Decoded: Digital Identity in Public Benefits

Center on Budget and Policy Priorities

Session 2: Digital Identity

Symonne Singleton (she/they)
Digital Services Analyst, CBPP
ssingleton@cbpp.org

Elizabeth Bynum Sorrell, PhD (she/her/hers)
Project Researcher, Digital Benefits Network
elizabeth.bynum@georgetown.edu

Agenda

Introductions

Key Terms + Level-setting

Introduction to Digital Identity Standards: NIST

Digital Identity + Public Benefits: Landscape Overview

Discussion

GEORGETOWN UNIVERSITY | beeckcenter social impact + innovation | Digital Benefits NETWORK

Supporting government to ensure public benefits technology is accessible, effective, and equitable — and increase economic opportunity.

SNAP | WIC | Medicaid/CHIP | TANF | Basic Income | UI | Child Care

Digital Identity in Public Benefits

- People in the public benefits space will likely interact with online services that may ask them to prove identity or create an account at some point
- Increasingly common during and after the pandemic, especially in the UI space
- Services like ID.me received big contracts, rollouts led to access concerns
- Unnecessary digital identity requirements may cause barriers
- Questions to answer:
  - How can we improve the digital identity landscape?
  - What is useful background information?

Key Terms

Digital Identity

Identity Proofing

Authentication

Application vs Case Management Portal

Biometrics

Knowledge-based verification (KBV)

Single-sign-on (SSO)

Two-factor authentication (2FA)

Digital Identity

- "The unique representation of a person engaged in an online transaction" - NIST Digital Identity Guidelines
- In context:
  - You may use a specific digital identity to access a service online (e.g., username, account)
  - Having an account or username does not mean a service provider knows who you are IRL
  - People represent themselves online in multiple, distinct ways

Identity Proofing

- Identity Proofing process by which a credential service provider (agency, or third party) collects, validates, and verifies information about a person.
  - Used to establish confidence that someone is who they claim to be
  - Sometimes referred to as Identity Verification
  - Can happen remotely or in person.
    - You may have also heard this called Remote Identity Proofing (RIDP).

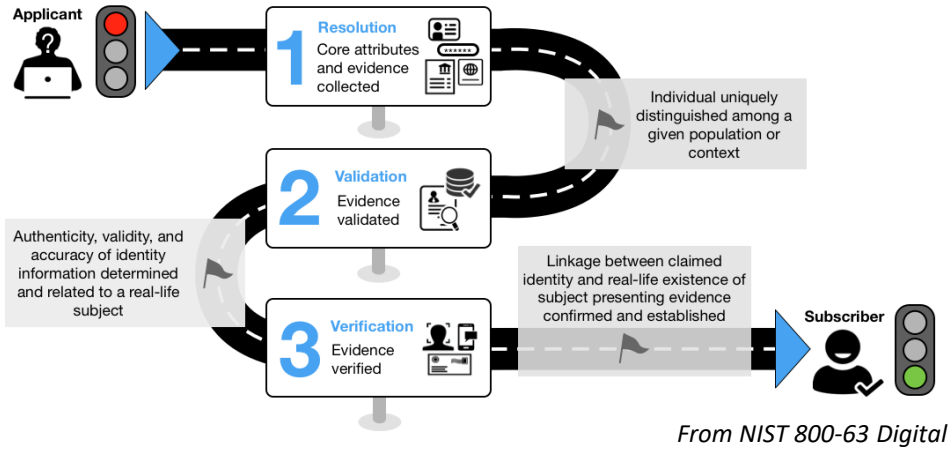


Figure 4-1 The Identity Proofing User Journey

From NIST 800-63 Digital Identity Guidelines

Authentication

- The process of determining the validity of one or more authenticators used to claim a digital identity--NIST
- Authentication establishes that a person attempting to access a digital service is in control of the technologies used to authenticate.
- Involves demonstrating you have control over one or more types of authenticators, e.g.,
  - Something you know – a password or pin
  - Something you have – one-time passcode (OTP) sent to a device, a certificate, a cryptographic key
  - Something you are – biometric information

Application vs Case Management Portal

- In public benefits, people commonly interact with their digital identity in two places:
  - At online application
    - Recommendation: No proofing before application
  - Accessing a case management portal
    - Some authentication or proofing may be necessary because private information can be accessed
- Status quo: if information is being returned from a confidential data source, then some type of proofing is necessary

