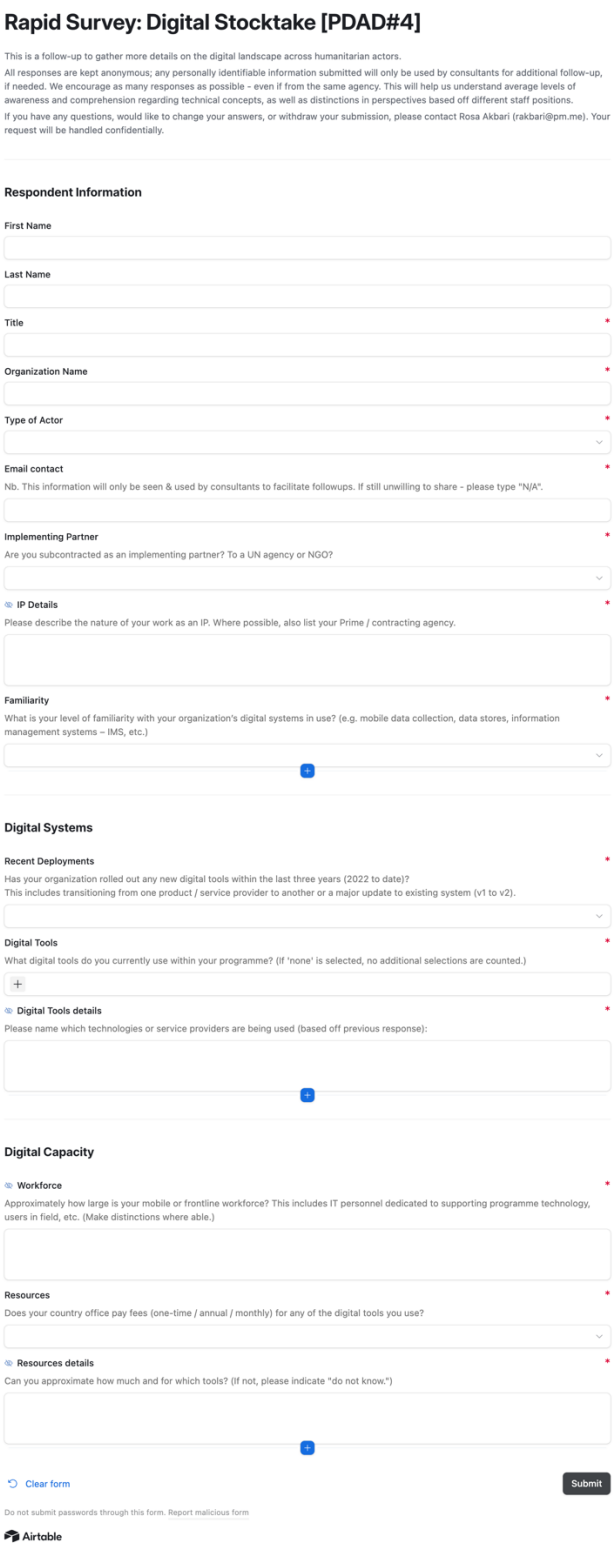
Do not submit passwords through this form. Report malicious forms

Airtable

Annex 3

LINK TO LIVE FORM

some follow-up questions hidden due to display conditions



Rapid Survey: Digital Stocktake [PDAD#4]

This is a follow-up to gather more details on the digital landscape across humanitarian actors.

All responses are kept anonymous; any personally identifiable information submitted will only be used by consultants for additional follow-up, if needed. We encourage as many responses as possible - even if from the same agency. This will help us understand average levels of awareness and comprehension regarding technical concepts, as well as distinctions in perspectives based off different staff positions.

If you have any questions, would like to change your answers, or withdraw your submission, please contact Rosa Akbari (rakbari@pm.me). Your request will be handled confidentially.

Respondent Information

First Name

Last Name

Title *

Organization Name *

Type of Actor *

Email contact *

Nb. This information will only be seen & used by consultants to facilitate followups. If still unwilling to share - please type "N/A".

Implementing Partner *

Are you subcontracted as an implementing partner? To a UN agency or NGO?

IP Details *

Please describe the nature of your work as an IP. Where possible, also list your Prime / contracting agency.

Familiarity *

What is your level of familiarity with your organization's digital systems in use? (e.g. mobile data collection, data stores, information management systems – IMS, etc.)

