User Experience Guidelines and Metrics

Title: IDEF Registry: Usability Guidelines and Metrics

- Introduction
  - About the IDEF Registry
  - Who Is this Document For?
  - Baseline Requirements for Usability
  - User Experience and Trust
  - Measuring the User Experience of the ID Ecosystem
- User Research
  - What is User Research?
  - Why Do User Testing?
  - User Research Basics
- User Research Methods
  - Expert Review Methods
    - Cognitive Walkthrough
    - Usability Heuristics
  - User Participant Methods
    - Selecting Participants
    - User Interviews
    - User Surveys
    - Laboratory Observations
    - Remote Testing
    - Field Research and Ethnographic Studies
    - Diary Studies
- Measurements
  - Quantitative Measurements
    - The System Usability Scale (Survey)
    - Sample questions for surveys
  - Qualitative Measurements
- Correcting Usability Problems
  - Severity Ratings
- Ethical Guidelines User Research Studies

Institutional Review Board Requirements

Usability in Identity Systems
Guidance Relevant to IDEF Usable Requirements
Identity Ecosystem Scenarios

Appendix A: Defined Terms
Appendix B: Sample User Research Study
Appendix C: Other Resources

Introduction

The contents of this page are meant to provide both practical examples of usability and guidance that can be adapted by participants of the Identity Ecosystem and systems administrators to fit their specific circumstances. Participants are encouraged to engage an expert with usability and user experience knowledge to help with the assessment. User Experience Metrics should enable measurement of the evolving baseline for participation in the Identity Ecosystem.

The contents of this page are based upon evolving requirements for IDESG participants.

About the IDEF Registry

The IDEF Registry is a publicly-accessible listing service of entities that provide online identity services (“Service Providers”) that have self-assessed and confirmed their conformity to the IDEF Baseline Requirements, as envisioned in the US National Strategy for Trusted Identities in Cyberspace (“NSTIC“). The IDEF Registry helps parties to evaluate the policies and operations of the Service Providers with which they interact, and to compare identity services across multiple Service Providers, to assure that their practices meet their needs for online security, privacy, interoperability and positive user experience.

Who Is this Document For?

This document is intended for parties evaluating the usability of services to be listed in the IDEF Registry. Participants may include providers of digital identity services, providers of web services, users of web services and other organizations who are committed to a higher vision for identity and a safer environment for online transactions, and who are interested in independently assessing their own identity management standards against a common set of criteria found in the Identity Ecosystem Framework (IDEF).

- Product Managers: User research is an investment that can be measured in avoided development costs and improved user performance and satisfaction. User research allows product teams to avoid the extra cost and time of producing a product that may require rework to address usability issues or that may ultimately be abandoned. Usability.gov offers a way to calculate the return on investment (ROI) of user centered design: https://www.usability.gov/what-and-why/benefits-of-ucd.html.
- Sales and Marketing Teams: Consumers expect usable products. Ensuring that your products function well and have a good user experience is a marketing advantage.
- Developers: User research provides developers a framework for a functional end product. Testing user tasks incrementally while a product is in development helps to limit scope and feature creep by focusing on what the user needs are and what can be feasibly developed.
- Legal team: User research can uncover accessibility, privacy and security issues, increasing the odds that any risks can be mitigated.

Baseline Requirements for Usability

Usability is defined as the "extent to which a system, product or service can be used by USERs to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." [ISO/IEC 9241-210]. The IDEF Baseline Requirements for usability includes seven requirements along with supplemental guidance. A link to each requirement is provided below.

USABLE-1. USABILITY PRACTICES
USABLE-2. USABILITY ASSESSMENT
USABLE-3. PLAIN LANGUAGE
USABLE-4. NAVIGATION
USABLE-5. ACCESSIBILITY
USABLE-6. USABILITY FEEDBACK
USABLE-7. USER REQUIREMENTS

These requirements can be summed up as assuring the best user experience via user-centered design practices, user testing of all aspects of the service, communicating via easy to understand and jargon-free language, addressing navigation and accessibility concerns and providing a means for users to give feedback and receive redress. Everyday consumers benefit greatly from these baseline requirements for usability, through a trusted and more enjoyable experience. Service providers benefit from an improved reputation and more trusted users.

User Experience and Trust

A review of research involving online trust conducted by Wang et al discusses characteristics and elements of online trust. The characteristics are similar to offline trust but have some distinctions specific to online environments:

- Trustor and trustee: Typically consumer and merchant, but often user and internet system or content.
- Vulnerability: Due to the complexity of internet transactions, users are uncertain and merchants (or online systems) are unpredictable.
- Produced actions: Whether conducting a transaction or simply browsing, the user must be confident that they have more to gain than to lose. Either way, the merchant or system benefits from an achieved transaction or gains data about a potential transaction.
- Subjective matter: Trust is subjective and varies from user to user depending on their experience and understanding of the system being used.

Elements of online trust are determinants of trust in an online environment. These elements represent beliefs that must exist in order for a user to trust the online system. Understanding these determinants can lead to effective and reliable design principles that enhancing consumer trust. The following elements of online trust are noted in Wang et al.

- Integrity: Belief that the merchant or provider will keep their promises and redress any concerns.
- Ability: Belief that the merchant has the competence to provide quality goods and services.
- Benevolence: Belief that the provider will put customer care above profit.
- Transparency: Belief that information provided on the site, such as product descriptions and privacy policies, are thorough and complete.
- Redress: Belief that the provider will address and repair any concerns the user may have around the way their information is being used.

In a review of research involving online trust, Usability.gov noted design elements that users find representative of a website they can trust. These elements are generally embodied by a user experience that is simple, aesthetically pleasing, believable, accessible and produces few to no errors. Trustmarks and certifications help, as do thorough product and service descriptions, tutorials, representative photographs and graphics and alternate ways to communicate with the site such as chat and instant messaging.

The UK's CESG National Technical Authority for Information Assurance provides additional guidance in "Good Practice Guide: Requirements for Secure Delivery of Online Public Services – Annex A". These trust elements are specifically in regard to public services, but can be referenced in any system in which trusted identities are key:

- Privacy: An online service will not unnecessarily compromise the privacy of actual or potential users, in respect of their personal, financial, or business information.
- Authenticity: Users can be assured that they are interacting with a genuine public service.
- Confidentiality: Sensitive information will only be accessible to those with a legitimate need, and used for a legitimate purpose.

- Integrity: Stored personal information will not be corrupted or changed incorrectly.
- Availability: Critical services will always be available when they are needed.
- Transparency: The user's personal information is held only for the purpose outlined on the site and agreed upon by the user
- Identity: The system will confirm the identity of those with access to information before enacting a transaction. In addition, the strength of the identity measures will be appropriate to the value of the information, and the need for confirming true identity (as opposed to authority) when completing the transaction. Identity compromise by the public service will be admitted and repair properly supported.
- Reliance: It is safe to act upon the displayed service outcomes.
- Payment Safety: Monetary transfers are correctly carried out between the correct parties and do not open individual financial details to exploitation.
- Accountability and Fairness: False accusations of fraud or unwarranted impositions of penalties will not be made and cannot be upheld, and that any dispute will be easily and fairly resolved.
- Inclusivity: Services will not disadvantage those with particular personal circumstances or disabilities.
- Non Discoverability: Search or query access to systems and data will not be accessible to an unauthorised individual or used for unauthorised purposes.

