USAID
FROM THE AMERICAN PEOPLE

Photo Credit: Guimba Souleymane, International Red Cross Niger

How To: Create Digital ID for Inclusive Development

A Companion to Identity in a Digital Age: Infrastructure for Inclusive Development

Acknowledgements

This guide was written under the Digital Frontiers project (United States Agency for International Development Cooperative Agreement No.AID-OAA-A-17-00033). The content and views expressed in this guide do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

Special thanks are extended to the guide author Chrissy Martin Meier as well as Aubra Anthony and Shachee Doshi of the Strategy and Research team in USAID's Center for Digital Development who have overseen the guide's development and provided invaluable feedback throughout. In addition, Stephanie Creed and Komal Bazaz Smith were the Activity Managers on the Digital Frontiers project and helped steer the guide from conception to publication. The guide has benefited from the guidance of many USAID staff including Rhonda Stewart, Ruco Van der Merwe, Krissy Celentano, Rachel Fowler, Rebecca Saxton-Fox, Morgan Holmes, Assia Ivantcheva, Cael Savage, Ethan Takahashi, Craig Jolley and Mina Hasaj who have generously shared their knowledge and expertise. Without your support, this guide would not have been possible. Finally, particular acknowledgement goes to the graphic designer Daphne Karagianis who prepared the guide for publication.

Contents

Why are we talking about identification?

1.1 billion people globally lack official identity, as estimated by the World Bank. Identity unlocks formal services as diverse as voting, owning a financial account, registering a business or other assets, enrolling in school, and having complete health records. Having a formal, sustainable identity is a key step in helping people to share in the gains of economic and social development.

Who should care about identification?

Identification is complex, and requires cooperation between a wide variety of stakeholders. While national governments are most likely to drive the establishment of formal ID services, development practitioners, including **donors, program managers,** and **M&E specialists,** should be aware of how their project or activity fits into the overall ID ecosystem in their country or context. When a development project decides to create their own ID, it can help achieve project objectives -- but it can also contribute to a fragmented, siloed ID ecosystem, creating problems you can read about in the introduction.

The purpose of this guide

This guide aims to: 1) illustrate how investments in ID systems can both positively and negatively impact individuals and their households, through the illustrative stories of Mary, Joy, and Samuel; and 2) provide specific how-to guidance to help donors, program managers, and M&E specialists get started in thinking about ID ecosystems. This guide is specifically targeted towards USAID staff and implementing partners who are providing **direct support** on ID systems, providing **advisory services** to government ministries, or are trying to find ways to **identify beneficiaries** in a project or activity (regardless of the sector).

How should I use this guide?

This guide is intended to be modular. In other words, you don't have to read from beginning to end. Click around to find the sections and tools most relevant to you. Start with the introduction, and go from there. Read, discuss with your colleagues, and think about how you can put some of these ideas into action in your own project or activity.

Photo Credit: Guimba Souleymane, International Red Cross Niger

Introduction

Photo Credit: Simone D. McCourtie / World Bank

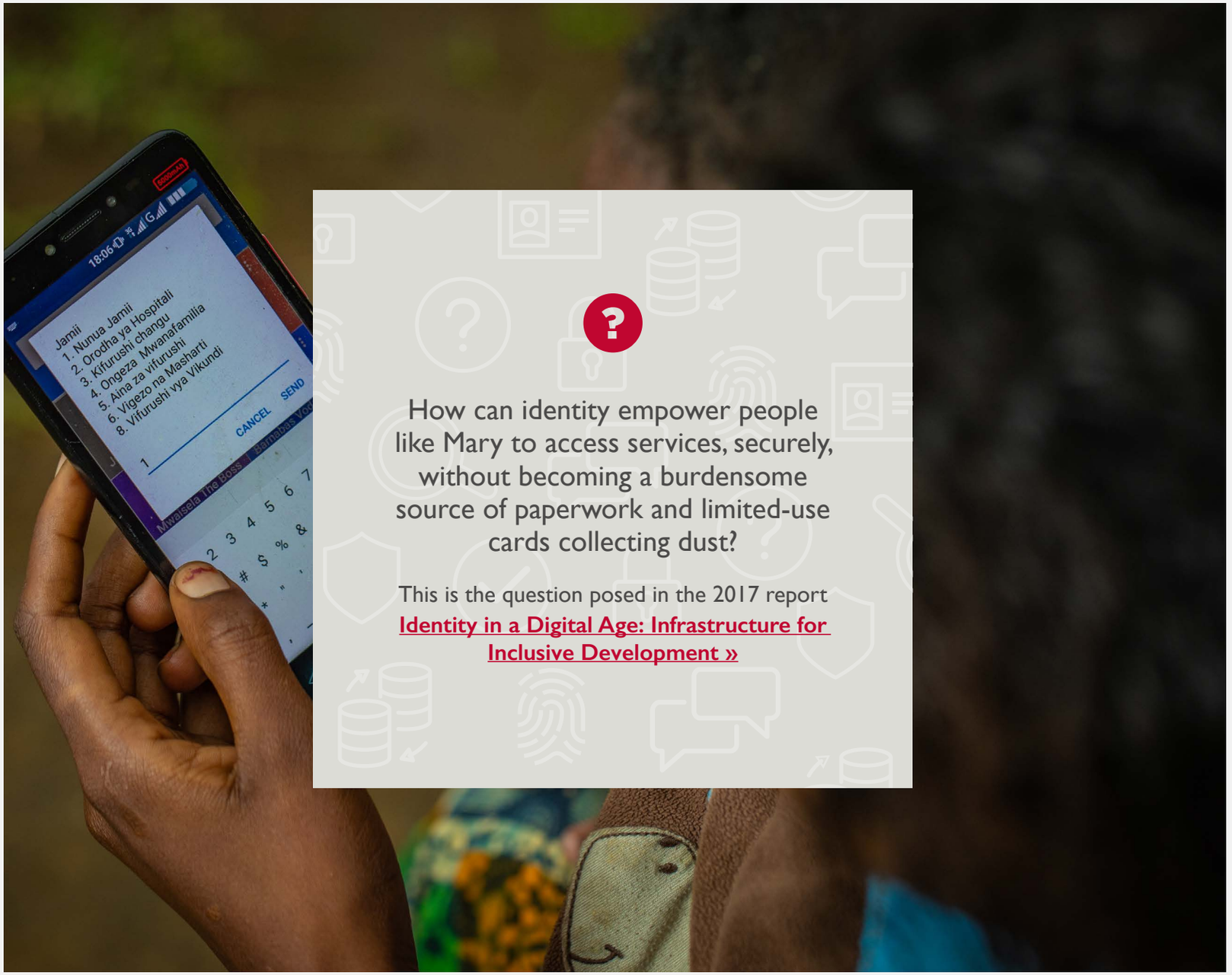
Mary is a primary school teacher in a rural village. She is passionate about teaching, but also has to take care of her three children and her own health, as she was diagnosed with HIV five years ago. Her life requires careful balancing of finances and time in order to ensure that she can teach, manage the small family farm, provide access to healthcare and education for her children, and save for a new house that will be more comfortable for her family.

In her current home, she keeps six different identity cards, all laminated and put in a box for safe keeping. Each identity card has a different purpose: one allows her to access her health care clinic, one identifies her as a member of her local agricultural cooperative, one allows her to vote in the national election, and so forth. However, she recently visited a local microfinance branch to open a savings account, and she was told that none of these six IDs were sufficient to open a bank account.

Recently, Mary encountered another ID-related challenge, when she had to take her child for an emergency visit to a health clinic in the city. Despite the fact that Mary has an ID card for her local health clinic, the urban clinic had no way to identify her or her child, or to access the child's records to see basic information on the child's medical history.

Each time she received one of the six IDs she owns, Mary felt temporarily empowered. Yet now, she is feeling that even with all of these ID cards, she cannot access the services that she most desperately needs.

When it comes to fragmented identity (as in Mary's six IDs), development programs are often part of the problem. Programs have to keep track of participants for monitoring and evaluation (M&E) purposes, and therefore often issue new, program-specific IDs to each participant. These are *functional* systems, which by definition serve only one purpose or program. Since they are single-use identities, they do not help Mary, in the long-term, to establish a multi-purpose identity that allows her to access the many services that she'll need over her lifetime.



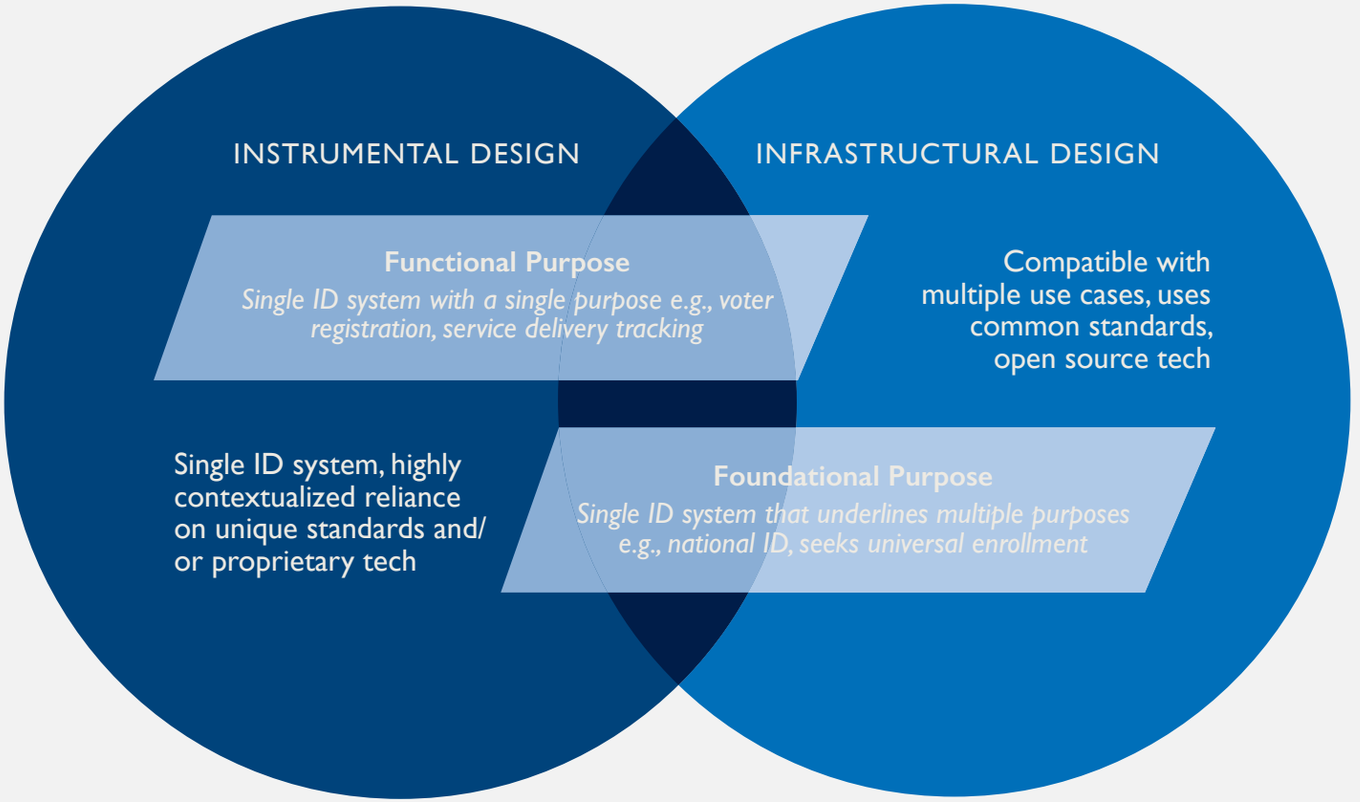
How can identity empower people like Mary to access services, securely, without becoming a burdensome source of paperwork and limited-use cards collecting dust?

This is the question posed in the 2017 report **Identity in a Digital Age: Infrastructure for Inclusive Development »**

Photo Credit: Riaz Jahanpour for USAID

The report describes two key shifts. First, creating more sustainable ID systems requires a shift from ***instrumental*** design that leads to isolated, single-application ID systems to ***infrastructural*** design of systems that can be repurposed for similar projects and are compatible with existing local systems. This first shift, which is the focus of this guide, will help support a second, longer-term shift from ***functional*** systems that serve only one purpose or program to more ***foundational*** systems that can serve as a public good and underlie multiple functional purposes.

IDENTITY IN A DIGITAL AGE FIGURE 1



These concepts may sound great on paper. Yet, when it comes to designing and implementing projects, USAID staff and partners have hundreds of competing priorities. The shifts described above are hard, and require behavior change among individuals, organizations, and the aid system as it has functioned in the past. This is no easy feat. On top of all that, the increasing use of digital technology for ID systems requires program designers and managers to have a grasp on complex concepts of technology, data protection, and privacy. Not only are these issues technically complex, they are dynamic, evolving every day as international companies, local governments, and global standards-setting bodies grapple with how to interpret these concepts in the face of today's rapidly changing technology and data landscape.