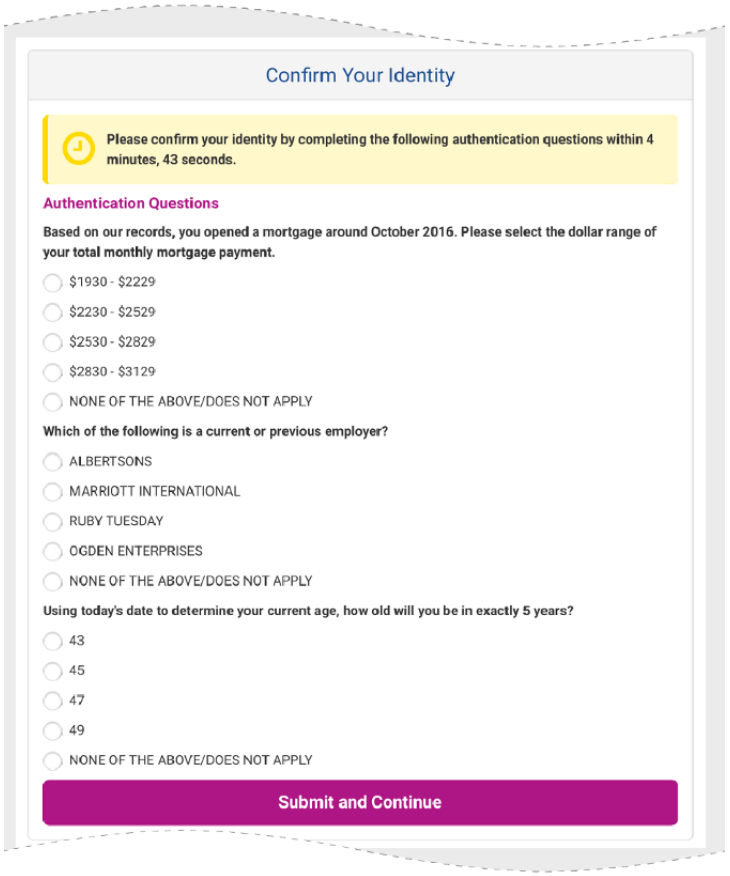
Biometrics

- In the context of identity, biometrics refers to automated recognition of individuals based on their biological and behavioral characteristics.
- Common forms of biometrics are:
  - Face recognition technology
  - Fingerprints
  - Voice recognition
- Equity concerns
- Security concerns

Knowledge Based Verification (KBV)

- Identity verification method based on knowledge of private information associated with the claimed identity.
- Increasingly popular as a response to security concerns during the pandemic
- This is also often referred to as knowledge-based authentication (KBA) or knowledge-based proofing (KBP).
- Requires answering multiple choice questions
- Info from credit history such as past addresses, information about cars purchased, and past cities of residence.
- Equity concerns – no credit history, identity theft etc.
- Security concerns - data breaches.

Example of identity proofing questions



Single-sign-on (SSO)

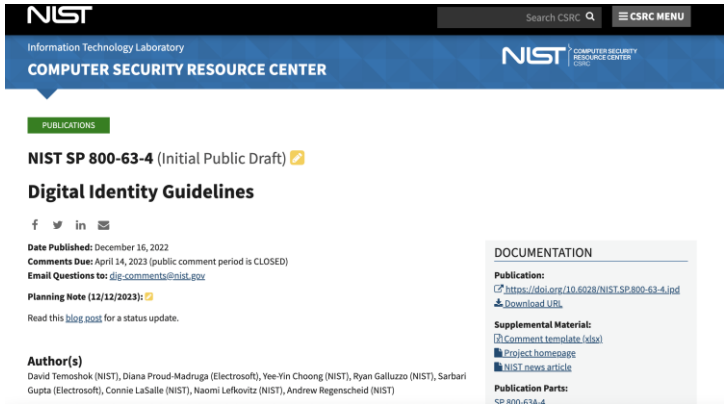
- An authentication framework that allows the use of a single set of credentials to login to multiple related software systems (ex., state-wide SSO).
- Authentication for one part of the system may automatically authenticate the user in other parts.
- There may be conflicting requirements for each system accessed
  - Ex: Medicaid or SNAP vs Drivers License renewal
    - Might be workable for people accessing certain portions of the system, but not for people accessing public benefits
- Typically, most restrictive requirements are applied, but this may lead to access concerns

Two-factor authentication (2FA)

- Authentication using two or more factors to achieve authentication.
  - using a password then responding to push notification from authentication app
- Multi-factor authentication (MFA) may require users to employ more than two authentication factors.
- Access + security concerns

What is NIST?