Wang et al cites Hemphill's Fair Information Practice Principles as ways to ensure that the online product or service provider can be trusted. These include having a transparent policy on the disclosure of personal information, options for how a consumer's personal data might be used in other contexts and an ability to access and view personal data, as well as a redress mechanism for when something goes wrong. These are key components of the IDEF requirements.

Trust elements can be translated into user heuristics, as discussed in Sundar et al (2016). They found that users applied six heuristics or cues in determining whether to submit personal data to a website. These included:

- Authority: Brand name, organization or trustmark increases users' disclosure of personal data.
- Transparency: Users were more likely to disclose personal data when the application explicitly displayed details of data management practices.
- Ephemerality: When it appears that data is only kept for a short while, such as in Snapchat images, users are more likely to disclose personal data.
- Fuzzy Boundary: When data appears to be transferred to a third party, users were less likely to disclose personal data.
- Publicness: Users were less likely to disclose personal data if the data was requested via a public computer station or via public WiFi network.
- Mobility: Users were less likely to disclose personal data while using mobile devices or if the data would be saved to the mobile device.

These heuristics can be used in expert or observational testing. In expert testing, the expert can ask if there is a visible trustmark or brand name, if data management practices are outlined in detail and easy to find, whether data is stored briefly or via a third party. For mobile situations, users can be tested to identify whether they are aware when they have established a secure connection and whether they trust the network with which they are connecting to the product.

Measuring the User Experience of the ID Ecosystem

This document outlines some methodologies for measuring user experience. These measurements of overall usability indicate the level of compliance with the Usable requirements of the ID Ecosystem Framework. Quantitative metrics obtained via user surveys, user log analysis and A/B Testing provide a success measure of the end user's experience. Qualitative research from interviews and observations provide an understanding of why users are making choices and what they understand about a system and the choices presented. Heuristics evaluations and expert walkthroughs provide a better understanding of system errors and interfaces.

User Research

What is User Research?

According to usability.gov (https://www.usability.gov/what-and-why/user-research.html), “user research focuses on understanding user behaviors, needs, and motivations through observation techniques, task analysis, and other feedback methodologies.” Wikipedia further defines user experience evaluation in terms of a system:

> *"**User experience (UX) evaluation** or **User experience assessment (UXA)** -- which refer to a collection of methods, skills and tools utilized to uncover how a person perceives a system (product, service, non-commercial item, or a combination of them) before, during and after interacting with it. It is non-trivial to assess user experience since user experience is subjective, context-dependent and dynamic over time."*
>
> -- “User Experience Evaluation,” Wikipedia. [1]

We have outlined below a number of user research techniques that you can use to evaluate your products and services against the IDEF Baseline Requirements for usability.

Why Do User Testing?

USABLE-2, Usability Assessment, requires that “Entities MUST assess the usability of the communications, interfaces, policies, data transactions, and end-to-end processes they conduct in digital identity management functions.” One of the four Guiding Principles of the National Strategy for Trusted Identities in Cyberspace is that identity solutions will be convenient and easy to use. In order to be effective, identity solutions must be intuitive, easy-to-use, and enabled by technology that requires minimal user training. Identity solutions must also bridge the ‘digital divide’; they must be available to all individuals, and they must be accessible to the disadvantaged and disabled.

User research and testing ensures that products and services are easy to use by a broad audience, regardless of the user’s abilities or constraints faced while attempting to perform tasks. If user research practices are followed throughout the design and testing of a product or service, it can also reduce design errors, and improve the user experience and marketability of the end product.

User Research Basics

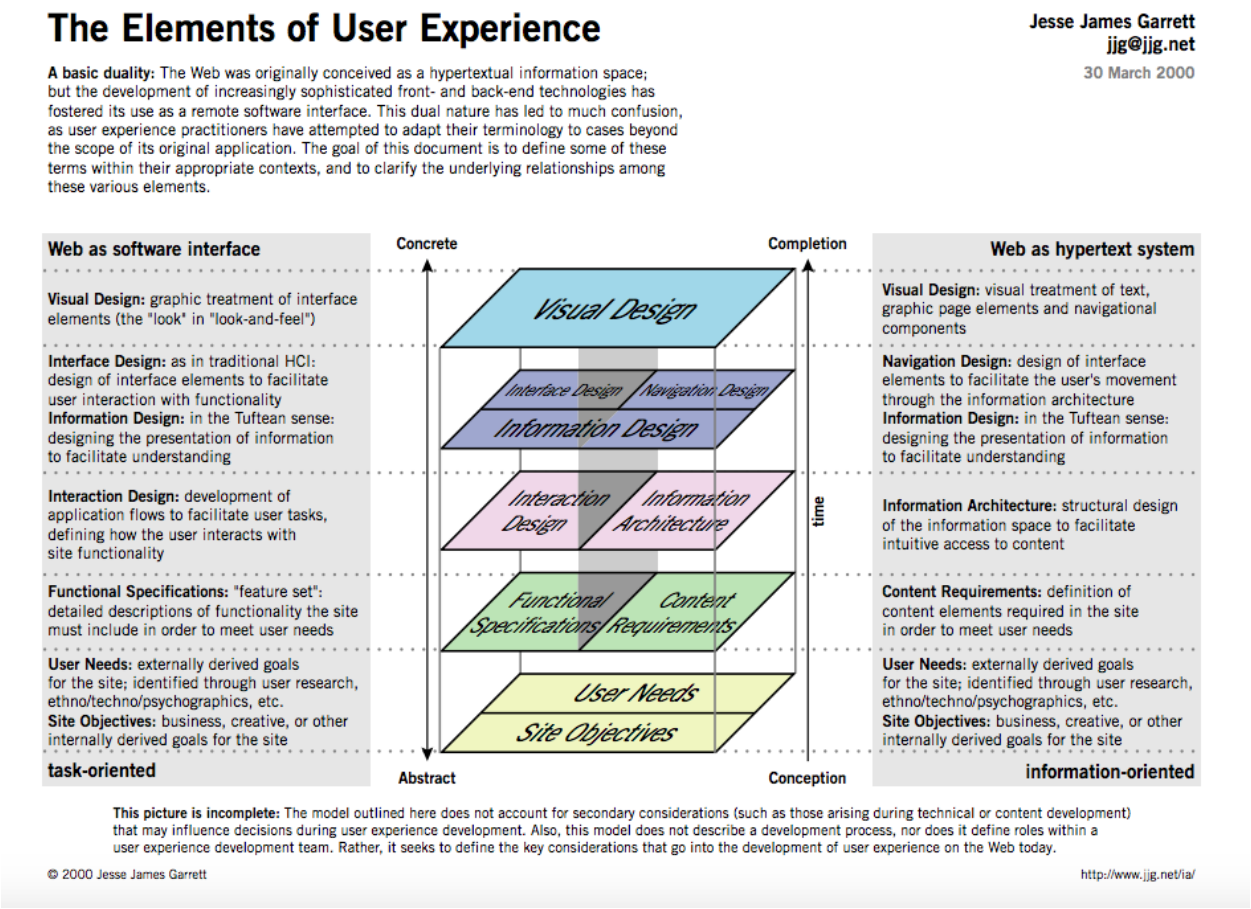
Two widely regarded texts outlining the basics of a good user experience include Peter Morville’s Honeycomb diagram and Jesse James Garrett’s *Elements of User Experience*.

