### 9. Usability Considerations

ISO/IEC 9241-11 defines usability as: Extent to which a product can be used by specified *users* to achieve specified *goals* with effectiveness, efficiency and satisfaction in a specified *context of use*. This definition focuses on users, goals, and context of use as key elements necessary for achieving effectiveness, efficiency and satisfaction. A holistic approach considering these key elements is necessary to achieve usability.

The overarching goal of usability for enrollment and identity proofing is to promote a smooth and positive enrollment process for users by minimizing user burden (for example, their time and frustration), and minimizing enrollment friction (for example, the number of steps a user must complete, and the amount of information they have to keep track of).

The enrollment and identity proofing process will set the stage for a user’s interactions with a given authenticator for access to an online service. Negative first impressions can influence later user perceptions of subsequent interactions with the organizations online services and practices. Therefore, organizations should strive to promote a positive user experience throughout enrollment and identity proofing.

Enrollment and identity proofing steps and processes should be designed and implemented to make it easy for users to do the right thing, hard to do the wrong thing, easy to recover when something goes wrong, and hard for someone to impersonate an individual. Enrollment and identity proofing process are effectively delivered when considered from the user perspective. Organizations that are cognizant of the overall implications of their stakeholders’ entire enrollment and identity proofing process, keeping in mind the combination of users, their goals, and context of use, will benefit from an improved experience for their users. Performing a usability evaluation on the enrollment and identity proofing process is critical, conducting them with representative users, realistic goals and tasks, and appropriate contexts of use.

The current section takes this holistic view in applying usability principles to the enrollment and identity proofing process, with the goal of raising implementers’ awareness of usability considerations associated with enrollment and identity proofing (for usability considerations for typical authenticator usage and intermittent events, see 800-63-3B).

**ASSUMPTIONS**

In this section, the term “users” means “Applicants” or “Subscribers.”

This section describes guidelines and considerations from the end-users’ perspective, as usability guidelines can only be written from the end-users’ perspective.

Accessibility and usability differ significantly; therefore, accessibility is out of scope for this section. However, organizations should obviously address accessibility in their implementation plans.

### 9.1 User Experience During Enrollment and Identity Proofing

The first step for organizations is getting to know the user to promote a smooth and positive enrollment process. Before users begin the enrollment and identity proofing process, organizations should match users with suitable CSPs based on users’ characteristics. From the user perspective, there are three primary stages to enrollment and identity proofing: pre-enrollment preparation, the enrollment and proofing session itself, and post-enrollment actions. Note that these stages may occur within a single session or there could be significant time elapsed between each stage (for example, days or weeks).

Usability considerations for each stage are detailed below. Most of the usability considerations apply to all identity proofing approaches. However, additional considerations are provided for specific proofing methods.

### 9.1.1. Pre-Enrollment Preparation

Since a successful enrollment session is challenging and frustrating without sufficient user preparation, this section is devoted to describing the necessary approach to help ensure sufficient pre-enrollment preparation. Ensuring that users are sufficiently prepared for their enrollment sessions is critical to the overall success and usability of the enrollment and identity proofing process. Such preparation can only be realized if users receive the necessary information (i.e., proofing and enrollment requirements) in a usable format, provided at an appropriate time. Users must be fully informed regarding exactly what identity evidence they need to bring to an enrollment session, regardless of whether it is in-person, virtual in-person, or remote. Such information must be conveyed from the users’ perspectives, not from the implementers’ perspectives. For example, while organizations need to know in advance what type of IAL is required for access to a particular information system, users do not need to know anything about IALs or whether the identity evidence required is scored as ‘adequate’, ‘strong’, or ‘superior’; users simply need to know exactly what materials are required, and how and where to provide them.