Digital Systems

Recent Deployments *

Has your organization rolled out any new digital tools within the last three years (2022 to date)?
This includes transitioning from one product / service provider to another or a major update to existing system (v1 to v2).

Digital Tools *

What digital tools do you currently use within your programme? (If 'none' is selected, no additional selections are counted.)

Digital Tools details *

Please name which technologies or service providers are being used (based off previous response):

Digital Capacity

Workforce *

Approximately how large is your mobile or frontline workforce? This includes IT personnel dedicated to supporting programme technology, users in field, etc. (Make distinctions where able.)

Resources *

Does your country office pay fees (one-time / annual / monthly) for any of the digital tools you use?

Resources details *

Can you approximate how much and for which tools? (If not, please indicate "do not know.")

Clear form

Submit

Do not submit passwords through this form. Report malicious form

Airtable

Annex 4
LEARNING FROM REAL-WORLD EXAMPLES

How Middleware Works: IndiaStack example

Example: Identity Verification

1. Service Request Initiated
• Bank, telecommunications, government, etc. portal needs to verify user identity for onboarding or transaction

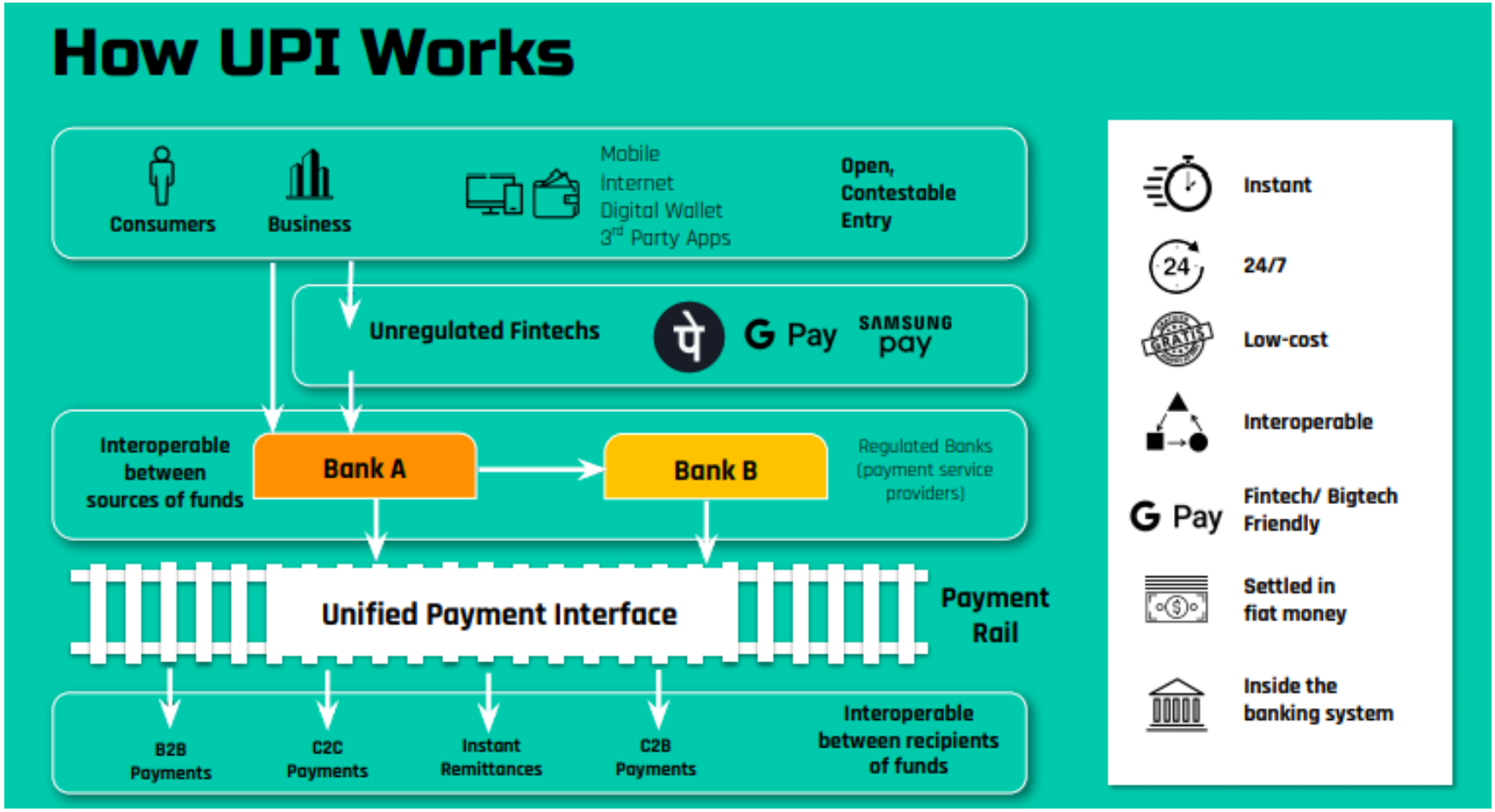
2. IndiaStack/Middleware API Call
• Request is sent via IndiaStack's Aadhaar Authentication API or e-KYC API to UIDAI's backend **[identity layer]**
• UIDAI is the *Unique Identification Authority of India;* equivalent to Somalia's NIRA