Peter Morville’s usability honeycomb outlines seven facets of the user experience. These facets can be considered goals for the product or service which contribute to the central goal of creating value:

http://semanticstudios.com/wp-content/uploads/2004/06/honeycomb.jpg

- Useful: Innovative and serves a need.
- Usable: Easy to use.
- Desirable: Expresses the value of image, identity, brand, and other elements of emotional design. Evokes delight or appreciation.
- Findable: Easy for users to navigate and to find what they need, as well as easy to find the product or service from search engines and other directory services.
- Accessible: Provides methods and assistive technologies for users with disabilities or constraints (hands free, driving, etc).
- Credible: Has sufficient authority, accuracy, objectivity, currency, and coverage to be considered reliable and believable.
- Valuable: Advances the mission or contributes to the bottom line and improves customer satisfaction.

Jesse James Garrett published Elements of User Experience, which contains a diagram outlining the aspects of a good user experience, beginning at the bottom with abstract concepts and building up to a concrete, complete product or experience. Each aspect of the user experience, from the visual design and interface down to the information architecture and functional specifications based on user needs and stakeholder objectives is a potential area for testing.

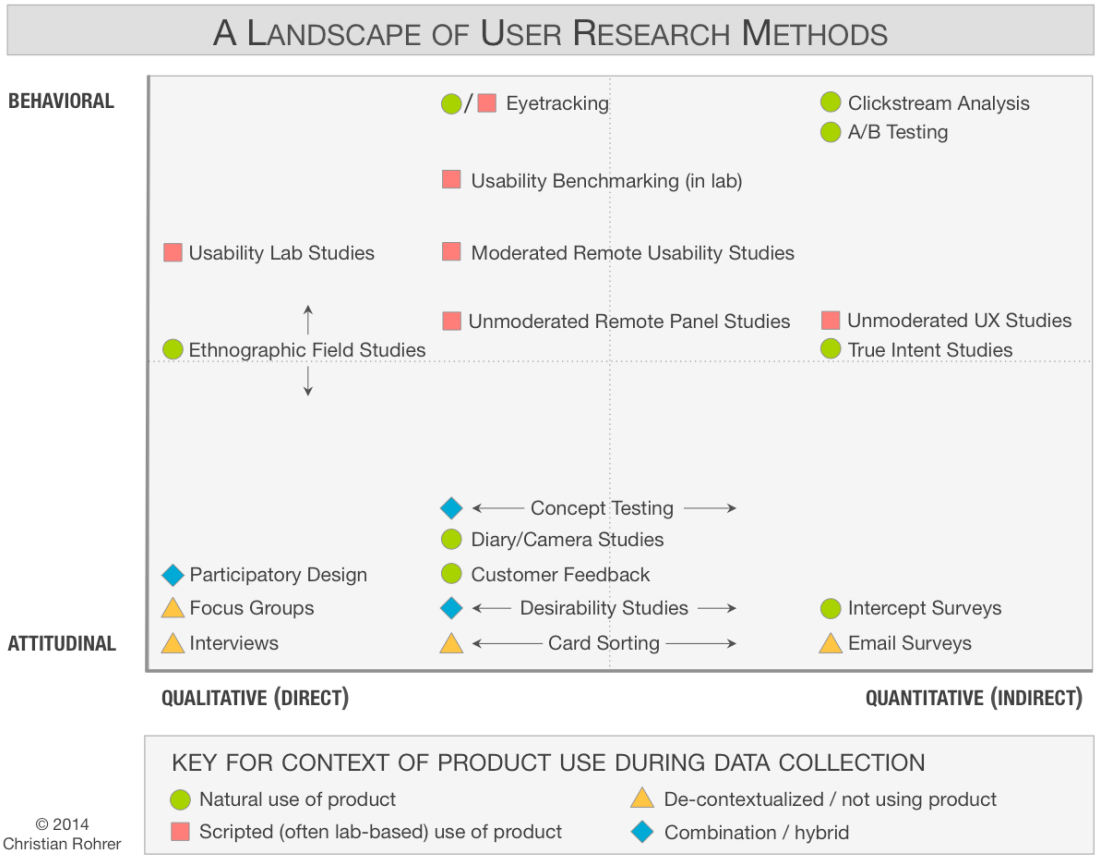


http://uxdesign.com/assets/Elements-of-User-Experience.pdf

User testing starts with the development of a concept around where user needs align with stakeholder goals. Is the product or service you are developing solving a problem or need the user faces? A user researcher begins by interviewing potential users as well as business stakeholders….

User Research Methods

User research methods can be divided into behavioral methods versus attitudinal methods and each of these can further be divided into qualitative and quantitative methods (See NNGroup diagram below). Behavioral methods can take place as scripted laboratory observations or observation of natural use in ordinary environments. Attitudinal methods may be unscripted, and may involve non-contextual studies, e.g., not using the product, conceptual studies or needs assessment surveys.



Source: Rohrer, C. (October 12, 2014). When to use which usability method. (Web.) NNGroup.

Qualitative methods tend to involve observation and open-ended questions, while quantitative methods offer measurable data, such as number and frequency of clicks, task timing and eye tracking methods, or survey responses graded on a scale. In When to use which Usability Method, NNGroup notes that "...qualitative methods are much better suited for answering questions about why or how to fix a problem, whereas quantitative methods do a much better job answering how many and how much types of questions."

In addition, some methods do not require test users at all. Some usability problems can be identified by an expert review. Below we outline a number of user research methods you may employ and we discuss which methods might be optimal for specific identity related tasks.

Expert Review Methods

Expert review methods are useful while developing a product or module before bringing in users to evaluate. An expert is a person who has experience and knowledge of usability research methods. Typically, an expert review method will require evaluation by 3 to 5 usability experts, though different kinds of tests may require different numbers of testers to reveal most potential

problems. According to the GSA's Research-Based Web Design & Usability Guidelines, expert review methods, such as cognitive walkthrough and heuristic evaluation, have a relatively high rate of false positive results and are generally best used to determine which processes should be tested with actual users. Subsequent testing with real users can reinforce whether a problem uncovered by the experts is a real problem that should be solved.

Cognitive Walkthrough

During the cognitive walkthrough, the evaluators discuss each step within an action sequence, telling a story of how a user might approach each step, the ease of use and understanding of each step and where they may make a wrong move or fail to complete a task. Components of the story include the following criteria, described by Wharton et al (1994):

- Will the user try to achieve the right effect?
- Will the user notice that the correct action is available?
- Will the user associate the correct action with the effect they are trying to achieve?
- If the correct action is performed, will the user see that progress is being made toward solution of their task?

Success with all four criteria indicates a success for the task defined in the cognitive walkthrough. Failure to satisfy two or more of these four criteria, unless a single criteria failure is severe, indicates a failure that should be corrected in the interface design. The severity of the failure depends on a number of factors, including how many of the criteria failed and whether the difficulties associated with the task prevent the user from completing the entire sequence. For example, if a user takes a long time to notice that the correct action is available or that it is associated with the effect they want to achieve, but eventually completes the intended action, this would be less severe than if the correct action is never found or if the user fails to recover from an incorrect action.

Experts may ask the following questions to evaluate these criteria. Note that not all of these questions may be pertinent to the system being evaluated:

Will the user try to achieve the right effect? ● Do the instructions or other copy clearly indicate what the system will do? ● Are there actionable elements, such as links, icons and buttons, on the page? ● Do the actionable elements clearly represent the action they will initiate? ● Are there elements that may distract the user from the task? ● Is help available for the task?
Will the user notice that the correct action is available?