- NIST standards matter because:
  - They are default industry standard
  - Private vendors refer to NIST standards
  - States may also refer to NIST, although they are not necessarily required to follow standards
- Standards-making organization, part of the US Department of Commerce
- NIST Publication 800-63, “Digital Identity Guidelines”
  - Details a risk-based process and technical requirements for managing digital identities
  - Currently revising guidelines



Risk Management

- Risk management is the process of identifying, assessing, and addressing possible security risks
- Types of risk could include:
  - Liability and policy violations
  - Public image
  - Release of sensitive information
  - Financial loss
  - Personal safety
  - Risk to an individual vs risk an organization
- Prioritize equity and access while considering risks

NIST Assurance Levels

- Guidelines include framework for "assurance levels" for identity proofing, authentication, and federation
- Higher level of risk (to organization, individual) → higher assurance levels to increase confidence in who someone is, or that they are same person returning to an account
- *Takeaways:*
  - *There are levels of identity proofing and authentication that move from least to most stringent (IAL1-IAL3)*
  - *Different services/systems, have different risks and identity proofing/authentication should be tailored accordingly*

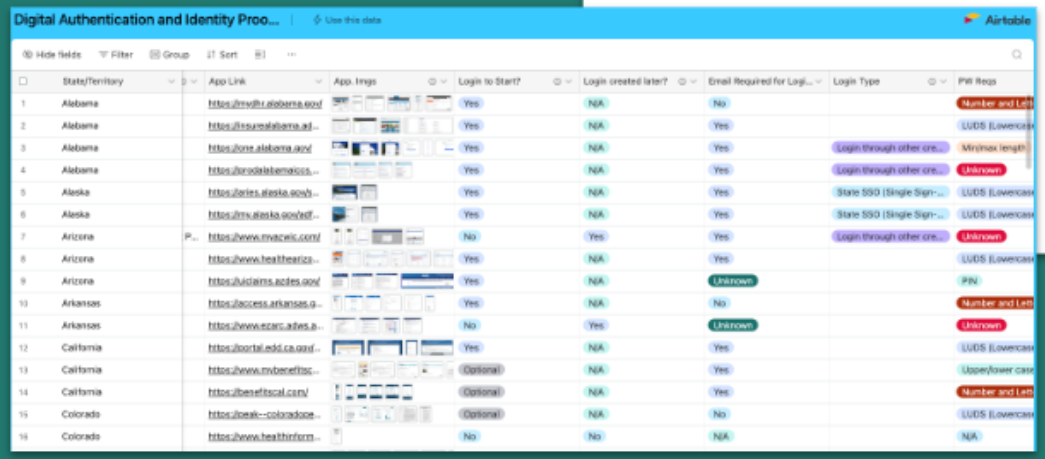
Equity Concerns Related to Identity Proofing + Authentication

- KBV: Limited or No Credit History
- Data: are we collecting unnecessary information, who stores or accesses it after proofing is completed?
- Access:
  - Documents
  - Technology
  - Language
- Biometric Bias: race and gender
- Psychological costs (dignity, distrust, surveillance)
- Consequence: if you can't meet identity proofing requirements, how can you access services?

Questions?

Landscape Overview

beeckcenter.org/ID



Digital Benefits Hub

About Explore Topics Connect

Digital Authentication and Identity Proofing in Public Benefits Applications

By Elizabeth Bynum Sorrell, Researcher and Ariel Kennan, Fellow

Digital Benefits Network at the Beeck Center for Social Impact + Innovation at Georgetown University

May 19, 2023, *last updated May 19, 2023*

Agencies that administer public benefits applications online continually balance multiple potentially conflicting priorities around privacy, fraud prevention, and accessibility to ensure equitable outcomes. As we started our research on digital identity in public benefits, we quickly learned that there was not a single, publicly available, source of information documenting digital authentication and identity practices across public benefit program applications. By releasing this dataset, we aim to make it easier to quickly understand the landscape of digital authentication and identity proofing practices currently in use across core public benefits programs, including:

- Supplemental Nutrition Assistance Program (SNAP)
- Temporary Assistance for Needy Families (TANF)
- Medicaid
- Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)
- Child Care Assistance (CCAP)
- Unemployment Insurance (UI)

Center on Budget and Policy Priorities

Landscape Overview

Looking at initial applications for SNAP, TANF, Medicaid, WIC, child care, and unemployment insurance, the DBN asked:

- When and how do applicants need to create a log-in to apply for benefits online?
- What kinds of PII are applicants required or requested to provide when applying online?
- When and how are applicants asked to take active steps to prove their identities in order to apply online?
- What identity proofing methods are applicants asked to use?