Provide users the information necessary to ensure they are fully prepared for their enrollment session. Such information allows users to make an informed decision regarding whether they wish to proceed with the enrollment process. Usability considerations associated with preparing users for their enrollment session include:

* Inform users of the entire enrollment process. Users need to know what to expect throughout the enrollment process, including what they will experience at each individual step of the process.
  + It is especially important to clearly explain expected timeframes to users. Users need to understand how long the enrollment process will take, so they can plan accordingly.
* Inform users why they need to participate in the enrollment process. Users need to understand the necessity for identity proofing and how it can benefit them.
* Minimize the number of steps required for enrollment, and make each step as clear and easy as possible for users. Users are easily frustrated by large numbers of confusing steps.
* If there is a fee for enrollment, users must be informed of the monetary amount of the fee, and the acceptable forms of payment. Offering a larger variety of acceptable forms of payment allows users to choose their preferred payment option.
* Inform users whether their enrollment session will be in-person, virtual in-person, or remote (and whether a user is allowed to choose). Only provide information relevant to the allowable session option(s). For example, if a user is best suited to complete an in-person session, do not provide information about virtual in-person or remote sessions, as superfluous information will confuse users.
  + For in-person or virtual in-person sessions, provide users information regarding the location(s) where the session will take place (and whether a user is allowed to choose their preferred location). Provide users with logistical information necessary to reach the enrollment session location(s). For example, provide directions for arrival via a variety of transportation means (e.g., car, public transportation) and parking and entrance information if applicable.
  + For remote sessions, provide users information regarding the technical requirements they must meet to complete a remote session (e.g., requirements for internet access).
  + Appointments for in-person or virtual in-person identity proofing sessions should be offered. Users should be encouraged to set up an appointment in order to minimize wait times at enrollment sessions. If walk-ins are allowed, it should be made clear to users that their wait times may be increased without an appointment.
    - Provide clear instructions to users regarding setting up an enrollment session appointment and reminders, and how to reschedule existing appointments.
    - Provide users with appointment reminders and allow users to specify their preferred appointment reminder format(s) (e.g., postal mail, voicemail, email, text message). Appointment reminders should include all enrollment session information pertinent to the user’s session: date, time, and location (or technical requirements for a virtual in-person session, for example a link to join a virtual session), description of required identity evidence.
* Inform users of the exact identity evidence and attributes needed for enrollment, and whether each piece is voluntary or mandatory in order to complete the identity proofing process. Inform users of the consequences for not providing the complete set of identity evidence.
  + All allowed and required identity evidence must be clearly described. Users need to know the specific combinations of identity evidence allowed and required for enrollment, including requirements specific to a particular piece of identity evidence (for example, a raised seal required on a birth certificate; or an original authenticator for obtaining a derived authenticator). This is especially important because users may face significant difficulty procuring the identity evidence necessary for enrollment.
  + Where possible, implement tools to make it easier for users to obtain the necessary identity evidence.
  + Inform users of any special requirements for minors and people with unique needs. For example, provide users with the information necessary to utilize trusted referees, such as a notary, legal guardian, or some other form of certified individual that can legally vouch for and/or act on behalf of the individual (see Section 5.4.4).
  + If forms are required:
    - Provide users fillable forms prior to their enrollment session. However, forms must also be available at the enrollment session (if it’s in-person), as users should not be required to have access to a printer.
    - Minimize the amount of information users must enter on a form, as users are easily frustrated and more error-prone with longer forms. Where possible, pre-populate forms to reduce the amount of information a user must enter.
* Characteristics of information presented to users, either digitally or in physical form.
  + Follow good information design practice for all user-facing materials (for example, information provided in preparation for enrollment, enrollment appointment reminders, enrollment codes, data collection notices, fillable forms).
  + Any user facing materials should be written in plain language for the intended audience. Avoid the use of technical jargon and write for a 6th to 8th grade literacy level. For example, keep writing style simple; use active voice and conversational style; sequence main points in a logical manner; use short words and sentences; avoid double negative expressions; use the same word consistently rather than synonyms to avoid confusion; use bullets, numbers, and formatting where appropriate to aid readability.
  + Legibility of user facing text or text entered by users should be considered, such as font style, size, color, and contrast with surrounding background. Font legibility is important because users have different levels of visual acuity. Illegible text will contribute to user comprehension errors or user entry errors (e.g., when completing fillable forms). For example, legibility considerations include:
    - The highest contrast is black on white.
    - Sans serif font styles are recommended for electronic materials; serif fonts are recommended for paper materials.
    - Fonts that do not clearly distinguish between easily confusable characters (such as the capital letter “O” and the number zero “0”) are not recommended for use. This is especially important for the use of enrollment codes.
    - If possible depending on the size of the display medium, a minimum font size of 12 points is recommended as long as the text fits for display.
* Provisions for technical assistance.
  + Information on how and where to acquire technical assistance should be clearly communicated to users. For example, provide users information such as a link to online self-service feature, chat sessions, and a phone number for help desk support. Ideally, sufficient information should be provided to enable users to answer their own enrollment preparation questions without outside intervention.