● Are actionable elements, such as icons and buttons, clearly visible? ● Are form fields visible? Do they appear to be editable? ● Are there elements that distract the user from noticing the correct action?
Will the user associate the correct action with the effect they are trying to achieve? ● Are icons and button labels representative of the action they perform? ● Are actionable elements, such as buttons and links, located near the instructions or icons with which they are associated? ● Are incorrect or unavailable actions visible, and if so are they grayed out, annotated or otherwise altered to indicate they are not available?
If the correct action is performed, will the user see that progress is being made toward solution of their task? ● When the action is performed, does the system change? For example, does the copy include confirmation that an action has been performed? Does it go on to the next step in the process? ● Is there a progress bar or a next/back buttons visible to indicate the user's position within the process?

Usability Heuristics

In a heuristic evaluation, the evaluators review an application against a set of usability principles. (Nielsen, Jakob. 1995). A heuristic evaluation is a usability inspection method in which a team of peers, usually designers, evaluate an interface against a specific set of heuristics or principles. These principles are more "rules of thumb" than specific usability guidelines, but are effective in spotting issues that might be in conflict with website usability.

The evaluation is conducted individually by a group of three to five people, then results are presented to the team leader who compiles a report of the findings. Nielsen recommends three to five as an optimum number of evaluators to ensure that the majority of usability problems will be located.

In the context of website and application UX, this would mean the user interface of the identity system, but it might also include any cross channel interaction and "experience" such as brand, trustmark, paper correspondence (such as the acknowledgements we sometime get in the mail about online transactions), advertisement/solicitations, etc. and how well it integrates with provider and other external/3rd party systems.

Following are Jakob Nielsen's 10 general principles for interaction design:

1. Visibility of system status: The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
2. Match between system and the real world: The system should speak the user's language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.
3. User control and freedom: Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo.
4. Consistency and standard: Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
5. Error prevention: Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
6. Recognition rather than recall: Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
7. Flexibility and efficiency of use: Accelerators -- unseen by the novice user -- may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.
8. Aesthetic and minimalist design: Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
9. Help users recognize, diagnose, and recover from errors: Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
10. Help and documentation: Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

http://www.nngroup.com/articles/ten-usability-heuristics/

Experts may evaluate these features by asking the following questions about a hypothetical user. Variations of these questions may also be used in user surveys (see below section on Laboratory Observations for details):

Visibility of system status

- At each point in the system, the user is aware of their options and what they can do next.
- Users can tell when the system is processing an action.
- Users can tell how long a process will take and when it is completed.

Relevant to identity services:

- Users know what data or other input is being requested and what will happen to it.
- Users can see how and whether private information is kept private.
- Users can tell if they are logged into their account.
- Users can see an indication that the session is secure.

Match between system and the real world

- Users can understand the language of the system.
- Concepts are presented in terms that are familiar.
- Terms or phrases are not too technical or jargony.
- The way that actions and information is presented is what users expect it would be.
- The process and actions follow a natural, logical flow.

Relevant to identity services:

- Icons and graphics match real world concepts. Examples:
    - Lock = Secure
    - Open Eye = Viewable
    - Closed Eye = Private
    - Green = Safe
    - Red = Danger
- Terms for passwords, passcodes, tokens, encryption keys, handshakes, etc. are sufficiently understood by the typical user or defined if the user's experience with the concept is minimal.
- Processes that require navigating to an external party asset, such as 2-factor or third party authentication, sufficiently address why this is happening.
- The flow for logging into a service or creating an account follows an expected order.

User control and freedom

- Users understand that they can stop the process at any time.
- Users can return to where they left off.

- Users can return to the previous state and make changes.

Relevant to identity services:

- Users can leave the system knowing that their data will be saved or deleted according to their expressed wishes.
- Accounts or other identity information may be deleted upon request.
- Where applicable, “right to be forgotten” requests will be honored.

Consistency and standards

- Users understand that the words and language used in the website have the same meaning throughout the website.
- Actions such as swipes, sliders, link clicks, checkboxes, buttons, refresh, minimize, close, etc. behave as expected within the platform being used (e.g. iOS, Android, Chrome, etc).

Relevant to identity services:

- Terms relative to login, passwords, accounts registration, security, privacy, interoperability, certification, authentication, authorization and transaction intermediation are defined and used consistently with the system and across related systems.
- Processes that reflect or are certified under a given standard for identity services behave as described by that standard.

Error prevention

- Users make very few or no mistakes.
- The system offers instructions or explanations when users enter information in a form.
- The system asks the user to confirm an action, such as submitting data.

Relevant to identity services:

- Error prevention is especially important for identity services, as an incorrectly entered or saved ID, password or other detail can make it impossible for a user to access services and can cause problems with interoperability with other services that share access or identity information.
- The system should offer help and confirmation of entered details. It should clearly demonstrate correct input, such as password character count and character type

requirements and proper formatting for items like phone numbers and dates. It should note mismatches with third party systems, if detected.

Recognition rather than recall

- Everything users need to make a decision about their next action is available to them.
- Users don't feel lost when they go from one page to another.
- Users know what they are supposed to do next.
- The website uses images or options that help users recognize what they need to do next.
- Users can find help documentation when they need it.
- Help is available that is relevant to the item the user is working on.

Relevant to identity services:

- Follow expected patterns for system processes, like data entry and account setup. For example, show a path for completion, such as which step the user is at in the process, which steps came before and what is next.
- Provide help documentation and relevant and appropriately placed tooltips or guidance copy when and where a user needs them.
- Use recognizable images or icons and use them consistently, when representing steps and actions in a process, e.g., green locks, gold keys and danger signs. Keep your audience in mind. Older users may recognize the floppy disk icon to mean "Save" but the youngest users may not. Newer interfaces sometimes use an arrow pointing down at a box to mean "Save" instead of a floppy disk, but not all users understand this iconography. Test icons and graphics for meaning among the target user groups.

Flexibility and efficiency of use

- Users are not given too much or too little information to complete the task.
- Users can expand or collapse help text if they want.
- Users can copy or repeat frequent actions easily.

Relevant to identity services:

- Copy should be concise and clear and directed to the experience and reading level of the user. Some concepts covered in the identity ecosystem may require more education or experience to understand than others. Some identity services may be

targeted to a sophisticated user, such as a system administrator, while others may be targeted to lay users or children.

Aesthetic and minimalist design

- Users are not given too much or too little information to complete the task.
- Users like the way the system looks.
- Users do not feel overwhelmed by the information presented.
- The presentation is not confusing.

Relevant to identity services:

- As in the last two heuristics, copy and design should be clean and clear.
- Do not introduce more content than needed. If an identity concept or process is complex, break it down into smaller bits of information or more steps.

Help users recognize, diagnose, and recover from errors

- When there is a problem, the system shows an error message and suggests an action.
- Users can understand the error message and know what they need to do to recover.
- If the user makes a mistake or find an error, it is clear that it is a system error, not a user error.

Relevant to identity services:

- Since identity is a sensitive and personal topic, language used in communicating errors should be respectful and mitigate any fear or upset a user may experience.
- Since identity services process sensitive information, messaging around errors should indicate the level of severity of the error and instructions for correcting the error or seeking remediation.
- The system should include a process for remediating incorrectly entered or saved data, especially since a compromised identity process could have major financial or legal implications (e.g., inability to access an account or identify a legal entity).

Help and documentation

- Users understand the instructions and documentation.