3. User Authentication
• Client provides Aadhaar number [UID]
• Client completes authentication factor (biometric, OTP, or demographic) + grants digital consent
• Middleware captures digital consent + generates encrypted consent artifact for transaction **[data / consent layer]**

4. UIDAI Response via IndiaStack Middleware
• Requesting Entity → Middleware [with layers] → routed to UIDAI ….
  - Middleware ensures secure routing, applies encryption, and validates service provider credentials
• Middleware returns a secure, digitally signed response to service provider:
  "Yes/No" authentication result, or
  Full KYC data (name, DOB, gender, address), if consented

5. Service Provisioning
• Requesting entity uses verified identity to open an account, process payments, deliver benefits, etc. within their own systems

KEY: Indicates a **[Component Layer of IndiaStack]**.



Source: 'Identity, Payments and Data Empowerment' - Nandan Nilekani (2019)

In simplified terms, each layer of IndiaStack hosts APIs/gateways to civil repositories (such as UIDAI). Where identity, payments, and secure data exchange (incl. consent) are distinct layers within the overall "stack." In the example below, the Unified Payments Interface (UPI) is the "middleware" used to support payments (not account opening, which also relies on data

exchange via the identity layer). In this example, the UPI [middleware] is actually *"a payments markup language that runs on a central switch operated by a bank-owned non-profit known as the National Payments Corporation of India (NPCI). In simple terms, there is one NPCI server which all the licensed banks are connected to. This server sends messages to and from between all the banks, with NPCI as the middleman."*[23]

Relevance Recommendation for FRS: Detail out what the middleware "layers" of Identity Verification/Deduplication comprise of and which agency will play ultimate hosting role. It is also important for all actors to understand these digital components do not represent data stores, only throughputs to exchange data between requestors and requestees—though this still does not negate the fact a piece of digital architecture still needs to be built, utilized, and maintained, which cannot happen without a designated entity (e.g. India's NPCI is the UPI's steward.)

[23] Vir, Aaryaman, and Rahul Sanghi. "The Internet Country: How India Created a Digital Blueprint for the Economies of the Future." *Tigerfeathers*, 14 Jan. 2021, tigerfeathers.in/p/the-internet-country.

Types of Data Registries[24]

Trait	**Social Registry** (Government-led)	**Integrated Beneficiary Registry** (Single Registry)	**Somalia Federation of Registration Systems** (Humanitarian only)	**Status in Somalia**
Focus	Collects and manages broad data, serving as an entry point for individuals or households to be considered for social assistance programmes	Centralizes existing data about beneficiaries already registered in one or more assistance programmes, while maintaining individual autonomy of data sources / IMS	Consolidates existing data about beneficiaries already registered in one or more assistance programmes, while maintaining individual autonomy of data sources / IMS	n/a
Primary Functions	Identification, registration, and eligibility assessment. More simply, a *targeting database*.	Tracking, managing, and coordinating delivery of assistance or services to registered beneficiaries	• Promoting accountable and effective humanitarian response by addressing aid diversion risks • Promoting principles of data minimization: reduce repetitive registrations conducted by disparate actors. For example, where a specific pool of actors run registration data collection on behalf of other agencies	n/a
Population Coverage	Current AND potential / future beneficiaries	Limited only to those enrolled in programmes	SRF caseload to be defined – new arrivals? Protracted IDPs? All vulnerable pop? Only active beneficiaries?	TBD
Governance	Managed by a central authority or government agency, with strict data governance and privacy standards	Cross-departmental or interagency coordination body to ensure collaboration and interoperability across different IMS	Undefined	**Low** or nascent
Operational Role	Targeting and eligibility assessments to determine who qualifies for social programs	Program management, monitoring, and coordination of benefits and services	TBD – identity management, referral management	TBD

[24] "Social Registry" and "IBR" refer to generic system traits, not specific to systems in use or under development in Somalia.