### 9.1.2. Enrollment and Proofing Session

As described above, prior to the actual enrollment session, users should have received the proofing and enrollment requirements and expectations in a usable format, provided at an appropriate time.

Usability considerations for the enrollment session include:

* At the start of the enrollment session (regardless of whether it is in-person, virtual in-person, or remote), remind users of the enrollment session procedure. Do not expect them to remember all of the information they received during the pre-enrollment preparation stage. Users need to know what to expect throughout the enrollment session, including what they will experience at each individual step of the session.
  + If the enrollment session does not follow immediately after the pre-enrollment preparation stage, it is especially important to clearly remind users of the typical timeframe to complete the proofing and enrollment phase. Users need to understand how long the enrollment session will take, so they can plan accordingly.
    - Provide rescheduling options (for in-person or virtual in-person), as users may need to reschedule their enrollment session appointment if they do not have adequate time to complete the enrollment session.
  + Provide a checklist with the allowed and required identity evidence to ensure that users have the requisite identity evidence to proceed with the enrollment session, including enrollment codes if applicable. If users do not have the complete set of identity evidence, they must be informed regarding whether they can complete a partial identity proofing session. Users should be notified regarding what information will be destroyed and what, if any, information will be retained for future follow-up sessions, and what identity evidence they will need to bring to complete a future session. Ideally, users should be allowed to choose whether they would like to complete a partial identity proofing session or not.
  + It is important to set user expectations regarding the outcome of the enrollment session. For example, will the user receive a authenticator immediately at the end of a successful enrollment session, will they have to schedule an appointment to pick it up in person, or will they receive it in the mail weeks later? Setting user expectations is critical, as many users have prior experience with identity verification that may drive their expectations (e.g., receiving a drivers license in person, receiving a passport in the mail).
* Characteristics of information presented to users, either digitally or in physical form.
  + Follow good information design practice for all user-facing materials (for example, data collection notices, fillable forms).
  + Any user facing materials should be written in plain language for the intended audience. Avoid the use of technical jargon and write for a 6th to 8th grade literacy level. For example, keep writing style simple; use active voice and conversational style; sequence main points in a logical manner; use short words and sentences; avoid double negative expressions; use the same word consistently rather than synonyms to avoid confusion; use bullets, numbers, and formatting where appropriate to aid readability.
  + Legibility of user facing text or text entered by users should be considered, such as font style, size, color, and contrast with surrounding background. Font legibility is important because users have different levels of visual acuity. Illegible text will contribute to user comprehension errors or user entry errors (e.g., when completing fillable forms). For example, legibility considerations include:
    - The highest contrast is black on white.
    - Sans serif font styles are recommended for electronic materials; serif fonts are recommended for paper materials.
    - Fonts that do not clearly distinguish between easily confusable characters (such as the capital letter “O” and the number zero “0”) are not recommended for use. This is especially important for the use of enrollment codes.
    - If possible depending on the size of the display medium, a minimum font size of 12 points is recommended as long as the text fits for display.
* During the enrollment session, there are several requirements to provide users with explicit notice at the time of identity proofing, such as what data will be retained on record by the CSP (see Section 4.2 and Section 8 for detailed requirements on notices). For each notice, as described above, usability considerations for characteristics of information presented to users, either digitally or in physical form, applies. The use of plain language and usable formatting is especially important for notices, since users have a tendency to gloss over and ignore complex legalistic text in long paragraph form. If CSPs seek consent from a user for additional attributes or uses of their attributes for any purpose other than identity proofing, authentication, authorization or attribute assertions, per 4.2(5), CSPs should be aware that requesting additional attributes or uses may be unexpected or make users uncomfortable. If users do not perceive benefit(s) to the additional collection or uses, but only perceive extra risk to their information, they may be unwilling or hesitant to provide consent or continue the process. CSPs should provide users with explicit notice of the additional requirements. For each notice, as described above, usability considerations for characteristics of information presented to users, either digitally or in physical form, applies. The use of plain language and usable formatting is especially important for notices, since users have a tendency to gloss over and ignore complex legalistic text in long paragraph form.