- Users can search for information about a topic or action they don't understand.
- Information or help is available for the action the user is working on.
- Users can find step by steps instructions for what they need to do to complete a task.
- The instructions and help documentation is not too long or overwhelming to read.

Relevant to identity services:

- All concepts relative to the identity service are defined and documented in clear, understandable language.
- Help is presented at points where users can get guidance or feedback on their actions.

User Log Studies

Certain types of user activity can be monitored and evaluated by studying usage logs, such as those provided by your hosting service or Google Analytics. Usage logs provide a wealth of information on user behavior. Usage logs can provide detailed information about user activity on an aggregate and can typically be filtered to specific study populations. Since monitoring user activity of individual identity service users may involve access to sensitive information or activity, it is important to insure that the proposed study follows the published terms of use, privacy policy and adheres to policy and relevant laws around such monitoring activity. In some cases explicit permission from the user may be required.

Clickstream Study

A clickstream study shows the path a user takes while interacting with a system. User logs, such as those provided by Google Analytics, can provide data on user paths taken while using the product. This type of study doesn't require explicit participation by users as it tracks data already collected by the server. Clickstream studies can show where users are entering and leaving the system, which pages or activities of the system are receiving the most traffic and sometimes where they go when they leave the system.

Some user research software can also measure where on an interface a user is clicking, swiping or otherwise interacting with a system. These studies can be used to create a heatmap or diagram of which interface features a user is interacting with over time and can be used to study the placement of icons, buttons, navigation and other elements.

Source: KISSmetrics (should replace with a user flow diagram from IDESG Google Analytics)

A/B Study

An A/B Study can be used to evaluate different interface options against one another in a live user test. The system randomly presents a user with one of two interfaces and monitors the user's activity. The testers can compare usage of one group who used Version A versus the group who used Version B. Did one group have a higher completion rate? Was one group faster?

Typically, the user is not aware that there are two versions; however, if the user is a current user they may notice a difference in the way the new interface is presented. The code that determines which interface to present can also assign values to the user indicating if they are a new or current users, based on profile data and whether they are logged in or not logged in, etc. Learning a new interface, even one with minor changes can affect user performance, and in itself might be a good thing to test.

True-Intent Study

Site visitors are randomly asked what their goal or intention is upon entering the site. Visitors may decline participation or agree to continue with the understanding that a process will be triggered that measures their subsequent behavior during the current session, and whether they were successful in achieving their identified goal upon exiting the site.

User Participant Methods

In user participant methods, all tests are conducted using participants representing a user population for the task or product being tested. To provide a comfortable testing environment, it

is important to refer to participants as “participants” rather than users or subjects. Participants should also understand that it is the product or task, , not the participant, that is being tested. For this reason, it is helpful to refer to your sessions as a research study rather than a test.

Selecting Participants

Identity ecosystem users may range from very experienced identity product users and developers to general internet users. Tasks that require a high level of expertise, for example configuring an authentication service requires more knowledge than a simple website login. The goals of the user test also determines the type and number of users to recruit for testing.

Depending on the task or the type of test, participants may be recruited from many sources. Tasks that require a higher level of expertise may be tested by participants culled from existing user or client lists and can also be members of your own organization. Many marketing and user experience research companies offer user testing recruitment which can be aligned with particular demographic or interest groups. Email surveys or user intercept surveys (where a request for survey participation is randomly generated while using a product) are ways to recruit users with a qualified interest in your product. Further, screening surveys can be used to identify suitable individuals among a preselected group of participants.

Additional guidance on recruiting and selecting participants are noted within the descriptions of several types of user tests below.

User Interviews

In a user interview, a facilitator presents a current or prospective user with a series of questions about an application or a set of tasks. The facilitator presents the questions in a neutral manner so as to elicit honest and unbiased responses, which are recorded for evaluation by the product team.

User interviews are often used in testing methodologies, such as phone surveys, focus groups and remote or in-person testing. Open ended interviews provide qualitative data and are great for exploring attitudes about a product or service and assessing user needs. Interviews may also use closed ended survey questions to provide quantifiable feedback.

User Surveys

A survey is a research tool for collecting information from current and prospective users of a product or service. Attitude and preference surveys can collect information about products and features that a prospective user would like. Customer feedback and satisfaction surveys can provide insight on what a customer likes or dislikes about a product they already use. Demographic information and other data, such as experience with a particular kind of product, can be used to screen participants for user tests.

Surveys should be designed with an introductory paragraph explaining what the objective of the survey is and why the user was selected to participate, or why they are being asked to fill it out. Surveys are typically anonymous and should include a statement that responses will be kept private. If you would like to invite respondents to participate in future studies, include a way to opt in. Either ask the respondent to enter contact information in the form or direct them to a signup form. If you would like to be able to follow up with specific users for further testing, include a question for their contact information, but be sure to state it will be kept private. A thank you message, before and after the survey is completed, is also helpful and appreciated.

Surveys can be delivered remotely or in person and can be paper or electronically based. Language should be clear and written at the reading or experience level of the intended participant. Each participant in a survey generally answers the same, pre-written set of questions; however, some surveys can be configured to ask additional questions based on answers to certain questions via “skip logic.” For example, “If the answer is Yes, skip to question 5.” Skip logic is a built-in feature in many electronic survey applications.

The format of a survey question depends on what you want to know about the user. Survey questions can be formatted as Yes/No, multiple choice, checkbox or fill in the blank questions. They may use scales, sorting or sliders to assign a value to a choice. Is the answer absolute (“what is your age?”) or relative (“on a scale from 1 to 10, how would you rate the quality of the overall customer experience?”)

If you use a scale, be sure to use a balanced scale that doesn't confuse the respondents or potentially skew the results.

Below is an example of a balanced scale:

1. Agree Strongly
2. Agree Somewhat
3. Neutral
4. Disagree Somewhat
5. Disagree Strongly

Below is an example of a skewed scale:

1. Agree Strongly
2. Agree Somewhat
3. Disagree
4. Disagree Somewhat
5. Disagree Strongly

Avoid question language that might influence the answer. For example, try to balance positively and negatively worded questions or keep the question neutral and have the respondent rate the

issue on a scale from bad to good. You may also wish to include “Don't know”or “Not applicable” answers.

Bad:

> How excellent was your service today?
>
> Bad 1 2 3 4 5 6 7 8 9 10 Good

Good:

> Please rate our customer service.
>
> Bad 1 2 3 4 5 6 7 8 9 10 Good

Surveys are also valuable tools for measuring a user’s experience before, during and after task-based tests. Appendix B links to a series of survey questionnaires that can be used before and after user tasks and tests. These questionnaires are described in more detail in the Laboratory Observations section below.

Surveys can be incorporated into many
True-Intent Study: Site visitors are randomly asked what their goal or intention is upon entering the site. Visitors may decline participation or agree to continue with the understanding that a process will be triggered that measures their subsequent behavior during the current session, and whether they were successful in achieving their goal upon exiting the site. All identifying data will be removed from the study. A follow up survey can ask questions about their experience with the handling of personal data and privacy.

Laboratory Observations

Laboratory observations are fully moderated and are conducted in a controlled environment with minimal distractions. An observer may be in the room with the user or the user may perform tasks alone with one or more observers in an adjacent room, behind one way glass or observing via video monitor or live screen capture. The session may be recorded via video camera and/or screen capture. Additional technology such as eye tracking technology, motion sensors, etc may be employed.