Despite these challenges, it is worth the effort for development programs to think about their role in building ID infrastructure. Why? As the World Bank and many other organizations have recognized[1], there may be no single factor that affects a person's ability to share in the gains of global development as much as having an official identity. Identity unlocks formal services as diverse as voting, financial account ownership, loan applications, business registration, land titling, social protection payments, and school enrollment. Robust identity systems can help protect against human trafficking or child marriage. In many ways, the roughly 1.1 billion people who lack official identity are discounted and left behind.

Digital tools and data-driven approaches are changing the face of development and humanitarian assistance by helping to improve health outcomes, lifting millions out of poverty, advancing democracy, empowering civil society, increasing transparency, and expanding the reach of education. Despite these gains, millions are excluded from the digital economy due to social, economic, education, and access gaps. USAID plays an active role in bridging this digital divide by working with Missions, governments, and the private sector to build an open, inclusive, secure, and reliable digital ecosystem that supports countries on their journey to self reliance. Incorporating a sound digital ID infrastructure is one critical way to empower citizens and communities in the developing world.

All development stakeholders (including you!) have a role to play in building the inclusive identity infrastructure that will deliver these long-term benefits. However, it's likely unclear what that role is, or what specific steps you can take if you're convinced that identity is important. Don't worry! This How-To Guide aims to help break down these issues into concrete steps, and to provide easy access to the many resources that are available on this subject.

As ID systems become increasingly reliant on digital, it is critical that they follow the ***Principles for Digital Development.*** This guide will emphasize strategies to follow these principles, especially:

- Design with the User
- Understand the Existing Ecosystem
- Reuse and Improve
- Address Privacy and Security

For more on each of the nine principles, visit **digitalprinciples.org**

Are you working on a project providing direct support to a government to build a national identity system, such as a voter ID system?

Read Samuel's story, which highlights some key ways in which a project can better gain Samuel's trust by thinking about how to design a voter ID system that Engages Multiple Partners in the Design Phase, takes care to Choose the Right Tech Vendor, and focuses on Data Protection. These steps can help to ensure that people like Samuel will take the time to register and vote by building his confidence in the system.

Read Samuel's Story »

Engage Multiple Partners in the Design Phase »

Choose the Right Tech Vendor »

Ensure Trust through Data Protection »

Are you working on a project providing advisory services to government partners on a sector-specific ID system, such as health or agriculture?

Read more about Mary's story, and to think about how to advise the Ministry of Education to help it achieve its goals while still ensuring that Mary gains an ID that serves multiple purposes and helps her to access the many services she may need in the long-run. By Engaging Multiple Partners in the Design Phase, Designing for Reuse and Interoperability, and thinking about Data Protection, the support to the Ministry of Education in this example helps to ensure that Mary is supported not only as a teacher, but also as a mother trying to manage her own health as she builds a better life for her children.

Read Mary's Story »

Engage Multiple Partners in the Design Phase »

Design for Reuse and Interoperability »

Ensure Trust through Data Protection »

Are you working on a project where you need to identify beneficiaries for the needs of one program or organization?

Perhaps you are an M&E specialist or a program manager looking for the best way to gather data on your program participants? Or you're a donor who is designing a new procurement? Read Joy's story, which demonstrates ways that you can help in Encouraging Infrastructural ID System Design in the Activity Design Process and further illustrates how taking steps to Engage Multiple Partners in the Design Phase, Ensure Trust through Data Protection, and Design for Reuse and Interoperability can benefit highly vulnerable households such as Joy's.

Read Joy's Story »

Encourage Infrastructural ID System Design in the Activity Design Process »

Engage Multiple Partners in the Design Phase »

Ensure Trust through Data Protection »

Design for Reuse and Interoperability »

Photo Credit: Athit Perawongmetha / World Bank

How can investments in ID systems support project beneficiaries?

Are you working on a project providing ***direct support*** to a government?

Are you working on a project providing ***advisory services*** to government partners?

Are you working on a project where you need to ***identify beneficiaries?***

Photo Credit: Guimba Souleymane, International Red Cross Niger

Samuel is an 18-year old mechanic with a primary school education who is trying to save up for a home for himself, his wife, and his two children. He's aware of an upcoming local election, but when asked, he says he is not planning to vote. He voted in the last election, but this year, he is told that he has to register for a new, biometric ID. Despite some of his frustrations with the current political situation, he doesn't think it is worth the time to register for a new ID. He registered for the last election and had to visit the government registration office three separate times, as he was told each time that he did not have all of the correct documents to register. On his final visit, he had to pay a fee to receive the ID, despite the fact that he thought it was free. He assumes that with a new, fancy biometric ID, the registration process will be even harder.

USAID has joined a multi-donor coalition committed to working with the government to help design and roll out the new biometric system and to increase participation in elections.

How can this investment be designed to support Samuel? Samuel needs to see value in the new ID in order to register: he needs to know that the process will be quick and easy, and that it will provide him with benefits. USAID decides to **Engage Multiple Partners in the Design Phase** and realizes that there is already a campaign planned by local civil society organizations to encourage youth to vote. Leveraging this type of campaign, which is already targeting people like Samuel, can make it much easier for him to register. It will also help the government to stay in budget—if they can use other networks to help with registration, then they will avoid the cost of setting up new registration booths for the sole purpose of this ID. The coalition decides that they will try to partner with this campaign, and perhaps a few similar networks, to train registration agents for the new ID.

During initial planning conversations for the new system, the government tells the multi-donor coalition that they intend to go with one specific tech vendor that demonstrated their new, proprietary biometrics technology for a few government officials at a conference last month. Understanding there are benefits to this specific system, the donors are still concerned, however, that this vendor has been selected without proper due diligence. Therefore, the donors walk the government through the process of **Choosing the Right Tech Vendor,** and find that the original tech vendor cannot provide any solid references for previous, large-scale implementations of their technology. Additionally, the system relies on a point-of-sale (POS) device for registration that is expensive and does not work with any other systems. Therefore, the coalition works together with the government to release a new RFP for a vendor who can provide references and demonstrate that their technology works in reality, not just in an office demonstration. The RFP also requests that the system can use a variety of different POS devices, including smartphones. Many registration agents already have smartphones, so this will mean that the government will not have to purchase a new device for every registration agent, which will drastically lower costs. It also means that it will be easier to ensure that this system can be used again during the next election without having to purchase much additional equipment.

When Samuel sees that he can register at a local booth through a smartphone application, he starts to gain confidence that registration is convenient and easy, and that the system is not overly complex so he'll likely be able to use this ID in the next election. However, he's still concerned about security: this election is supposed to be contentious, and he's worried that if he provides all of his data to this electronic system, another political party may be able to access it. He's read about data breaches from major international companies in the news recently: how is this any different?

The coalition discusses how they can **Ensure Trust through Data Protection** for Samuel and all other citizens. They have, for example, decided that all data will be encrypted, so that it cannot easily be viewed by any unauthorized party. The biometric information will be stored in a separate database from the demographic information, so Samuel's fingerprint scans cannot be matched easily to his personal information and voting preferences. These security measures, and other information on the collection and use of Samuel's data, are provided to him in a pamphlet with clear language and illustrations; demonstrated to him through a video in his local language that he views at the registration booth; and described to him face-to-face by the registration agent. These steps ensure that Samuel is confident that his data is secure, and he can confidently sign his name to provide his consent to use the data in the ways described to him.

What are other ways that this investment can provide value to Samuel?

What are other risks for Samuel that the government and the multi-donor coalition need to avoid?

Think about Samuel's situation (or one of your own project participants!) as you read through the five tools in this guide.

Photo Credit: Riaz Jahanpour for USAID

Let's visit Mary again. As you may recall from the introduction, Mary is a primary school teacher in a rural village. She is passionate about teaching, but also has to take care of her three children and her own health, as she was diagnosed with HIV five years ago. With little free time, she sometimes must take a whole day off of work to travel to the bank to get her pay.

A USAID partner in Mary's country has just been asked to support the Ministry of Education to develop a system for tracking teacher attendance.

How can this investment be designed to support Mary? This new system, as conceived, will provide clear value to the Ministry of Education. The Ministry is concerned about teacher absenteeism, and an electronic system will help the Ministry to measure the extent of this problem and to have better data to inform policy decisions. Yet, this does not provide clear value for Mary. In fact, she worries that this will only cause her more problems, since she sometimes has to miss work in order to go to the health care clinic for her HIV treatment.

What are some ways that Mary might see value in the system? Perhaps, Mary learns that the new system will also pay her automatically, on-time each month. She can pick up her salary at her local mobile money agent at her convenience rather than taking the day to travel to pick up her pay, providing her with an extra day that she can take off when she needs to visit the health clinic. She might see even more value if her monthly support from the Ministry of Social Welfare is delivered into the same account. She's read in the newspaper that the government may cancel the support program entirely due to the prevalence of "ghost worker" accounts set up by corrupt politicians so that they can benefit from the service; a robust identity service could root out ghost workers and save her benefits from cancellation. Fortunately, USAID discovers by **Engaging Multiple Partners in the Design Phase** that the Ministry of Social Welfare is planning a new ID system of their own, and now has agreed to cooperate with the Ministry of Education to connect the two initiatives. By working together, the two ministries hope to make it harder for any individual politician to push back against implementing a more transparent system. They are also developing a plan for meeting both

of their individual functional goals while using the same registration process and ID smartcard. In doing so, the two ministries are considering how to **Design for Reuse and Interoperability.**

Mary also worries about having her personal data all in one place. In her village, there is still a stigma against people with HIV, and she wants to ensure that this information remains private. What if, she asks, one day I use my new ID at the local health care clinic? Will others see that I am receiving treatment for HIV? She is told that she can trust the system: the system will use an ID card that stores all of her information in an encrypted, restricted-visibility manner. When she uses her ID card to show that she attended school, the school will only be able to see that the ID card corresponds to Mary. In other words, the school will only see one of two responses: Yes, this ID card belongs to Mary, or No, this ID card belongs to someone else. They will not be able to see or access any other information on Mary, such as her medical history. This is one way that the new system can be used for multiple functions and still **Ensure Trust through Data Protection.**

Photo Credit: Michael Dawson/FHI 360

Joy lives in a rural village which has experienced drought three separate times in the past ten years. She maintains a small farm, through which she grows food mainly for subsistence, but sometimes she has extra food to sell. She just found out that she is pregnant, and a friend informed her that she qualifies to receive support from the government through the national social protection plan. However, last year, when the lack of rain meant that she could not sell any produce from her farm, she traveled across the border to find work, and therefore was not in her village when registration for social protection took place. Even if she could register, Joy is a bit nervous to register in a national database as she is part of an ethnic minority who has been targeted by the government in the past. The USAID Mission in Joy's country is preparing to release a new RFP for a program aiming to both improve farm output and increase nutrition in two provinces in the country, including Joy's village.

How can this investment be designed to support Joy?

The Mission understands from previous consultations that many aid-funded activities in the country have created their own, separate ID systems, and they don't want the limited funds available for this activity to be used to create yet another system from scratch. Therefore, in the RFP, they put language encouraging the implementer to demonstrate that they have mapped the local ID ecosystem and determined whether they can use an existing ID system, join forces with other partners who are also looking to create a new system, or at minimum, design a new system in such a way that some or all components can be used by other partners in the future. By integrating this language into the RFP, the donor is **Encouraging Infrastructural ID System Design in the Activity Design Process.** This is great news for Joy: similar to Mary, she already has at least five IDs from other projects, and has provided her data (such as name, household size, and income level) more times than she can count over the years. She hopes that the next time she goes through the hassle of registering for an ID, it will help her to access a variety of services and remain useful for a longer period of time.

Once the implementer for this activity is selected, they begin by **Engaging Multiple Partners in the Design Phase,** conducting the ID system mapping through a Design Workshop in which many of the relevant partners participate. The ID component of their project is tricky: they need to gather a lot of data on each program participant for their own reporting; they need to find a way to lower the burden on Joy in terms of getting a new ID; and they need to maintain a positive relationship with the government while still respecting the concerns of minorities like Joy. In the Design Workshop, they find out that IDs have been used in the past as a way to identify and persecute ethnic minorities. They also learn that several of Joy's fellow farmers have trouble with fingerprint scanners due to labor-worn fingers. They choose to remove the "ethnicity" field from their data collection process and to offer both fingerprint registration and build in a fall-back identity verification process via photo, for those who are excluded from biometric registration due to their worn-down fingerprints.