* If at all possible, avoid using KBV, as KBV is extremely problematic from a usability perspective. It is error-prone and frustrating for users given the limitations of human memory, and has a low probability of success.
  + The types of questions used in KBV are often extremely difficult for users to answer correctly. The questions often ask users to recall old, infrequently used information, or information that changes over time. Although such information may be available in private databases, it does not necessarily mean that users can accurately recall, recognize, or find the requested information. KBV questions must still have relevance to users for them to be able to answer correctly. For example, if users lived somewhere for a very short period of time many years ago, it is very unlikely they will remember the address.
  + As described above, usability considerations for characteristics of information presented to users, either digitally or in physical form, apply to the phrasing of all KBV questions. It is especially important that KBV questions are clearly phrased, as ambiguity can lead to user errors when answering. For example, if asking about a user’s remaining mortgage balance, the KBV question should clearly specify which mortgage because users may have multiple mortgages. This question can be phrased as “What is the remaining mortgage balance on your primary residence?” to reduce ambiguity without compromising the integrity of the proofing process and without revealing unnecessary details about the individual.
  + Free form versus multiple choice KBV questions have different usability implications. Free form responses require recall memory, whereas multiple choice responses require recognition memory.
    - If free form responses are required, all semantically correct answers should be accepted. For example, accept all aliases for a user’s school name: full name, short name, and widely used nickname. Acceptable responses should not be case-sensitive and should ignore the use of pronouns such as ‘the’ or ‘a’.
    - If multiple choice KBV responses are used, they should be written to limit confusion.
  + If users are eligible to opt-out of KBV questions, they should be informed. As described above, usability considerations for characteristics of information presented to users, either or in physical form, apply to the phrasing of the KBV opt-out option.
  + Prior to being asked KBV questions, users must be informed of the number of allowed attempts. As they progress through the KBV process, users must be informed of the number of remaining attempt(s).
  + Prior to being asked KBV questions, users must be informed that KBV questions will change on subsequent attempts.
  + Prior to being asked KBV questions, users must be informed about timeouts. During the KBV session, users should be given timeout inactivity warnings prior to timeout.
* If an enrollment code is issued:
  + Users should be notified in advance that they will receive an enrollment code, when they should expect it, the length of time for which the code is valid, and the means by which it will arrive (physical mail, mobile telephone (SMS or voice), landline telephone, email, or physical mailing address).
  + When an enrollment code is delivered to a user, it should include instructions on how to use the code, and the length of time for which the code is valid. This is especially important given the short validity timeframes specified in Section 4.5.6.
    - If a machine readable optical label, such as a QR Code, is used (see Section 4.7), then provide users with information on how to obtain QR code scanning capabilities (e.g., acceptable QR code applications).
  + If enrollment codes expire or are lost before use, users should be informed that they will be required to repeat the enrollment process.
* At the end of the enrollment session,
  + If enrollment is successful,
    - Users should receive confirmation regarding the successful enrollment and be informed regarding next steps. For example, when and where to pick up their authenticator, or when it will arrive in the mail.
  + If enrollment is partial (due to users not having the complete set of identity evidence, users choosing to stop the process, or session timeouts),
    - Users should be notified regarding what information will be destroyed and what, if any, information will be retained for future follow-up sessions, and what identity evidence they will need to bring to complete a future session.
  + If enrollment is unsuccessful,
    - Users should be provided with clear instructions for alternative enrollment session type(s), for example, offering in-person proofing if users failed remote proofing.
* If users receive the authenticator during the enrollment session, they should be given information relevant to the use and maintenance of the authenticator. For example, instructions for use (especially if there are different requirements for first-time use or initialization), information on authenticator expiration, what to do if the authenticator is lost or stolen.
* Provisions for technical assistance.
  + Information on how and where to acquire technical assistance should be clearly communicated to users. For example, provide users information such as a link to online self-service feature, chat sessions, and a phone number for help desk support. Ideally, sufficient information should be provided to enable users to answer their own enrollment questions without outside intervention.
* Depending on enrollment session type (in-person, virtual in-person, or remote), additional usability considerations apply.
  + In-person
    - At the start of the enrollment session, operators should explain their role to users. For example, will operators walk users through the enrollment session step by step, or will they observe silently and only interact with users as needed?