Carol Barnum recommends using a Thinking Aloud protocol, in which test participants complete a set of user tasks, while speaking audibly about what they are doing and experiencing. (Barnum, Carol M. (2011), *Usability Testing Essentials*. Burlington, MA: Morgan Kaufmann.) Having participants talk aloud while completing tasks allows the observers to record additional

insights about user tasks that might not have been noted if the participant were to perform tasks silently.

Speaking aloud can seem awkward to a participant who is unfamiliar with this testing method, so observers should remind them to describe their actions and encourage them to be honest in any critique. To make the participant more comfortable, observers should ensure them that it is the system, not the user that is being tested and that there are no mistakes or wrong answers on any task or survey question.

In a moderated Thinking Aloud test, the participant performs tasks in a controlled environment, typically a usability lab, while a test moderator observes. The test environment should mimic the environment in which the product is being used. This may include a desk, table and chairs or a couch or other informal seating and the device (desktop or laptop computer, tablet or mobile phone, etc.) on which the user may typically perform tasks being tested. Windows and doors should be closed and phones or other unnecessary devices should be turned off to minimize distractions. Any screen capture software or video equipment used to record the participant's activity, facial expressions and commentary should be set up and tested before inviting the participant to the lab.

Evaluators should prescreen participants for any specific knowledge, experience or demographic group to be studied. For example, test participants may need to have some familiarity with using the device or type of application being tested. A pre-screening questionnaire can rule out participants who do not meet test criteria. See ethical guidelines and sample consent forms below.

A typical setup for a laboratory observation has the test participant sitting in front of the computer, while a moderator sits next to them, recording observations in a notebook or tablet. The moderator follows a script, which is included in Appendix B. Task descriptions are prepared ahead of time and included in the script.

The participant completes a pre-test questionnaire (Appendix B) to capture information about their experience with the research tasks. This questionnaire is used to obtain information about the participant that may be useful to know in analyzing their test session.

After each task is completed, participants complete a Post-Task Questionnaire, reproduced in Appendix B. The Post-Task Questionnaire includes a small number of questions about the task completed, with answers rated on a scale from 1) Strongly Disagree to 7) Strongly Agree.

At the completion of both tasks, the participant is presented with a Post-Test Questionnaire (Appendix B). This questionnaire is modified from the CSUQ , Computer System Usability Questionnaire, developed by James Lewis at IBM. (Barnum, Carol M. (2011), Usability Testing Essentials. Burlington, MA: Morgan Kaufmann, an imprint of Elsevier, Inc. p. 181.) It is a

Likert-type questionnaire with 16 questions on a 7-point scale. This questionnaire helps to elicit feedback from the participant on their total experience with the test.

Remote Testing

Remote testing is possible due to the availability of conferencing and screen sharing software, survey software and various testing tools such as remote card sorting tools and online prototyping software. This is an advantage if test participants are not located in the same area as the observer or if time and financial constraints do not allow travel to the testing environment. A disadvantage is a lack of a controlled testing environment, limited observation and unavailability of technologies such as eye tracking. (The following services are for informational purposes only and do not represent a specific requirement.)

Conferencing tool Examples:

- Skype
- GoToMeeting
- WebEx
- JoinMe
- ReadyTalk
- Google Hangouts

Document Sharing Tools examples:

- Google Drive
- Microsoft OneDrive
- Dropbox

Remote Video and Screen Capture examples:

- Clearleft Silverback

Testing Suite examples:

- Optimal Workshop
- Loop11

Etc.

Field Research and Ethnographic Studies

Field research occurs outside the laboratory setting and may include man-in-the-street interviews, surveys, observations and home or office visits. The advantage of field research is that participants may feel more comfortable and less guarded in an environment they know well. Feedback may be more spontaneous. Also, aspects of the environment in which the participants live their daily lives can provide insights into user behavior that are not apparent in a controlled, distraction-free laboratory.

An ethnographic study is an observation of users in their natural environment. This could be an office worker at their desk, a person in their home office or living room, a commuter on a train, etc. In an ethnographic study, an observer will have the participant perform tests in the field and record observations in a notebook or test form. Depending on the study, the participant may be asked to complete pre- and post-task and pre- and post-test questionnaires and any specific tasks to be completed, as in a laboratory test.

The observation may also be open ended. You may wish to ask the participant to demonstrate how they usually go about the kind of task your product or service is meant to support. It may involve observing a participant as they use a competitor's product or service. In any case, it is a great way to observe the kinds of distractions or constraints a user may have in their natural environment.

Man-in-the-street or "guerilla" style interviews are ideal for testing brand recognition, feature awareness or needs, reactions to a new product/service, or "how would you use this" and "what do you think of" types of questions. They also may capture a population of users and of-the-moment feedback that could be missed in a carefully curated laboratory study. Be sure to collect demographic information or any details that assist with comparing to your target user or controlled study participants to ensure you are addressing relevant concerns.

Diary Studies

A diary study is an unmoderated, user research method in which participants are asked to log their activities over a period of time. According to Reiman (Rieman, John. 1993. "The Diary Study: A Workplace-Oriented Research Tool to Guide Laboratory Efforts"), the most powerful, quantitative data from a diary study is the amount of time spent on a particular activity. A diary study is useful for getting feedback about how long users stay on the site, which features they are using and how it might compare to other similar products.

The length of time for conducting a diary study depends on the task or function being evaluated. Some tests may take place over a period of days, weeks or months. Since a diary study is a remote user test it is recommended to deliver periodic reminders to participants via email or phone. The frequency of reminders depends on the length of the data collection period.

After the data collection period is completed, evaluators analyze the data and prepare findings and recommendations for the product team to use in designing the product or correcting user issues.

An example of a diary study in identity services might be to ask a group of participants to track their login behavior over a period of time. Data collected could include the following:

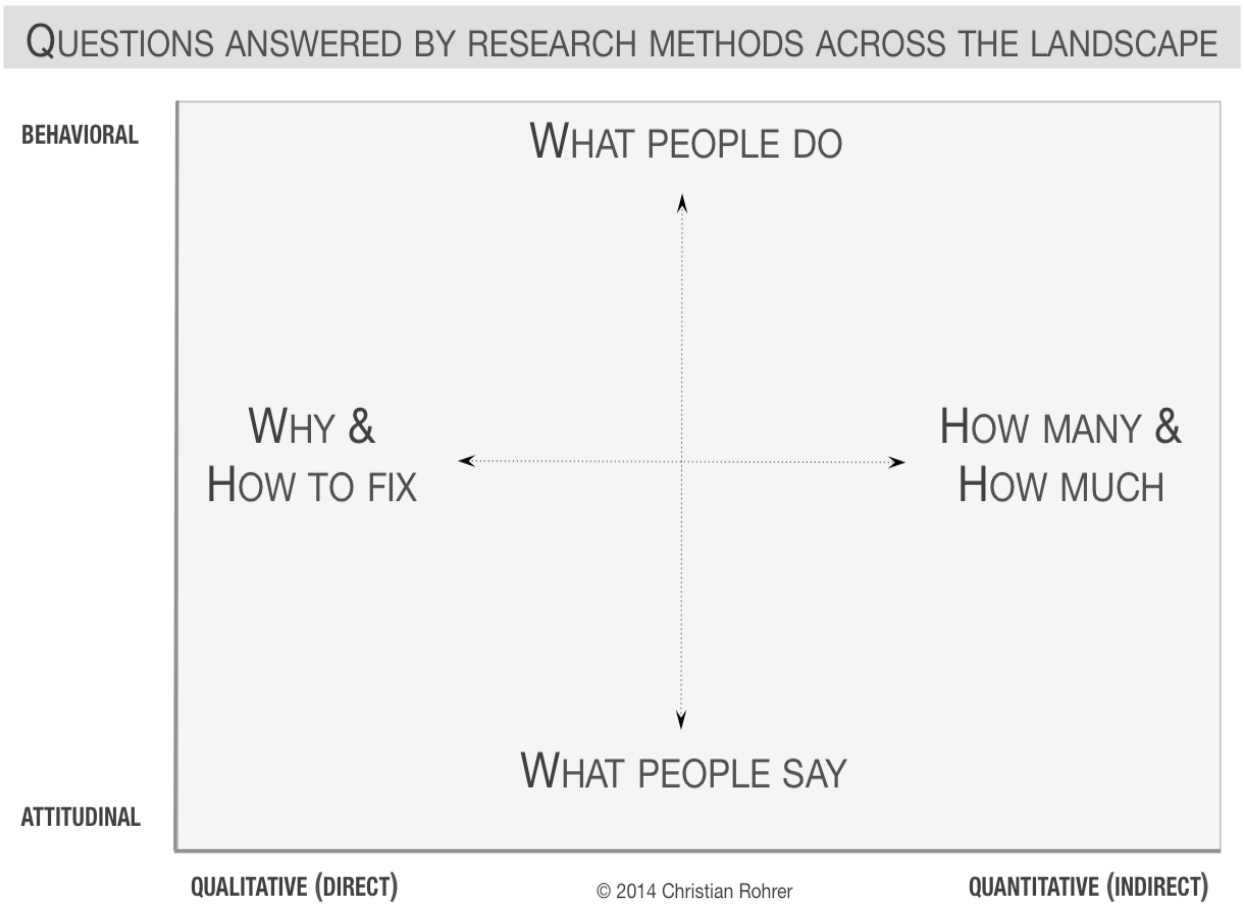
- URL of the sites they use
- Type of site

- Whether or not a login was required
- Whether or not they needed to create a new login account
- Whether the login process used a simple username password combination, 2-factor authentication or federated login
- Length of time or number of steps to complete login
- Whether or not a transaction was involved
- Relative strength of the password used
- Relative strength of the password required
- Whether the used a password reminder

Some other things to check for may include how often the user logs into a particular service, whether or not they set their browser to automatically log into a site, whether and how often they change passwords, if they are prompted to change a password, etc. Generally for a diary study, tracked activities should be those where the user is actively performing a task they can report on rather than a back-end processes that they would not see or aren't aware of.

Measuring the User Experience

According to NNGroup, qualitative methods help to answer questions about why or how to fix a problem, and quantitative methods are better for answering “how many” and “how much.” Qualitative studies provide data on user attitudes and behaviors through direct observation, while quantitative studies produce data with specific numerical values. Having such numbers helps prioritize resources, for example to focus on issues with the biggest impact. The following chart illustrates how the first two dimensions affect the types of questions that can be asked:



In the research methods diagram presented in the User Research Methods section above, we noted a number of methods and where they fall on the qualitative to quantitative scale. Quantitative methods often involve analyzing user activity during the use of the product. These methods include clickstream analysis and A/B Testing, which can provide measurements of recorded, completed tasks via user logs. They may also involve surveys and voluntary user monitoring, as in unmoderated UX studies and True Intent Studies. Eyetracking studies, card sorting and customer feedback or diary studies also produce quantitative and qualitative measurements. Affinity diagramming, focus groups, open ended interviews and other observation-based studies may provide more qualitative than quantitative information.

Quantitative Measurements

Quantitative measurements may include a measurement of the number and frequency of clicks, task timing and eye tracking methods—in other words things that are countable. These queries may include reviews of system logs, which can provide data as to whether and how often a particular action was completed, as well as direct user surveys. It is important to understand that quantitative measurements do not necessarily lead to understanding why a user chose to do one thing versus another. This sort of inquiry only allows for understanding what and possibly

how things are happening in a system and can suggest more qualitative findings, such as user satisfaction, and whether a certain category of prospective user will use or abandon the service.

The following is a sampling of questions one might ask users about an identity service being tested:

1. Can the user accomplish the task set out to accomplish?
2. Is the Trustmark discoverable and self-describing?
3. Does the user feel safer as a result of the appearance of the Trustmark?
4. Does the user feel that the site is safe overall?
5. Does the user understand the necessity for a strong identity for their providers?
6. Does the user know whether the identity of the provider is strongly bound to a real-world entity?

A qualitative measurement for certain questions may be found in system logs. For example, how many users successfully created an account versus those who abandoned the process at some point? Questions such as whether a trustmark is discoverable can also be measured in user testing where the presented task is “find the trustmark”. These questions can be asked in a survey after users have had an opportunity to spend time using the system. The answers can also be interpreted by an observer noting whether a task was completed or not. The survey could be conducted in a formal laboratory test series, or in intercept surveys of users currently using the system and email surveys sent to registered or other known users.

The goal might be 90% affirmative for most of the above usability questions, with a minimum acceptable score of perhaps 60%. This goal may vary by product or service. Questions directly related to trust might be set at a higher value. For example, does the user feel safer as a result of the appearance of a trustmark? Since safety is a major requirement of a trustmark, the goal might be even higher: 99%, with a minimum 80% of those answering in the affirmative. In this case even 80% may seem a bit low. It is also possible to measure questions such as these on a scale, such as the System Usability Scale noted below. The IDESG is not currently setting thresholds for these figures, however.

The System Usability Scale (Survey)

The System Usability Scale (SUS) (Brooke, 1986) is a suggested, 10 item questionnaire where the typical 5-response option might be used to ask for feedback. For example, users could be asked to provide answers on a scale from 1-5, where 1 represents "success" or "good" experience and 5 represents "failure" or a "poor" experience, with specific descriptions of these

success and failure marks tuned to the system and questions asked. Include similar questions phrased in both positive and negative terms to help prevent biased responses. For example:

- The instructions were easy to understand.
- The instructions were too complex.
- I was able to complete all of the tasks in the allotted time.
- I did not have enough time to complete all the tasks.

It may be helpful to include a comment box on all surveys so that if users discover a problem not addressed in the test, they will have an opportunity to share their perspective. Any open ended answers should be codified and categorized, and surveys should be adjusted to incorporate the user perspective as much as possible. Generally, the less specific questions are, the more likely the user will submit feedback about problems the investigators may have missed. The IDESG welcomes feedback to help improve identity services throughout the overall identity ecosystem.

Sample questions for surveys

1. I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

Qualitative Measurements

Not all user feedback is directly quantifiable. Open ended comments such as, “I don't understand these instructions,” “I feel stupid when I can't get to the next page,” or “This graphic is distracting (ugly, confusing, etc),” fall into the category of qualitative feedback. Measuring qualitative input allows the investigators to rate and categorize non-quantitative user input and prioritize solutions. Collected verbatim responses used for site improvement can also be mined for sentiment and measured quantitatively. For example, how often did commenters use the word “liked” or “frustrating”? How many comments were positive, negative or neutral. Framing problems into categories and measuring frequency at which problems in each category appears can provide a useful measurement for addressing and prioritizing observed issues.

As noted above, qualitative studies provide data on user attitudes and behaviors through direct observation. As such it may require some subjective evaluation to turn a qualitative observation into a useable data point. For example, some feedback may relate to the look and feel of the product or website or to the functionality or interactivity of a process. If a significant number of users complained about the color scheme and the majority have an issue with a specific color or

icon, this is a data point that can be grouped and turned into a measurement (e.g., “40% of users did not like the red color of the headings text.”)