During the Design Workshop, the implementer finds out that another large NGO in the country has already registered nearly all vulnerable people in the country. The new activity can use this same registration process. However, since the new activity will gather information on health and nutrition that may be considered sensitive, they will store the data on their own protected servers. They also decide only to share anonymized data with the government. This provides the government with some value from the system, helping to maintain a positive relationship, but it does not provide any personally identifiable information given local concerns about potential misuse of information by the government. When Joy learns this, she is relieved, as she has more confidence that the government will not receive additional information on her besides what is required for the social protection plan. This level of confidence is the result of the implementer taking the time to **Ensure Trust through Data Protection** and taking a nuanced approach to **Designing for Reuse and Interoperability.**

Photo Credit: Photo: Albert Gonzalez Farran

PART II

How-To Guides

Considerations when designing the identification component of any development project

How-To: Encourage Infrastructural ID System Design in the Activity Design Process

Photo Credit: Riaz Jahanpour for USAID

Donors can support the shift to infrastructural ID systems at many stages of the program cycle. For those activities that begin with a request for proposals (RFP), the procurement process can be a good place to start. Integrating language on sound investments in ID systems into an RFP can make partners aware of USAID's support for such long-term infrastructure investments, and encourage partners to budget the time and resources necessary to use ID systems that serve more than a one-time functional purpose, when possible. To do this, consider:

SAMPLE LANGUAGE FOR RFPS

During the activity design phase, language can be added that specifically encourages partners to consider the broader ID infrastructure in project design.

REVIEWING OVERALL RFP LANGUAGE

During the activity design phase, there are best practices that can help to encourage innovation and remove barriers to supporting the local ID ecosystem.

COST CONSIDERATIONS

There are costs associated with infrastructural ID approaches, which should be considered based on the specific country context.

SAMPLE LANGUAGE FOR RFPS

The following statement intends to provide an example of generic language that can be integrated into an RFP. Based on market research conducted during the activity design, this language can and should be modified as the context or activity demands. In contexts where USAID personnel already have a strong understanding of the ID ecosystem, they should consider making this language more specific.

USAID encourages partners to directly use, or to make efforts to interoperate with, existing identification systems, rather than issuing new IDs to beneficiaries, where possible and appropriate. When deemed necessary to create a new system for identification, USAID encourages partners to demonstrate how such a system can be built so that it can be leveraged and/or repurposed by other government ministries and/or development partners. The objective of these considerations is to ensure that USAID programming supports the expansion of digital identification infrastructure and foundational ID systems, which are more effective for long-term development than functional ID systems designed only for a single purpose.

This is an example of a key message of Identity in a Digital Age: where foundational, national ID systems are not yet available or adequate, donors can still discourage further fragmentation of the ID landscape, thereby helping to create pathways to a more sustainable identity infrastructure. However, it is just one example, where integrating with a local partner's existing system was determined to be the best strategy for that context and for the project objectives. For more on this, refer to the section on: **Ensuring Trust Through Data Protection »**

EXAMPLE

While developing a recent RFA for the Karamoja sub-region in Uganda, the Office of Food for Peace noticed that many people in the region did not have a national ID. However, WFP had recently undertaken a comprehensive registration push for its beneficiary identification and management system, SCOPE. Therefore, the RFA included the following language:

SCOPE is a web-based application used for participant registrations, intervention setups, distribution planning, transfers, and distribution reporting. Ultimately, it is envisioned that SCOPE will be used across development actors in Karamoja. If SCOPE is successfully implemented by the time of the award(s) being awarded, or during the lifetime of the award, it is anticipated that awardees will work within the WFP SCOPE system.

In response, a Food for Peace partner, Mercy Corps included this language in a subsequent Scope of Work for a consultant to support the Resource Transfer component of its Apolou development food security activity.

Liaise with WFP and M&E team to ensure interoperability of beneficiary database with general Apolou CommCare database and WFP SCOPE single registry.

REVIEWING OVERALL RFP LANGUAGE

Recent feedback from industry partners suggests that there are good ways to promote innovation and digital infrastructure through alternative RFP language. These best practices can be considered when drafting an RFP that intends to promote innovation generally, or to allow partners the flexibility to design the ID component of the activity in a way that best supports the broader ID infrastructure in a given context. Some points to consider include:

- **RFPs with more detailed scopes of work** tend to restrict innovation. In the context of ID, RFPs that are prescriptive about the ways to identify beneficiaries may restrict partners' ability to collaborate, integrate with, or use local ID systems. More generally, RFPs that ask for a specific set of results, instead of activities written up as results, leave it much more open to offerors to innovate in general, and specifically with ways to ID their beneficiaries.

- **What gets measured gets managed;** thus, you may choose to allocate points in your proposal evaluation plan to taking an *infrastructural approach* to ID. If you choose to do so, it is important to define exactly what is meant by an infrastructural approach to ID in terms of results in the context of your specific activity (for example, designing a system for reuse, or interoperating an existing ID system). Leave it to offerors to propose a path to get there.

- **Guidance to Technical Evaluation Committee** is as important as changing the RFP language. *For example:* Recognize that taking an infrastructural approach to ID may be slower, as it requires more collaboration and partnership that takes time in terms of negotiations and implementation. This should be accounted for, and allowed for, in estimated project timelines. It may also mean a certain level of risk (for example, that a partnership falls through); therefore, it is important to recognize that failure can be a good thing if it contributes to learning and adaptation that ultimately moves the project closer to achieving its objectives. Support for digital infrastructure on a project comes not from the proposal alone, but from a willingness to take certain risks on the part of the offeror, and the willingness of the client to accept those risks.

- **Allow implementers more flexibility in designing programs/budgets.** *For example:* allow offerors to propose the proportion of the budget allocated for grants/ local subcontracts, and permit bidders to select positions of key personnel (and define the qualifications). More flexible job requirements/descriptions for personnel, including COPs, encourages more diverse and integrated staffing, and allows for hiring of unique and relatively new skill sets relevant to digital ID and designing for reuse and interoperability of ID systems.

COST CONSIDERATIONS

As with any change, a shift towards infrastructural ID will likely incur costs. Donors and partners will have to work together in order to properly assess these costs, and weigh them with the benefits to the overall digital ID infrastructure of a country and impact on intended beneficiaries. The ID4D team at the World Bank has completed a thorough assessment of **Public Sector Saving and Revenue** that will be highly useful in thinking about cost, especially for those projects which are providing advisory services or direct support to a government or ministry. The following table provides an overview of that paper as it relates to this Guide. While every project, country, and context will be different, the table lists some possible costs, and on the other hand, possible sources of savings and offsets to consider.[2]

Both costs and savings will be influenced in any given context by presence of an existing ID system from which a project or partner can benefit. Additionally, it will depend on the existing coverage and robustness of this system. There are four key contextual factors that influence the assessment of the costs and savings in the previous table[3]:

1. **Digitization:** to what extent have databases, credentials, data transfer, etc. been digitized?
2. **Unique ID:** to what extent has a foundational system issued a unique ID to all residents, which can help with authentication for other functional purposes?
3. **Integration and Interoperability:** to what extent do existing foundational and functional systems allow for integration, and how easy, secure, and cost-effective is such integration?
4. **Digital Authentication:** to what extent is there already a network of trained agents with authentication devices that can be used for authenticating identities?

POSSIBLE COSTS TO CONSIDER

Time dedicated to involving multiple partners in the design process (such as convening costs)

System procurement and maintenance OR cost of integration with an existing system

Time for proper user testing per Choose the Right Tech Vendor

Authentication devices (e.g., biometric scanners)

Registration drives (it will likely be necessary in each case to register participants into a specific program, but administrative costs may be lower if they are already registered in a foundational system)

User training and education (both end users and those responsible for registration and authentication)

POSSIBLE SOURCES OF SAVINGS & OFFSETS TO CONSIDER

Use of an existing system (already established by government or donor partner), which will become more common over time as more partners design for reuse and interoperability

Reduction of fraud in payments by reducing "ghosts," duplicates, ineligible beneficiaries, and impersonation

Increased tax collection or collection of fees (depending on the projects or line ministries involved)

Reduction of administrative cost, including elimination of investment in redundant systems and redundant data collection

Time saved on behalf of beneficiaries if redundant registration processes are avoided

How-To: Engage Multiple Partners in the Design Process

Photo Credit: Riaz Jahanpour for USAID

Engaging multiple partners in the design process when building a new ID scheme is critical to ensuring that individual programmatic investments in ID systems work together to form a sustainable, inclusive infrastructure for development.

How can a program effectively engage partners in this process? The following section outlines two actions for doing so:

ACTION I: ASK

Who is working on ID systems in your context?

ACTION II: CONVENE

Bring key partners together to create an ID systems map

ACTION 1

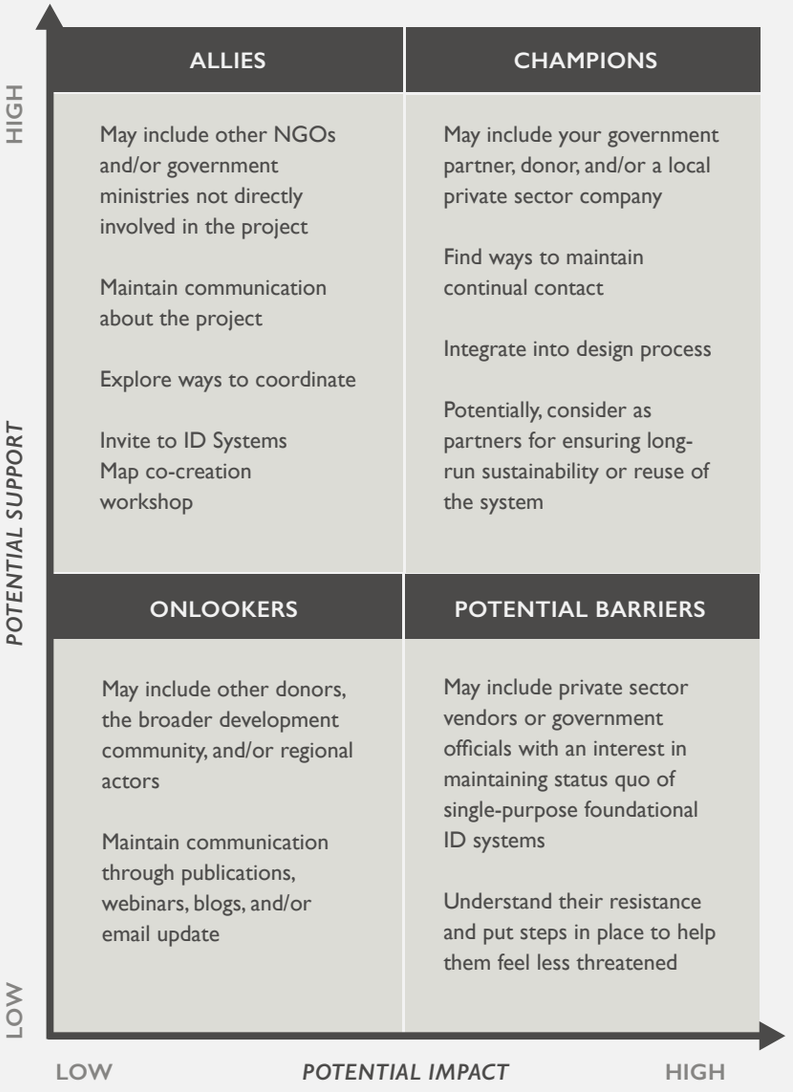
ASK: WHO IS WORKING ON ID SYSTEMS IN YOUR CONTEXT?

> "Frequently, donor ID investments miss opportunities to build on prior work."
>
> —INTERVIEW WITH USAID FOREIGN SERVICE OFFICER

During the initial stages of your project, it is important to understand who else is working on ID systems - both foundational and functional, and both technological and paper-based - in your country or context. Desk research and key informant interviews can be used to identify these existing and/or in-progress ID-related activities. For example, if you are building a beneficiary management system for health, it is necessary to know if and how the Ministry of Health is identifying individuals already. It is also necessary to know if the Ministry of Social Welfare, for example, is planning a new national (foundational) ID system. Likely, there are one or more donors or implementing partners who are already identifying the same beneficiaries. Listing these stakeholders and understanding where and how they are investing in identification is critical to the next step: creating an ID systems map.

A great place to start is Identification for Development (ID4D), part of the World Bank Group. ID4D brings global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems. Their website has extensive research on ID systems, including a **Global Data Set** and **country diagnostics** for 17 countries across the developing world. They are actively working to advance foundational ID systems in many of these countries, and therefore can be a key resource for understanding a given context.