Reviewed 158 combined and standalone online applications across these six programs

Landscape Overview

- 75% of applications require applicants to login/create an account to start an application.
- 31 applications use govt. single sign-on services (SSOs)
- ~1/3 of applications require or prompt active identity proofing actions as part of an online application process.
    - Use of identity proofing varies across programs

Digital Identity in Public Benefits: Landscape Overview

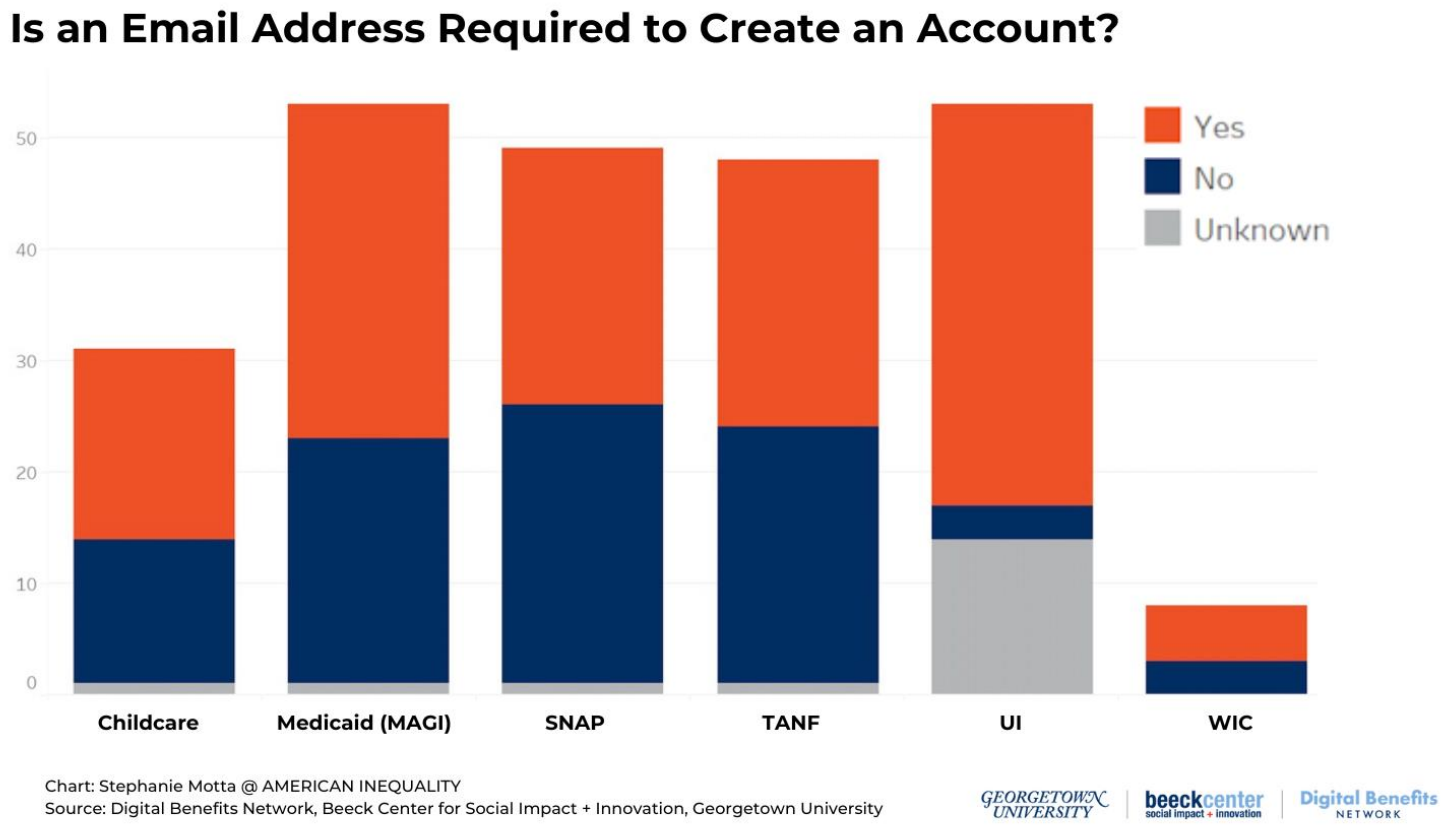


Chart: Stephanie Motta @ AMERICAN INEQUALITY
Source: Digital Benefits Network, Beeck Center for Social Impact + Innovation, Georgetown University