Integration Role	*Entry point* for social protection schemes (incl. programme IMS)	Coordination *hub between* active social protection schemes and IMS	*Identity management* & referral *hub between* active humanitarian programmes and IMS to primarily support: De-duplication, referrals • Bilateral integration APIs and 'interoperability bridges' do exist among largest actors • Number of functional IMS across all actors is less clear	**Medium low** – some of largest IMS have demonstrated bilateral interoperability. Unclear how this translates to whole-of-system integration. Referral systems are also under review and may prove to need further strengthening before serving as a defining driver for the FRS
Data Included	Broad, census-based data on general population or certain demographics. Focuses on socioeconomic and demographic profiles, including employment, housing, income, etc. Updated periodically to reflect changes in household circumstances[25]	Programme specific data about individuals or households receiving assistance, including types of assistance, frequency, and longitudinal history. Regularly updated by routine data collection per programme implementation cycle tracking status of assistance, delivery, etc.	Data collected by the SRF Other supplementary data collected by individual agencies would be shared on a purpose-driven basis. (e.g. to adjudicate a duplicate beneficiary)	**Medium high** in terms of data volume, once major agencies adopt SRF **Low** or nascent in terms of organizational spread, until SRF is fully rolled out
Data Sources	Assessments, enrollment campaigns, and other systems (e.g. civil registries)	Data aggregated from programme-specific IMS (e.g. health, cash transfers)	Data aggregated from programme-specific IMS (e.g. cash transfers, NFI)	**Low** or nascent, until all IMS are identified and integrated. More importantly, with contingencies in place for organizations operating *without functional IMS*
Data Relevancy	Updated periodically to reflect changes in household circumstances.	Regularly updated by routine programme data collection tracking status of assistance, payment delivery, etc.	Regularly updated by routine programme data collection tracking status of assistance, payment delivery, etc.	**Nascent**, until all IMS are identified and integrated. More importantly, with contingencies in place for organizations operating *without functional IMS*

[25] In the case of Somalia Unified Single Registry (USR), update frequency and feasibility remains undefined

Design	To store and *process large amounts of data* from multiple sources (e.g. tax registry). When linked with IBRs, can act as a pool of eligible participants to register into programmes.	To *integrate* and *synchronize* data from multiple programme-specific databases. When linked with social registry, can provide comprehensive view over assistance delivered to a single person or household.	Hybrid? This is dependent on how teams intend to use SRF data, and more pointedly – *if they have functional IMS to link* or not.	**Medium low** – in theory, SRF data can be used as a targeting database – more similar to a social registry. If this is the case, the FRS
Key Use Cases	**- Identifying** vulnerable populations for targeted programs **- Targeting:** Evaluating eligibility for multiple programs based on unified data	- **Monitoring** assistance or service delivery **- Coordinating** assistance or service delivery across multiple programmes	Hybrid? This is dependent on how teams intend to use SRF data, and whether its driving targeting or capturing activities / transactions after fact. More simply, if the SRF will in fact be used a **registration tool**, or whether it is Part 1 of a multi-step process to assess, target, and official register a new recipient.	
Challenges	- Major inclusion and exclusion errors based on quality of assessment / census - Requires frequent updates in order to maintain timely, relevant data	- Potential for duplication of data if coordination processes are weak - Relies on other programme IMS for timely data and assured data quality	TBD – - Still potential for duplication of data if coordination processes are weak - Major inclusion and exclusion errors based on SRF, use of biometrics, etc. - Introduction of new technologies introduce data protection risks; requires complex Data Privacy Impact Assessments (DPIA) - Depending on host / design, sustainability of systems (uptime, maintenance, etc.) dependent on somewhat unsustainable revenue streams (e.g. project grants)	
Integration Complexity	- Does NOT provide Unique ID / Digital Identity management - Needs to link with diverse databases (e.g. civil	Requires integrating multiple programme IMS across different actors, each often with inconsistent data formats and standards	TBD – dependent on existing systems involved and final agreements on SRF/ FRS	**Medium high** - Technical capabilities shown across some systems; subject matter expertise exists, though concentrated

	registries, tax systems) for accurate targeting			