One way to document stakeholders as you conduct your research is to categorize each stakeholder as an Ally, Champion, Onlooker, or Potential Barrier. [4]



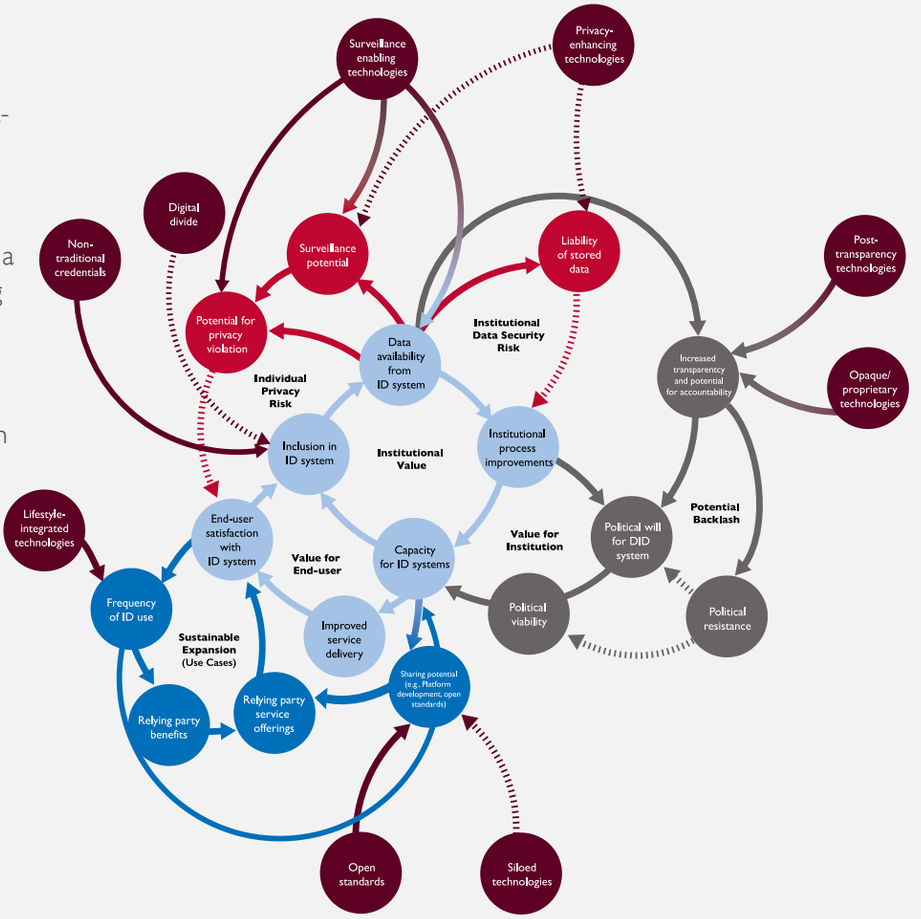
ACTION 11 CONVENE: BRING KEY PARTNERS TOGETHER TO CREATE AN ID SYSTEMS MAP

Identity in a Digital Age illustrates the complexity of an ID system through this map, which provides a useful illustration of a general ID systems map.

However, in order for a systems map to be useful for decision making, it needs to be adapted for each specific context. Creating this context-specific systems map is a great way to convene partners and ensure that everyone has a chance to actively engage in the design process. The following section outlines a ***6-Step*** process[5] for such a convening. It is envisioned that the bulk of step 1 through 4 can be completed in a 1-day convening, while steps 5 and 6 will be conducted on an ongoing basis through the remainder of the design process.

The goal is to understand key influences and risks that will help you gain insight into how you can maximize positive impacts on the system (by helping to shift toward an infrastructural, foundational system compatible with multiple use cases, common standards, and open source tech design) and mitigate any negative impacts that you may have on the overall system (increasing fragmentation, privacy risks, or political backlash).

IDENTITY IN A DIGITAL AGE FIGURE 24



ACTION 11 CONVENE: BRING KEY PARTNERS TOGETHER TO CREATE AN ID SYSTEMS MAP

Co-Creation Workshop: 6 Steps for ID Systems Mapping
Each of these 6 steps will be outlined in more detail.

1. FRAME THE QUESTION

2. EXPLORE THEMES

3. BUILD YOUR MAP

4. HIGHLIGHT KEY INFLUENCES & RISKS

5. CRAFT A NARRATIVE

6. SOCIALIZE & ADAPT

ACTION 11

1. FRAME THE QUESTION

It is important that all participants agree upon a framing question, which will help to ensure that everyone agrees on the ultimate outcome of the workshop. This question can be revisited whenever the discussion seems to be getting off track to ensure that the conversation remains relevant.

A general framing question might be:

> ***How can we best meet our project requirements while positively supporting the development of inclusive ID infrastructure in this country?***

or, if you are able to use a story of a real project participant similar to those of Mary, Joy, and Samuel above, you can describe the individual briefly and ask:

> ***How can we best design [the ID component] of this investment to deliver value for this person?***

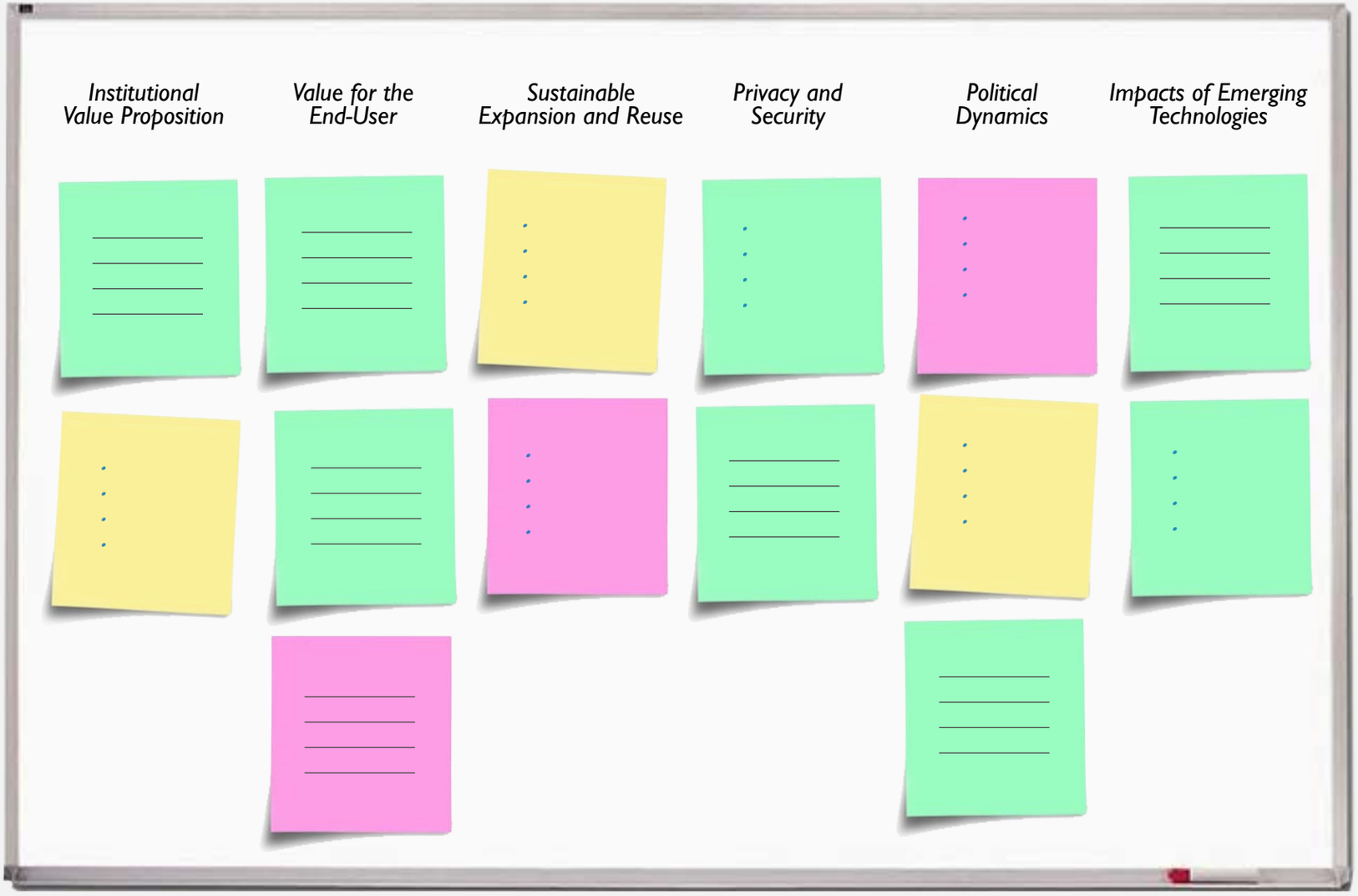
However, drawing on Step 1: Who is Working on ID systems?, you can likely make the framing question more specific. For example:

> ***Knowing that the World Bank is supporting the government to develop a foundational ID system that will be implemented in the next 5 to 10 years, how can we make sure that the ID system we use now for our agricultural development project supports or ties into this effort?***

ACTION 11

2. EXPLORE THEMES

Identity in a Digital Age outlines six key thematic areas that create a digital identity system. The second step in creating your own system map is to have all workshop participants brainstorm the *key factors* at play within each of these thematic areas. Have each participant write key factors for each of the 6 themes. Factors should be in note form, with one per post-it note. After participants have completed brainstorming factors, ask them to place each factor under the correct category.



ACTION 11

2. EXPLORE THEMES

Below is a sample table using the six thematic areas outlined in the original report, as well as suggested questions within each area to explore as participants brainstorm. The chart below is meant to be purely illustrative and to help you get started in making a map that is relevant to your project. The thematic areas may need to be adapted to be relevant to your context, and you may choose to add other thematic areas that are more important to your project.

THEMATIC AREA	GUIDING QUESTIONS	EXAMPLES OF KEY FACTORS
1 **Institutional Value Proposition**	• Which institutions will derive value from the ID system? • What are all the intended and unintended benefits that the ID system may have for these institutions? • Which of these benefits are *functional* goals that support project goals? Alternatively, which benefits are *instrumental* in that they are derived from the ID system itself, and therefore are not sector-specific?	*NGO—Health Outcomes—Functional* *NGO—Increased Capacity for ID Systems —Instrumental*
2 **Value for the End-User**	• What are the potential intended and unintended benefits of the ID system on the end-user? • Which of these benefits are functional and might end with completion of the project, and which are infrastructural and may be more long-term?	*Inclusion in program—functional* *Inclusion in foundational ID system—instrumental* *Increased comfort with technology and concept of data protection—instrumental*

Continued on page 29-30

ACTION 11

2. EXPLORE THEMES

THEMATIC AREA	GUIDING QUESTIONS	EXAMPLES OF KEY FACTORS
3 **Sustainable Expansion and Reuse**	• What other institutions may want to use the ID system that you are creating? • Which components might they want to use? For example, the registration process, the ID number or ID card, or the technology platform behind the ID system? • Where else might individuals use the new ID to derive additional value? For example, banks, insurance companies, etc.	*Ministry of Social Welfare—needs a way to register beneficiaries more quickly* *NGO partners—other NGOs are also registering farmers in different geographic areas and may want to use the same ID card* *Banks—might pay for ID data to have more information on potential clients*
4 **Privacy and Security**	• What are potential *individual privacy* risks that end-users may face as a result of being part of this ID system? • Are there ways in which this ID system can increase security for individuals? • What are the *institutional data security risks* that may arise from collecting this data?	*Individual—risk - theft of personal data* *Individual—benefit - more control of personal data now that they have an ID card* *Institutional—will be held liable in case of a data breach* *Institutional—can't achieve program goals if individuals don't register because they don't trust the system*
5 **Political Dynamics**	• In what ways is political support necessary to sustain this ID system? • Where is political support most likely to come from? • What are the risks of political backlash? • Where is political backlash most likely to come from?	*Ministry of Agriculture support—critical as they are intended long-term owners of the system* *Ministry of Social Welfare—potential backlash if this is seen as interference with the ID system that launched 5 years ago*

ACTION 11

2. EXPLORE THEMES

THEMATIC AREA	GUIDING QUESTIONS	EXAMPLES OF KEY FACTORS
6 **Impacts of Emerging Technologies**	Focusing on technology that the system will use for data storage, registration and ongoing authentication: • What are the cultural norms around technology use? • Which segments of our target population are most likely to be excluded from the system if we use this technology (e.g., Digital Divide)? • How will this technology impact the frequency of ID use? • Does this technology support sharing and future platform development?	*Fingerprint biometrics—already used and trusted - but, some beneficiaries are manual laborers and may have worn-down prints* *ID card—increase security but people might lose it* *IT Platform—have to pay expensive licensing fees, not sure who will/can pay once funding is over*
7 **New thematic area**	_____ _____ _____ _____ _____	

Once all of the post-its are collected, allow the participants to take a break while the facilitator organizes the post-its and groups them according to similar themes. Ask for clarity on those that don't seem to fit or aren't legible.