    - If users choose to complete a partial enrollment session (due to not having the requisite set of identity evidence), provisions to schedule a follow-up session to complete the enrollment process should be offered. The previously identified usability considerations for appointments still apply.
    - If biometrics are being collected during the enrollment session, provide users clear instructions on how to complete the collection process. Instructions should be provided just prior to the collection process. Verbal instructions with corrective feedback from a live operator are the most effective. For example, instruct users where the biometric sensor is, when to start, how to interact with the sensor, and when the biometric collection is completed.
    - If users receive the authenticator during the enrollment session, operators should demonstrate use of the authenticator. Operators should help users test the authenticator during enrollment sessions to ensure the authenticator works correctly and users understand its operation.
  + Virtual in-person
    - If enrollment sessions are conducted in publicly observable spaces (e.g., a kiosk in a bank or supermarket), users may be concerned that others can view their activity and identity evidence. Care should be taken in the design and placement of the enrollment station to minimize user concern of being observed by others. Users may be reluctant to bring identity evidence to certain public places (bank versus supermarket), as it increases exposure to loss or theft.
    - At the start of the enrollment session, users need to be informed that they must not depart during the session, and that all their actions must be visible throughout the session.
    - At the start of the enrollment session, operators should explain their role to users. For example, will operators walk users through the enrollment session step by step, or will they observe silently and only interact with users as needed?
    - If users choose to complete a partial enrollment session (due to not having the requisite set of identity evidence), provisions must be made to schedule a follow-up session to complete the enrollment process. The previously identified usability considerations for appointments still apply.
    - If biometrics are being collected during the enrollment session, provide users clear instructions on how to complete the collection process. Instructions should be provided just prior to the collection process. Verbal instructions with corrective feedback from a live operator are the most effective. For example, instruct users where the biometric sensor is, when to start, how to interact with the sensor, and when the biometric collection is completed.
    - If users receive the authenticator during the enrollment session, operators should demonstrate use of the authenticator. Operators should help users test the authenticator during enrollment sessions to ensure the authenticator works correctly and users understand its operation.
  + Remote
    - Since remote identity proofing sessions are conducted online, general web usability principles should be followed. For example, design the user interface to walk users through the enrollment process; reduce users’ memory load; make the interface consistent; clearly label sequential steps; make the starting point clear; design to support multiple platforms and device sizes; and make the navigation consistent, easy to find, and easy to follow.
    - At the start of the enrollment session, information on how and where to acquire technical assistance should be clearly communicated to users. This is especially important since there is not an operator present for remote sessions. The previously identified usability considerations for providing technical assistance still apply.
    - Explain clearly to the users who is collecting and who is retaining which information they’re providing. For instance, if a user is going to stay on the CSP site to enter financial information that will be sent to a 3rd party vendor, explain this to users so they understand the path their data will take.

### 9.1.3. Post-Enrollment

Post-enrollment refers to the stage immediately after enrollment but prior to typical usage of an authenticator (for usability considerations for typical authenticator usage and intermittent events, see 800-63-3B). As described above, users should have already been informed at the end of their enrollment session regarding the expected delivery (or pick-up) mechanism by which they will receive their authenticator.

Usability considerations for post-enrollment include:

* CSPs should strive to minimize the amount of time that users wait for their authenticator to arrive. Shorter wait times will allow users to access information systems and services more quickly.
* Users should be informed if they need to go to a physical location to pick up their authenticators. The previously identified usability considerations for appointments and reminders still apply.
* Along with the authenticator, users should be given information relevant to the use and maintenance of the authenticator. For example, instructions for use (especially if there are different requirements for first-time use or initialization), information on authenticator expiration, what to do if the authenticator is lost or stolen.
* Provisions for technical assistance.
  + Information on how and where to acquire technical assistance should be clearly communicated to users. For example, provide users information such as a link to online self-service feature, chat sessions, and a phone number for help desk support. Ideally, sufficient information should be provided to enable users to answer their own authenticator questions without outside intervention.