GEORGETOWN UNIVERSITY | beeckcenter social impact + innovation | Digital Benefits NETWORK

Center on Budget and Policy Priorities

Landscape Overview

- ~1/3 of applications require or prompt active identity proofing actions as part of an online application process.
    - Use of identity proofing varies across programs

Digital Identity in Public Benefits: Landscape Overview

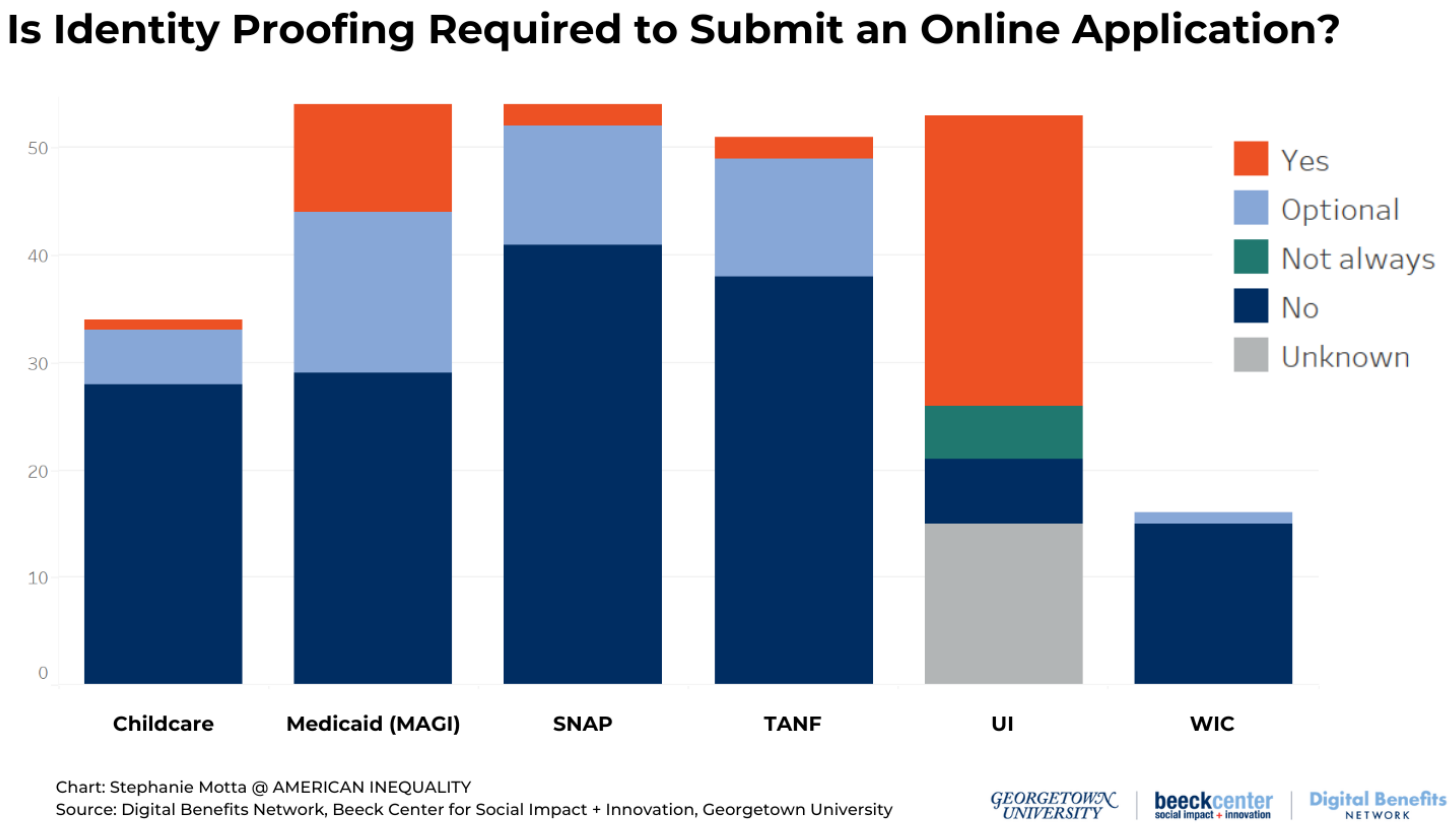
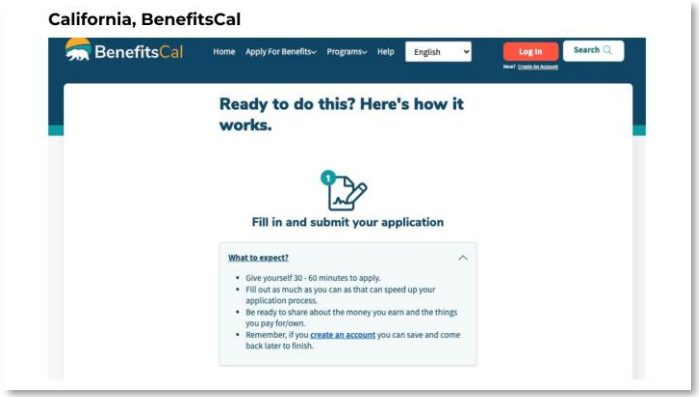