ACTION 11

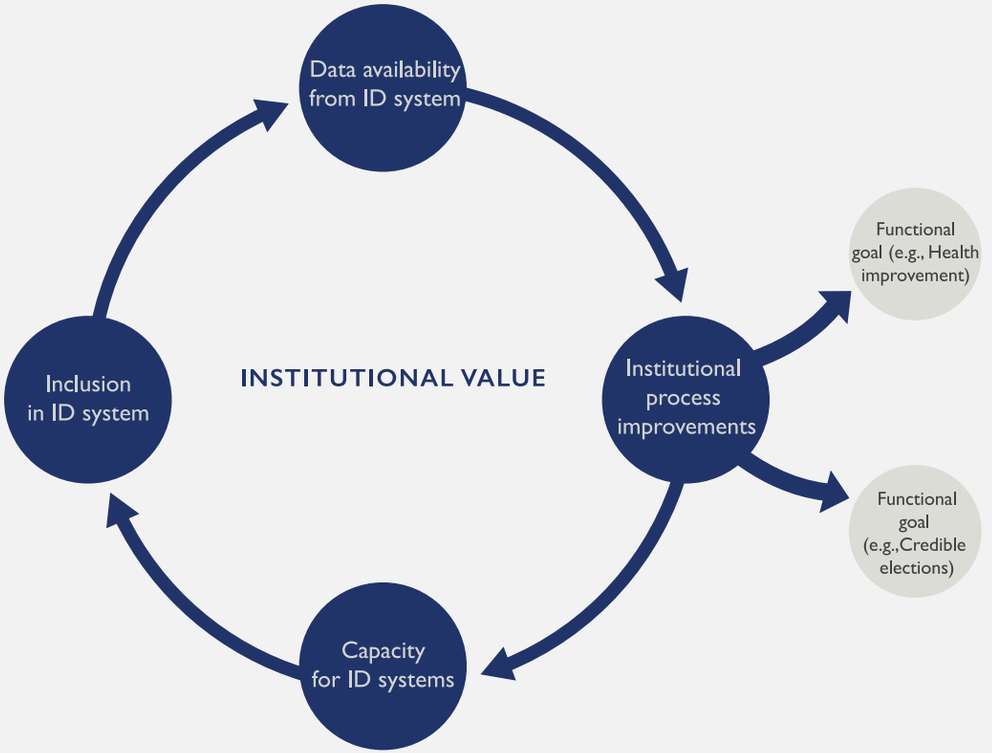
3. BUILD YOUR MAP

Now that you have a wide variety of factors that will influence each thematic area, it's time to build your map by creating interconnected feedback loops. Systems maps are, by definition, complex, so it helps to take this one step at a time. The aim is to create a systems map, such as the one below from *Identity in a Digital Age*, that is contextualized for the digital ID system that you are operating.

To facilitate this, ideally, make use of a large whiteboard where the facilitator has already been able to draw the basic structure of the diagram.

Each theme is a different color, each factor is a circle, and arrows between the circles indicate *influences* rather than a direct cause-effect relationship.[6]

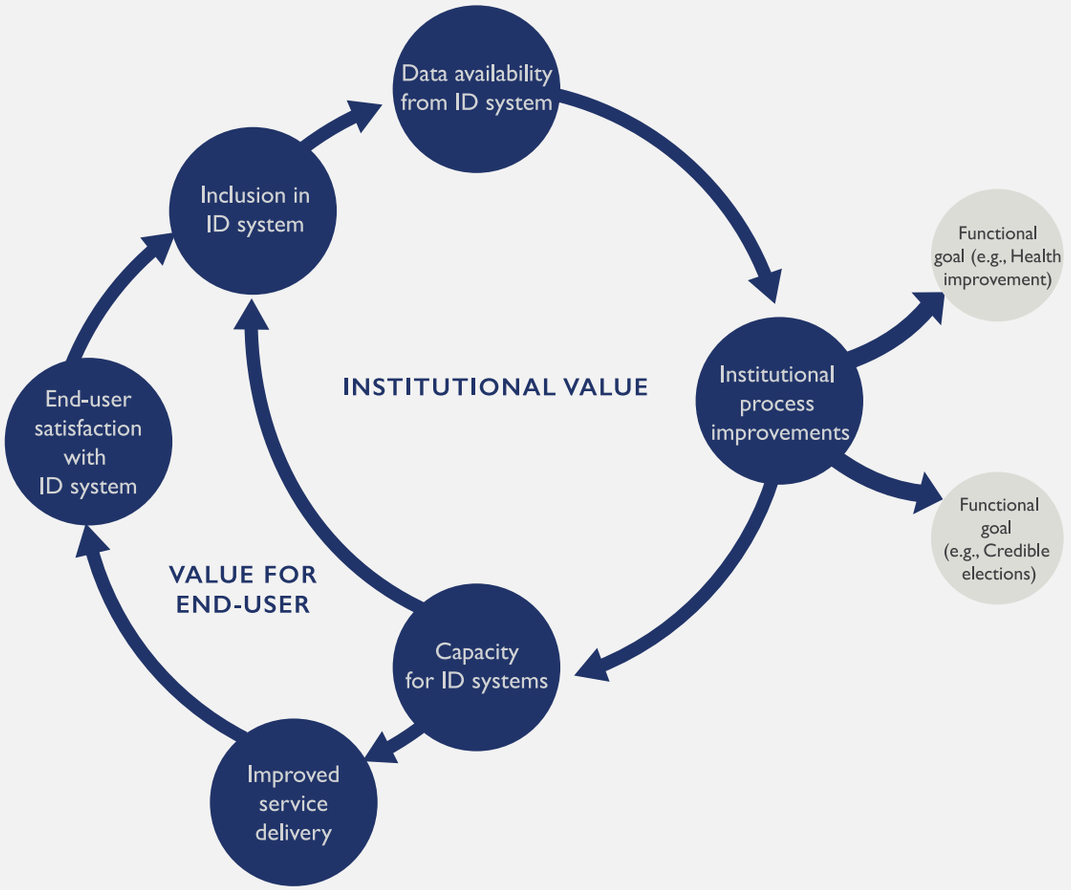
Start with Theme 1: Institutional Value Proposition. How do these individual factors influence each other? How are the instrumental factors reinforcing each other and the overall system? List the *functional* benefits as well, but visualize that they are outside of the broader system.



ACTION 11

3. BUILD YOUR MAP

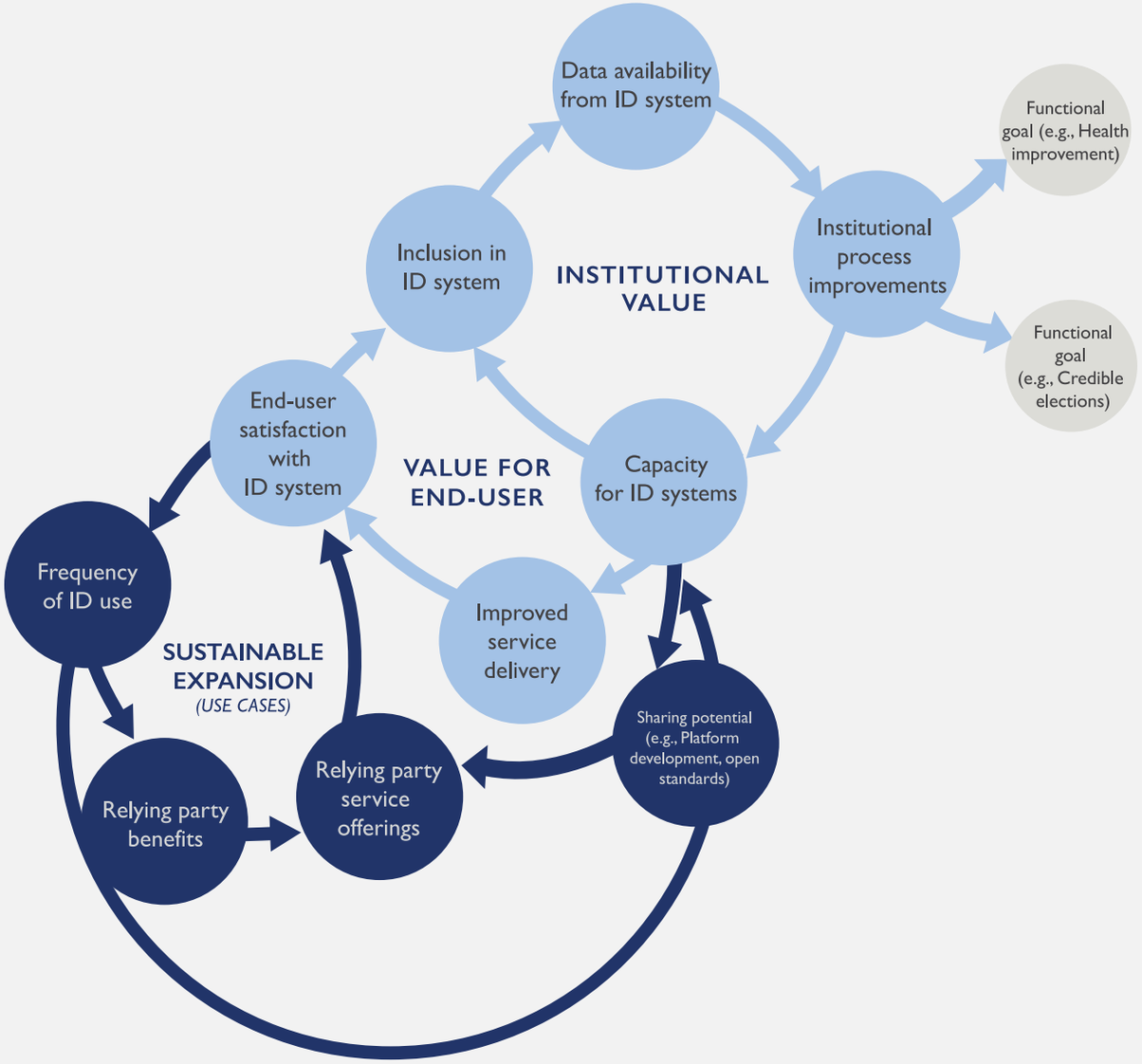
Then, connect the factors listed in the post-its under Theme 2: Value for the End-User.



ACTION 11

3. BUILD YOUR MAP

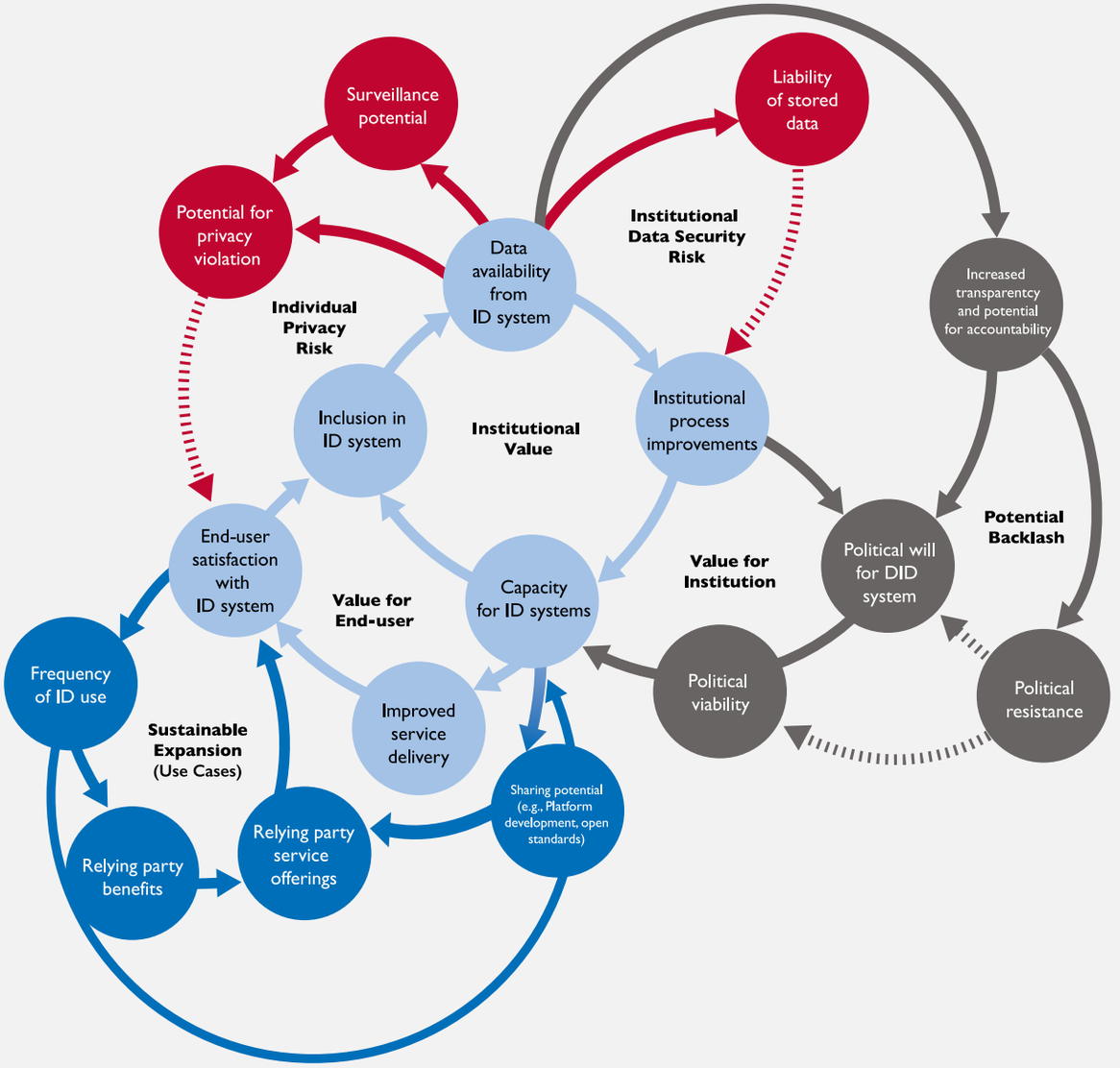
Next, connect the factors listed in the post-its under Theme 3: Sustainable Expansion.



ACTION 11

3. BUILD YOUR MAP

Next, connect the factors listed in the post-its under Themes 4 and 5, Privacy/Security and Political Dynamics.

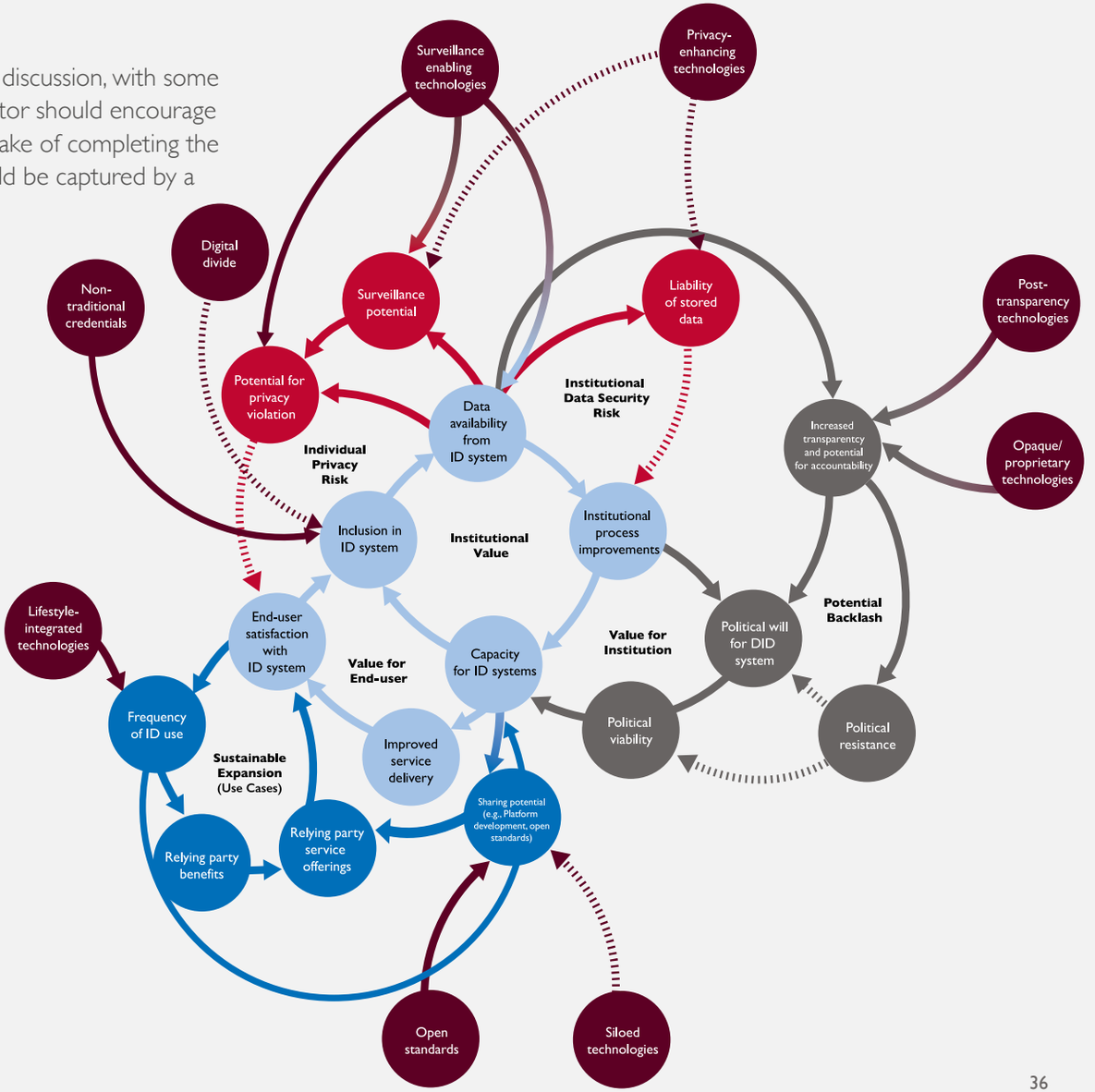


ACTION 11

3. BUILD YOUR MAP

Finally, connect the factors listed under Theme 6, connecting each factor to the circles that the factor is likely to have the most influence on.

Creating this map should result in dynamic discussion, with some debate and disagreement. While the facilitator should encourage resolution of these disagreements for the sake of completing the map, the nature of the disagreements should be captured by a notetaker for future reference.



ACTION 11

4. HIGHLIGHT KEY INFLUENCES AND RISKS

Now that you have your map visualized, ask participants to reflect on the influences and connections that they see. Which influences are the strongest? What are the most likely risks? Visualizing key influences and risks will help to prioritize the most likely factors that project designers will need to focus on - without isolating them so that their influence is no longer viewed as connected to the larger system.

This can be an open discussion, or the facilitator can provide stickers to each participant. For example, if the stickers are green and red, participants can place green stickers on each arrow that they see a key influence, and a red sticker on each factor that they see as a key risk.

ACTION 11

5. CRAFT A NARRATIVE

The map that you've created tells a story. But...this story is not clear at all to anyone that was not part of the process and therefore can't follow all of the arrows and circles and colors. The next step is to develop a narrative from your map. This will let you socialize the ideas behind the map with partners in order to get feedback and to iterate on the map accordingly. It will also set you up for designing a digital ID system that meets both your program's functional needs and the infrastructural needs of the broader digital ID ecosystem.

This step may take place within the workshop, or you may choose to do this on your own once you've had time to synthesize and process the information. You can then send the narrative back to workshop participants for input.

To craft a narrative, start by revisiting your framing question.

EXAMPLE

Knowing that the World Bank is supporting the Government to develop a foundational ID system that will be implemented in the next 5 to 10 years, how can we make sure that the ID system we use now for our agricultural development project supports this effort?

Then, provide background on how you generated the information contained in the map.

EXAMPLE

We started by Asking Who is Working on ID in this country, and gained a strong understanding of the local and international actors involved by conducting desk research, interviewing key informants, and spending time with the government ministry that we are partnering with on this project. We used this research to generate a list of the most relevant stakeholders, who were invited to a 1-day interactive workshop.

Finally, pull out highlights from the systems map, discussing each of the 6 themes as well as the key influences and risks.

EXAMPLE

By mapping out the key factors in this system, we realized that, although our main partner is the Ministry of Agriculture, we also have to get buy-in from the Ministry of Social Welfare, as they are a key part of the longer-term foundational ID system plan. In addition, it became clear as we mapped key risks that biometric technologies, especially fingerprint scans, are not trusted here because of a previous data breach, and therefore if we continue with this approach then we risk isolating some of our intended participants.

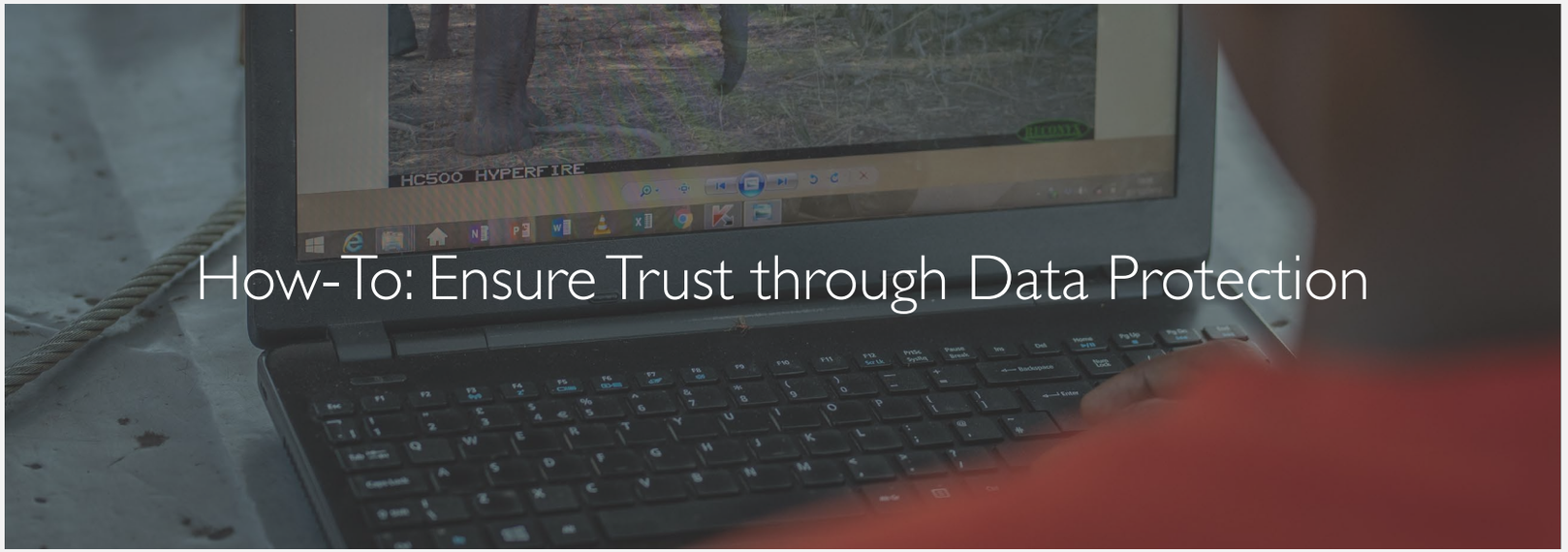
ACTION 11

6. SOCIALIZE & ADAPT

A 1-day workshop is not intended to create a perfect map that captures all of the complexity of an ID ecosystem. Therefore, it should be considered a starting point which you can use to:

- Identify gaps that require additional interviews or user research
- Solicit and capture new information from additional stakeholders
- Identify key leverage points: in other words, identify places within the existing ID ecosystem where an intervention could have more or less impact, and/or identify how your intervention might affect the dynamics of the current ID ecosystem
- Monitor your project during implementation - regularly revisit the map, especially the key risks, to see if you are still on track in terms of supporting the overall ID system, rather than only meeting project needs
- Use the results of this exercise as you move onto **Ensure Trust through Data Protection, Choose the Right Tech Vendor,** and **Design for Reuse and Interoperability.**

Photo Credit: © Dominic Chavez/World Bank



How-To: Ensure Trust through Data Protection

Photo Credit: Riaz Jahanpour for USAID

Digital IDs are a source of digital data. As such, they present similar tensions as other sources of digital data. On one hand, the data collected is valuable and can be shared with development agencies, government ministries, and private sector companies to provide much-needed services to individuals and households. On the other hand, data in the wrong hands can be dangerous, especially for highly vulnerable populations. Special considerations need to be taken when working with digital ID systems, especially if there is any data sharing for any reason. Preventing the inappropriate use of data you've collected -- whether by data-sharing partners, data thieves, or your own staff—is all part of ***data protection.***

USAID's **Considerations for Using Data Responsibly at USAID** provides an overview of responsible data use. That document, as well as a number of other dedicated USAID policy documents, address data protection within USAID activities. This section provides a much shorter, non-prescriptive snapshot of data protection definitions and issues specifically related to digital ID. For more information, refer to Considerations for Using Data Responsibly at USAID (which includes links to USAID policies and references on data privacy and security) as well as resources from other organizations referenced at the end of this section.

This section intends to help you think through how to design for reuse and interoperability with the broader ID ecosystem, and to deliver value to individuals through data sharing, while still following best practices in terms of data protection in order to minimize potential risk.

There are some basic concepts of data protection that are helpful for considering whether, and how, to share data from your digital ID or beneficiary management system. The following are some basic definitions relevant to data protection in the context of digital ID. In addition to Considerations for Using Data Responsibly at USAID, you can find more detailed explanations of these concepts in the **Handbook on Data Protection,** written in partnership between the International Committee of the Red Cross (ICRC) and the Brussels Privacy Hub. The Handbook provides much more extensive definitions and examples, and is a great resource for those who would like to learn more.