Chart: Stephanie Motta @ AMERICAN INEQUALITY
Source: Digital Benefits Network, Beeck Center for Social Impact + Innovation, Georgetown University

Promising Design Patterns

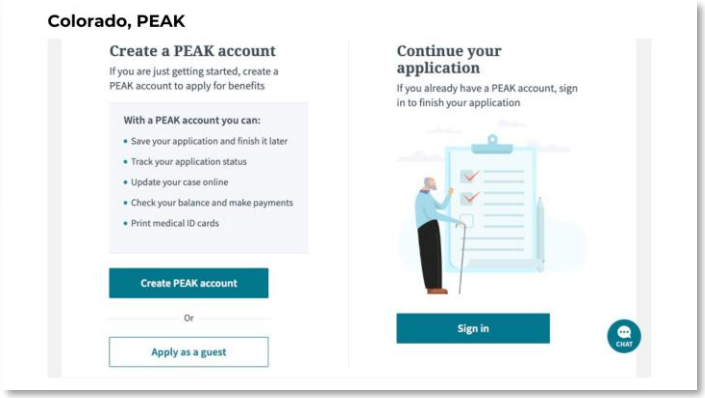
- Application processes that do not require account creation or identity proofing to submit an initial application
- Account creation processes that are optional, with clear explanations about the benefits
- Online application processes that allow users to opt out of online identity proofing, with clear instructions
- In-person identity verification pathways

California, BenefitsCal



https://beeckcenter.org/digid_practices

Colorado, PEAK



Discussion

- Jamboard
  - Optional: add name + state to sticky note
- Questions:
  - What is happening in your state's benefits online application portal?
    - *What are the requirements? Do you have to identity proof before application or access case management? (specify which benefits program application/system you're referencing)*
  - What challenges have you seen clients face with authentication and/or identity proofing? How has it impacted them?
  - What additional information or resources would support you in advocating for improved digital identity experiences in your state?

Takeaways:
Questions to consider

- What is the status in your state?
  - If there is identity proofing that is prohibitive, why is it being included?
    - Is it necessary or required?
      - No? Remove the step
      - Yes?
        - How can I make it better?
          - Reorder the steps
          - Rephrase the questioning in plain language or translation
          - Provide clear in person alternatives
            - Ex: trusted application assister approving ID in person

Questions?

Resources

- Shaping Digital Identity Standards – Center for Human Rights and Global Justice (NYU Law)
- Removing Barriers to Access from Remote Identity Proofing - CBPP
- Digital Authentication and Identity Proofing in Public Benefits Applications - Digital Benefits Network
- Promising Practices for Digital Identity in Public Benefits – Digital Benefits Network
- What is Digital Identity? - Digital Benefits Network
- Digital Identity Glossary – Digital Benefits Network
- NIST Digital Identity Guidelines (Draft 4) - NIST
- Benefits Enrollment Field Guide – Code for America
- Digital Identity Risk Assessment Playbook - Identity, Credential, and Access Management Subcommittee (ICAMSC)