1. Data Protection Law is a challenging concept since it varies between countries and regions. For example, the United States has very different data protection laws than those laid out under the Asia Pacific Economic Framework, which are different still from Europe, which recently adopted the General Data Protection Regulation (GDPR). On the other hand, some developing countries may have little to no data protection regulations. USAID implementing partners should be aware of these differences, especially if they are working in multiple countries, and be sure to follow USAID guidance, local regulation, and best practices to ensure the most appropriate level of protection for any given context.

2. Privacy by Design is a concept that emphasizes the need to ensure that privacy and data protection are not afterthoughts, but rather built into an organization or program's processes and procedures. Examples of ways to ensure that an organization or program is designed for data protection include:

- conduct an Information Audit to understand what data you already have on any customer, client, or partner organization and whether they consented to share it;[7]
- check 3rd-party data (e.g. data that existed before a project's start date) for personally identifiable information (PII), sensitive information, and indirect identifiers;
- establish a Data Management Plan if your organization does not already have one;
- consider how to generalize individual, group, and location-related data so that it cannot be used to identify vulnerable populations;
- conduct staff training to disseminate these policies and procedures.

3. Lean Data[8] approach to data collection and processing may help when it comes to data protection. Lean Data is a broad concept that encourages organizations to shift away from the use of complex, costly data collection methods and toward the use of simple, inexpensive tools. Some Lean Data concepts relevant to data protection and digital ID include proportionality, purpose limitation, data minimization and informed consent.[9] These may be relevant points of consideration when thinking through data protection issues around digital ID.

Informed consent[10] is another important concept - and one that may be more complex than it sounds. The table further explores the tension highlighted at the beginning of this section: data sharing can be good, in that it allows individuals to receive goods and services based on their confirmed identity. However, it can also be dangerous if a particularly vulnerable population ends up with their data shared or accessed by the wrong groups. As the ICRC *Handbook on Data Protection* points out, "it is necessary to consider the sensitivity of data and the appropriate safeguards to protect Sensitive Data on a case-by-case basis."[11] Since USAID and our implementing partners often work with vulnerable populations, the chart below provides a framework by which to think about the level of data protection that may be appropriate for any given population, based on the characteristics of that population.[12]

Important note: ID systems include:

1. **Registration:** The processes and technology by which individuals are registered and issued an ID;
2. **Use:** The processes and technology by which individuals actually use that ID;
3. **Storage:** The servers and databases that store the data, and;
4. **Data:** The actual information collected on individuals registered in the system.

The first 3 components can be shared and reused, even if the actual data is not shared for privacy reasons. This section focuses specifically on data sharing, rather than the reuse and sharing of other components of the system (covered **here**).

Photo Credit: Riaz Jahanpour for USAID

This table is illustrative, and not prescriptive, and is only meant to guide thinking during the design of the program. It is also specifically tailored to ID systems which are more likely to contain personally identifiable information (PII), which tends to be more sensitive than other types of data. Therefore, this table does not address the sharing of all types of data generated by a development project. For more information on this, refer to *Considerations for Using Data Responsibly at USAID.*

Table # 1: Design Considerations for Context-Appropriate Data Protection

	HIGHER RISK	MEDIUM RISK	LOWER RISK
Population Characteristics *(illustrative and non-exhaustive)*	Systemic discrimination; and/or high prevalence of mental illness; and/or trauma; and/or little education or ability to understand risks and benefits	Vulnerable; and/or at-risk; and/or some education and literacy	Some education and literacy; and/or ability to take advantage of economic opportunities provided via data sharing; and/or ability to take advantage of recourse mechanisms
Examples *of populations that may have these characteristics*	Displaced persons, especially those not settled in a relatively stable location; persecuted religious and ethnic minorities; victims of gender-based violence (GBV); children	Women; persons with disabilities; LGBTI persons; sex workers; resettled refugees or those in a long-term location	Smallholder farmers; entrepreneurs; university students
Likely ability to give ***Informed Consent*** *based on characteristics*	Limited ability to give informed consent	Some ability to give informed consent	Ability to give informed consent
Design Considerations	Higher levels of security in terms of limiting system access and ability for staff to download data Limit data sharing with external partners Minimize amount of data collected (ask: what is necessary to know versus what is nice to know?) Tightened data storage protocols and security	Avoid overlaying ID details with specific demographic details Consider proportionate data sharing with external partners, with documented assurances that data will not be shared further Consider budgeting more time and creating education materials to gain informed consent	Consider proportionate data sharing with external partners, with documented understanding of how data may be shared further Budget appropriate time and education to gain informed consent Consider how your ID systems can interoperate with foundational and/or other development ID systems to support the overall ID infrastructure and improve customer experience

How-To: Choose the Right Tech Vendor

Photo Credit: Riaz Jahanpour for USAID

Choosing the right tech vendor is a critical piece of any digital ID implementation. In the context of USAID-funded activities, a project that needs to ***identify beneficiaries*** may choose to procure a beneficiary management system (BMS) that both identifies and collects additional data on participants for M&E purposes. A project that provides ***direct support*** or ***advisory services*** to a government ministry may instead be looking for a system focused only on identity and authentication. Regardless, there are similar considerations for choosing the right tech vendor—and by implication, the right technology.

There are many risks to avoid when choosing a tech vendor. The following section details five key tips for avoiding many of the common risks reported by USAID implementing and government partners when selecting an identity system.

TIP 1
Don't let the solution define the problem

TIP 2
Avoid vendor lock-in

TIP 3
Understand and document all costs

TIP 4
Insist on references and testing

TIP 5
Seek expert, impartial advice when needed

TIP 1: DON'T LET THE SOLUTION DEFINE THE PROBLEM

> "Given one hour to save the world, I would spend 55 minutes defining the problem and 5 minutes finding the solution."
>
> —ALBERT EINSTEIN

Tech vendors, by definition, will have stock solutions that they provide. These may or may not be the appropriate solution for your problem. Ensuring that you've properly **Engaged Multiple Partners in the Design Phase** is one critical step. Understanding your own project needs, or problems that you are trying to solve, is the next step. It is critical to do so before drafting an RFP or engaging with a tech vendor, to ensure that the vendor does not have an opportunity to let their solution define your problem.

The original report **Identity in a Digital Age** provides a thorough analysis of different technologies [biometrics, mobile ID, algorithmic ID, blockchain-backed ID, and user-controlled ID] and which problems they may solve, which problems they will likely not solve, and which problems they will likely create. This is a great place to start.

The following table can serve as a 'worksheet' for thinking through your problems, potential technology solutions, risks of these solutions, and risk mitigation strategies. Completing such a worksheet for your own project will help to draft an RFP for procuring the appropriate technology solution for your project needs. As you complete the worksheet, remain open to the fact that many problems may not be solved by technology at all. These problems should still be documented and used when developing trainings, policies, and procedures for the identity system.

Photo Credit: Riaz Jahanpour for USAID

Sample Worksheet: Finding the Right Solution for the Right Problem

PROBLEM *(non-exhaustive examples)*	**TECHNOLOGY CONSIDERATIONS** *(non-exhaustive examples)*	**RISKS** *(non-exhaustive examples)*	**RISK MITIGATION** *(non-exhaustive examples)*
Database needs to be updated continuously (to account for deaths, births, and/or changes to individual qualifications for certain program benefits)	No one technology can solve for this; it's a question of processes and procedures. However, a tech vendor may have experience with this, and may be able to suggest low-cost procedures for keeping the database up-to-date	High costs for ongoing systems use and maintenance will make it hard to keep the system up-to-date	Specifying needs in contract; clearly outlining roles and responsibilities between partners; agreeing upon costs for ongoing use and maintenance in initial contract
Highly illiterate population with low mobile ownership	Biometrics will likely be more feasible than mobile authentication or user-controlled IDs that require management of one's own personal data	Biometrics (for example, a fingerprint or iris scan) may still lead to some exclusion if not all participants can provide the scan (respectively, if their fingerprints are too worn to scan, or their iris scan is not unique)	It may be necessary to have a *multimodal*[13] system that provides for multiple biometrics or a paper-based backup option
At-risk population with particularly high concerns of data privacy for fear of persecution	Data needs to be encrypted; the system must require multi-factor authentication; and the server must be held in a secure location	Regardless of security, unwanted actors might still request the data (e.g., a government might make a legal claim to the data) or find ways to access it (it is not safe to assume that encryption is 100% secure)	Adopt an approach of data minimization - only collect the least amount of data necessary —and have clear policies for how long data will be stored.
Citizens might not trust a new system because of a history of government corruption	Blockchain or distributed-ledger technologies (DLTs) may be applicable, since the data held on a distributed ledger is not held by any one central authority. Also, it cannot easily be changed without detection.	Data on a public blockchain is, by definition, open and transparent. Therefore, while it is extremely difficult to change the data, extra precautions need to be taken for any personally identifiable information collected.	Personally identifiable information will likely need to be held in a separate system, either a traditional database or a private permissioned blockchain to encrypt the data.
Problem:	_____ _____ _____	_____ _____ _____	_____ _____ _____

This table is not meant to be an exhaustive list of problems, solutions, risks, or risk mitigation strategies. It can, however, serve as an example of a way to ensure that you've defined your problems and project needs sufficiently before launching into the vendor procurement process.

TIP 2: AVOID VENDOR LOCK-IN

Supplier lock-in is a situation in which a customer using a product or service cannot easily transition to a competitor. This is usually the result of proprietary technologies that are incompatible with those of competitors. However, it can also be caused by inefficient processes or contract constraints. This can lead to high costs over time if your project is required to pay for high maintenance costs or system upgrades.

The first thing to understand is most tech vendors **try to lock customers in**. Vendors are understandably nervous about customers changing providers and therefore it is not necessarily in their self-interest to make transition between different solutions easy. Some vendors may have already realized that, on the contrary, helping their customers avoid lock-in improves the customer experience and therefore helps them retain customers over time. However, this cannot be assumed. It is therefore critical to keep this in mind throughout the RFP and contract negotiation processes.

A few ways that lock-in may occur:

- Data is not stored in a transferable format, so it will not translate to any other system without extensive manual changes to the formatting;
- The system does not provide an easy way to extract data if you want to transfer to another system;
- Systems upgrades are required and costly.

A quick analogy: can you download all of your emails and easily transfer them to another email server if you want to change? Likely, no; you're locked-in to your current email provider.

Here are some key ways to avoid vendor lock-in:

- Always ask in the RFP and contract negotiation process: "How do I get my data out in the future if I need or want to?" and "How do I make changes and modifications to the system going forward?"
- Select vendors who already comply with the draft **Technical Standards for Digital Identity.** The ongoing work to create technical standards for digital identity is a critical piece to ensure interoperability of systems and to help all organizations and governments avoid lock-in.
- Where possible, use open-source technologies. These allow for other developers, such as your own IT staff, to access the code to make changes in the future so that you aren't reliant on the original vendor for every change.

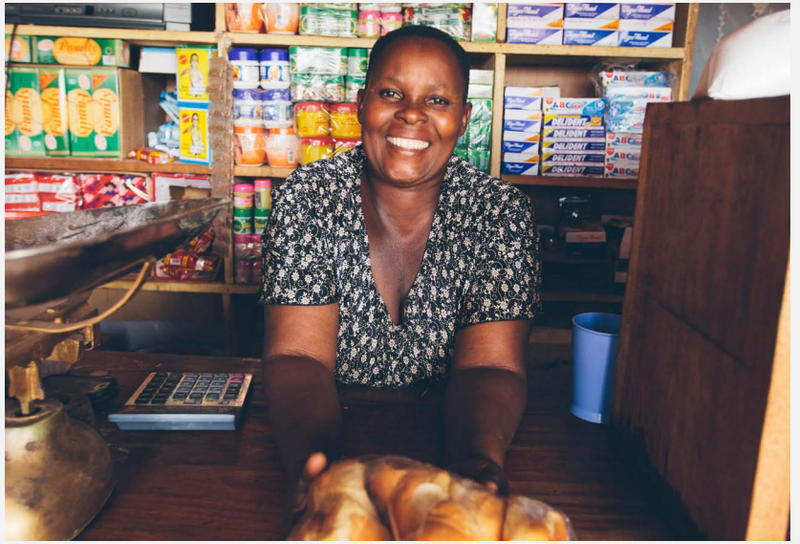


Photo Credit: Bobby Neptune/USAID

TIP 3: UNDERSTAND & DOCUMENT ALL COSTS

There are three main phases in the identity lifecycle.[14] Each will come with its own costs that must be considered from the beginning.

1. Registration, including enrollment and validation;
2. Issuance of documents and credentials; and
3. Use, or authentication/authorization of individuals who qualify for a given service.

Throughout the entire lifecycle, the vendor is also (ideally) responsible for:

1. Maintenance, including avoiding system outages and updating software to prevent fraud or other attacks;
2. Providing ways to update the list of authorized individuals in the case of birth, death, or changes to the qualifications for participation in the system; and
3. Troubleshooting and making small changes based on lessons learned during implementation.

Each of these costs should be accounted for and documented in the contract and Service Level Agreement (SLA).

Why? If all costs are not accounted for in the beginning, it is possible that the system may not be fully implemented or maintained over the long run, undermining the objectives of the program. As the 2016 Review of National Identity Programs conducted by the International Telecommunications Union (ITU) found, "while many programs include a central registry of citizen biometric information, few possess the equipment to verify citizens on site for financial or social transfers, elections, or other functions."[15] This can lead to costly identification efforts that are, "cosmetic, rather than functional,"[16] leading to severe problems for users and a subsequent lack of trust. It also undermines any efforts to Design for Reuse and Interoperability, as will be covered in the next section.

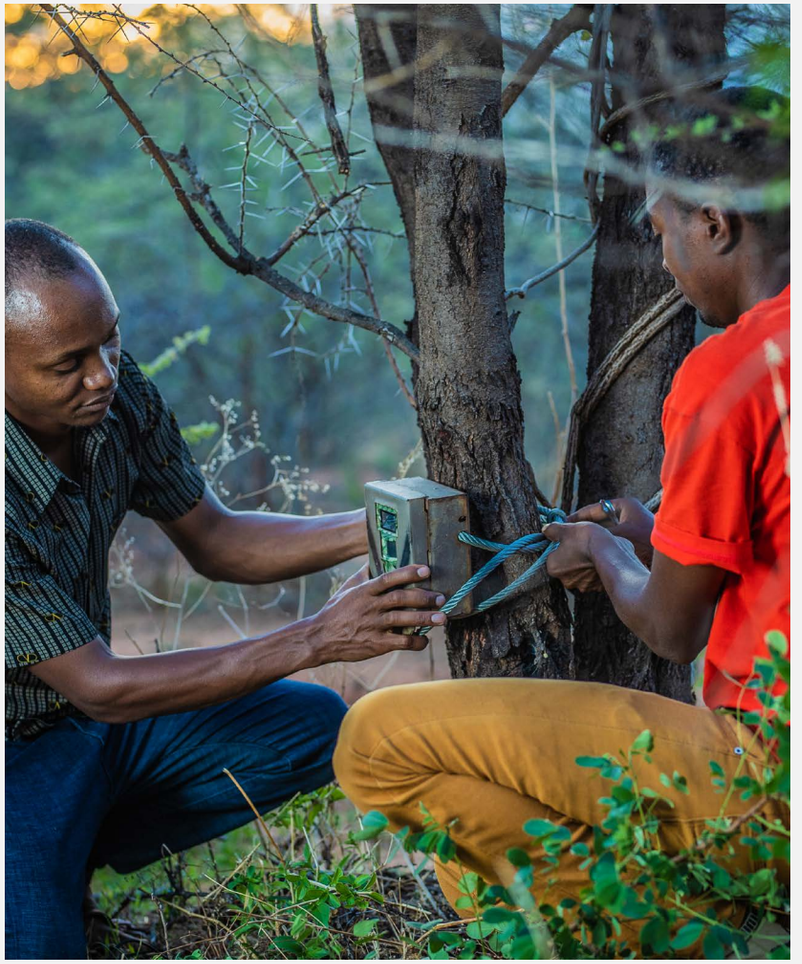


Photo Credit: Riaz Jahanpour for USAID

TIP 4: INSIST ON REFERENCES & TESTING

Just as with interviewing candidates for a job opening, asking questions is critical, but references may be even more informative. Once you have a shortlist of potential vendors, insist on the following:

1. References to clients who have worked with this tech vendor in the past.
2. If possible, a visit to witness an ongoing implementation of the technology.
3. Testing, not only in an office environment, but also with potential participants and in the intended geographic locations.

Some sample questions to ask of previous clients:

1. How quickly does the vendor respond in case of a problem?
2. What happens in case of a system outage? Have you experienced many system outages?
3. How does the system work in more challenging locations, such as those with low connectivity?
4. What has been your experience with making small improvements to the system during implementation?

TIP 5: SEEK EXPERT, IMPARTIAL ADVICE WHEN NEEDED

Digital ID is a new area, but not entirely new. There are initiatives such as ID4D and ID2020 that intend to promote inclusive digital ID and are highly familiar with the entire industry. There are consultants that have worked on previous implementations and may be helpful. Seek such expert, impartial advice during the procurement, testing, and contract process if needed to avoid the risks listed above.

Photo Credit: Mohammad Al-Arief/The World Bank

How-To: Design for Reuse and Interoperability

Photo Credit: Riaz Jahanpour for USAID

An ID system includes multiple functions, each which includes separate components that can be shared and reused. These functions include:

REGISTRATION

The processes and technology by which individuals are registered and issued an ID

USE

The processes and technology by which individuals actually use that ID

STORAGE

The servers and databases that store the data

DATA

The actual information collected on individuals registered in the system

When designing an ID system for a single project, it is possible to design that system from the start so that one or more of these components can be reused. This is a key strategy for supporting a shift from *instrumental* design that leads to isolated, single-application ID systems to *infrastructural* design of systems that can be repurposed for similar projects and are compatible with existing local systems.

During the **Mapping Workshop,** you ideally asked and documented the following questions regarding Sustainable Expansion:

- Which other institutions may want to use the ID system that you are creating?
- Which components might they want to use? For example, the registration process, the ID number or ID card, or the technology platform behind the ID system?
- Where else might individuals use the new ID to derive additional value? For example, banks, insurance companies, etc.

This information will come in handy now, as you can use it to fill in the following worksheet. This worksheet, which is filled in with illustrative information below, can help ensure that you are properly designing for reuse. Keep in mind that many of these steps can be difficult: working through procurement issues to determine how to transfer ownership or negotiating branding between multiple partners can be time consuming. Throughout the process, remind all stakeholders that investing the time and resources necessary to create sustainable, reusable systems will deliver significantly more value to all stakeholders, and most importantly to people like Mary, Joy, and Samuel, in the long run.

Sample Worksheet: Designing System Components for Reuse

FUNCTION	COMPONENT	INSTITUTION	CONSIDERATIONS
Registration	Registration drive included training of field staff, educational materials, and booths	May be relevant for the Ministry of Social Welfare's upcoming registration drive	Training needs to be well-documented so that it can be turned into a Training of Trainers; educational materials can have limited branding so that they can be reused
Use	Identity	Another Ministry has expressed interest in using the same ID card for an upcoming project	There are several ways for one organization to accept another organization's identity (a concept termed *federation*). • An organization can accept credentials issued by another organization, but still authenticate and authorize the individual locally (ex: a passport); • An organization can accept specific characteristics (attributes) describing an individual from another organization (ex: a credit score); • An organization can accept an authorization decision from another organization (ex: a driver's license accepted in a different state) With digital IDs, federation protocols like SAML (Security Assertion Mark-up Language) can help ensure that one organization can communicate the authentication of an identity to another organization.[17]
	Biometric Scanners	(same as above)	This is a hardware procurement, so it is necessary to clarify with the donor in advance if you can transfer ownership to another agency after your project is complete.

FUNCTION	COMPONENT	INSTITUTION	CONSIDERATIONS
Storage	Beneficiary Management System	Another Ministry has expressed interest in using the same ID card for an upcoming project	This is a software procurement, so there is need to clarify ownership with the donor in advance. Also, if purchasing a server, this is a hardware procurement, so the same applies. In addition, consider where the server is stored - if it is in your office, and the Ministry does not have the appropriate facilities, this will make the transfer harder. Using a storage facility may be a better option, if the Ministry is open to it. Cloud-based and open-source software will make it both easier to transfer and/or share ownership.
Data	ID number	(fill in the blank) _____ _____ _____	The ID number can serve as the ID number (unique identifier) for another organization's identification needs.
	Demographic information	(fill in the blank) _____ _____ _____	Demographic information needs to be considered in the context of **Data Privacy and Protection.** Data format and standards that match those of partners should be adopted where possible. The technology should allow for data to be easily exported and uploaded into a new database (with proper authorization). See more on this in the section on **Choosing a Tech Vendor.** If data might be shared with financial institutions, then it will need to comply with local KYC requirements.
	Additional information collected for M&E	(fill in the blank) _____ _____ _____	Special care should be paid to such additional information beyond sharing it with the donor. For example, if there is information on health conditions of patients, this should not be attached to any demographic or identifying information when sharing with external partners.

Designing for reuse is important, especially if you have identified a partner that is interested in using your system in the future. Designing for interoperability is critical, even if you haven't yet identified a partner, since it can ensure that your system can connect to and support foundational ID systems that may be planned in the near future. The best way to design for interoperability is to ensure that you follow the **Technical Standards for Digital Identity.** The standards, currently in draft form, are based on the work of the International Organization for Standardization (ISO). The ISO standards have been drafted in cooperation with many other prominent countries and industry consortia, are followed by most large-scale ID programs, and are widely supported and used by industry consortia.

Photo Credit: UN Photo/Bernardino Soares

Moving Forward

It is critical to balance the benefits of identification with empathy for the privacy, dignity, and agency of individuals. Ultimately, the key to sustainable ID investments is to see them as part of a broader journey to self-reliance. We can do so by taking steps, such as those outlined in this guide, to promote ID systems that are locally owned and operated, thereby minimizing long-term reliance on foreign financial support or technical capacity. Taking this type of infrastructural approach may not always be easy, but it's worth it when considering how ID systems support the broader goal to strengthen the regulatory, infrastructural, and workforce dimensions of digital ecosystems.

Photo Credit: Bobby Neptune/USAID

Resources

[1] See: World Bank Group and Center for Global Development (2017). "Principles on Identification for Sustainable Development: Toward the Digital Age."

[2] Note that these considerations assume that you are working on a digital ID system rather than a paper-based system. As noted in the introduction, digital systems are becoming increasingly common and tend to offer more opportunities for infrastructural design (such as designing for reuse and interoperability).

[3] Adapted from "Public Sector Savings and Revenue from Identification Systems," ID4D, The World Bank, 2018.http://pubdocs.worldbank.org/en/745871522848339938/PublicSectorSavingsandRevenueIDSystems-Web.pdf

[4] Adapted from Talent Futures Executive Coaching and Consulting http://www.talentfutures.com/3-4-2-Tools-Stakeholder-Mapping.htm

[5] Adapted from the Omidyar Networks Systems Practice Workbook, https://docs.kumu.io/content/Workbook-012617.pdf

[6] Church, Cheyanne and Mark Rogers, "Designing for Results," Search for Common Ground 2006. pg 6. https://www.sfcg.org/Documents/manualpart1.pdf

7 For more, refer to elan's Privacy Impact Assessment Tip Sheet http://elan.cashlearning.org/wp-content/uploads/2016/05/Privacy-impact-tipsheet.pdf

[8] For more on Lean Data broadly, see https://ssir.org/articles/entry/the_power_of_lean_data, and in the context of data protection, refer to Considerations for Using Data Responsibly at USAID.

[9] Proportionality means that organizations will try to only collect data that is necessary to achieve their purpose and only store data for the minimum time necessary to serve that purpose. Purpose Limitation encourages organizations to only process data when there is an explicit and legitimate purpose. Data minimization encourages organizations to collect and process only the minimum amount of personal data required to achieve an objective.

[10] Informed consent, as defined by the U.S. government, involves three features: (1) disclosing sufficient information about direct risks and benefits to a participant so he or she can make an informed decision on whether to participate, (2) making sure the participant truly understands this information, and (3) making sure the decision to participate is truly voluntary. In general it is best practice to seek consent whenever an activity involves individuals; however, it is federally required when it involves human subjects research. Design Considerations for Context-Appropriate Data Protection provides a framework for appropriate design decisions for a digital ID system based on population characteristics, including level of vulnerability and likely ability to understand and provide informed consent.

[11] Kuner, Christopher and Massimo Marelli, Handbook on Data Protection in Humanitarian Action, ICRC and Brussels Privacy Hub, July 2017. pg 23 https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

[12] ICRC 55.

[13] For more on multimodal biometric systems, refer to ID4D's Technical Standards for Digital Identity, page 25. http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf

[14] WB, GSMA, and SIA October 2014.

[15] "Review of National Identity Programs," ITU, May 2016. https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review%20of%20National%20Identity%20Programs.pdf

[16] Gelb and Clark, "Identification for Development: The Biometrics Revolution," CGD, January 2013. https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf

[17] Technical Standards for Digital Identity, page 5.

Additional Resources on Data Protection

"Data Privacy, Ethics, and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda," United Nations Development Group, 2018
https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf

Handbook on Data Protection in Humanitarian Action, ICRC and Brussels Privacy Hub, July 2017. pg 23
https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

The Data Protection Starter Kit created by the Electronic Cash Transfer Learning Action Network (elan) and the Cash Learning Partnership (CALP)
http://www.cashlearning.org/news-and-events/news-and-events/post/399-introducing-the-elan-data-starter-kit

USAID

FROM THE AMERICAN PEOPLE