Correcting Usability Problems

Severity Ratings

Severity ratings can be used to determine where to allocate resources to fix the most serious problems discovered in the heuristic analysis and can also help estimate of the need for additional usability efforts. Ratings that indicate a disastrous set of usability problems may indicate that the product should not be released; however, a product may be released if it's problems are judged to be primarily cosmetic.

- The severity of a usability problem is a combination of three factors:
- The frequency with which the problem occurs: Is it common or rare?
- The impact of the problem if it occurs: Will it be easy or difficult for the users to overcome?
- The persistence of the problem: Is it a one-time problem that users can overcome once they know about it or will users repeatedly be bothered by the problem?
- The market impact of the problem: what effect does the problem have on the popularity of a product, even if they are "objectively" quite easy to overcome.

Even though severity has several components, it is common to combine all aspects of severity in a single severity rating as an overall assessment of each usability problem in order to facilitate prioritizing and decision-making.

The following 0 to 4 rating scale can be used to rate the severity of usability problems:

0 = I don't agree that this is a usability problem at all

1 = Cosmetic problem only: need not be fixed unless extra time is available on project

2 = Minor usability problem: fixing this should be given low priority

3 = Major usability problem: important to fix, so should be given high priority

4 = Usability catastrophe: imperative to fix this before product can be released

http://www.nngroup.com/articles/how-to-rate-the-severity-of-usability-problems/

NOTE: some heuristics systems use different ratings scales. We recommend using a consistent scale for all reviews and systems.

Ethical Guidelines User Research Studies

Because user research involves human participants in test environment, it is important to ensure that the participants’ safety, comfort, and autonomy is addressed. Guidelines for the treatment of user research participants ensure protection from any physical or psychological harm that may be caused by the test or the test environment.

Institutional Review Board Requirements

An Institutional Review Board (IRB) is an institutional committee that reviews and approves tests involving human participants. In the United States, IRBs are governed by Title 45 Code of Federal Regulations Part 46. (Code of Federal Regulations". HHS.gov. 2010-01-15.) An IRB is required by any institution conducting psychological or behavioral studies if it is receiving funding from the US government. In most cases, An IRB will not be required for a commercial study; however, IRB guidelines represent a best practice for the treatment of users and user collected information.

Some of the guidance below is based upon the IRB language, which may be downloaded here: The Office of Human Research Protection. Institutional Review Board Guidebook. "Chapter 3, Section A: Risk/Benefit Analysis." pp. 1-10,http://www.saylor.org/site/wp-content/uploads/2011/08/PSYCH202A-3.1.4-Institutional-Review-Board.pdf.

===Survey guidance===

1. Consent to participate must be voluntarily given, as well as the option to decline participation in the survey.

2. Individuals should be able to exit the survey at any time.

3. Survey questions should be comprehensible by a wide audience.

4. Surveys should be concise and easy to answer.

5. Surveys should be open to all users to ensure the widest possible range of individual respondents.

6. Surveys should include an introductory explanation of how the user's personal information and responses will be treated, what level confidentiality they can expect and links to privacy policy, trust frameworks and other policies that govern collection of personal information.

7. Any results of surveys should be aggregated and depersonalized to protect the participant's privacy.

8. Results of the survey could be made available as long as privacy of participants can be insured by the system.

Usability in Identity Systems

Guidance Relevant to IDEF Usable Requirements

This section discusses specific, prescriptive guidance for user tests that address each of the Usability requirements in the IDEF.

USABLE-1. USABILITY PRACTICES

Entities conducting digital identity management functions MUST apply user-centric design, and industry-accepted appropriate usability guidelines and practices, to the communications, interfaces, policies, data transactions, and end-to-end processes they offer, and remediate significant defects identified by their usability assessment.

SUPPLEMENTAL GUIDANCE

The term "user-centric" design is a key tenet and requirement of the IDESG founding document: the National Strategy for Trusted Identities in Cyberspace (NSTIC) dated April 15, 2011. This term is further described in Appendix A of the Baseline Functional Requirements and is a common term in the User Experience domain.

REFERENCES

Consult the UXC Resources page for examples of non-normative UX practices. An archived version as of October 2015 is stored at:https://workspace.idesg.org/kws/public/download.php/60/UXC-Resources.docx

Consult the UXC Dictionary page for examples of UXC definitions of terms in these requirements and supplemental guidelines, in addition to those provided in Appendix A of the Baseline Functional Requirements to this document. An archived version as of October 2015 is stored at:
https://workspace.idesg.org/kws/public/download.php/59/UXC-Dictionary.docx

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ASSESSMENT, DESIGN, REMEDIATION, USABILITY

Usability Guidelines for Usable-1

Usable-1 requires adhering to user-centric design, and industry-accepted appropriate usability guidelines and practices, to the communications, interfaces, policies, data transactions, and end-to-end processes they offer, and remediation of significant defects identified by their usability assessment.

Communications:

1. Readability: Text should be appropriate to the reading level of a general or identified target audience.
2. Plain Language: No acronyms or jargon, acronyms spelled out and defined, accessible
3. Assistance: Instructions and help documentation should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too long. Assistance for impaired users should be available, easy to find and, if possible, provided automatically when common assisted devices are detected (e.g., screen readers, TTD)

Interfaces: See Nielsen Norman Group's 10 Usability Hueristics
http://www.nngroup.com/articles/ten-usability-heuristics/

Lettered statements can be answered affirmatively in an expert walkthrough. Most of the following should be addressed during design (Usable-1) and can be tested by users during assessment (Usable-2).

1. Visibility of system status:
    a. At each point in the system, I am aware of my options and what I can do next.
    b. I know what data or other input is being requested and what will happen to it.
    c. I can see how and whether private information is kept private.
    d. I can tell when the system is processing an action.
    e. I can tell how long a process will take and when it is completed.
2. Match between system and the real world:
    a. I understand the language of the system.
    b. Concepts are presented in terms that are familiar to me.
    c. I do not see terms or phrases that seem too technical or jargony.
    d. The way that actions and information is presented is what I expected it would be.
    e. The process and actions follow a natural, logical flow.
3. User control and freedom:
    a. I can stop the process at any time.
    b. I can return to where I left off.
    c. I can return to the previous state and make changes.
    d. I can leave the system knowing that my data will be saved or deleted according to my expressed wishes.
4. Consistency and standard:
    a. I understand that the words and language used in the website have the same meaning throughout the website.
    b. Actions such as swipes, sliders, link clicks, checkboxes, buttons, refresh, minimize, close, etc. behave as expected within the platform I am using (e.g. iOS, Android, Chrome, etc).

5. Error prevention:
    a. I make very few or no mistakes.
    b. The system offers instructions or explanations when I enter information in a form.
    c. The system asks me to confirm an action, such as submitting data.
6. Recognition rather than recall:
    a. Everything I need to make a decision about my next action is available to me.
    b. I don't feel lost when I go from one page to another.
    c. I know what I am supposed to do next.
    d. The website uses images or options that help me recognize what I need to do next.
    e. I can find help documentation when I need it.
    f. Help is available that is relevant to the item I am working on.
7. Flexibility and efficiency of use:
    a. I am not given too much or too little information to complete my task.
    b. I can expand or collapse help text if I want.
    c. I can copy or repeat frequent actions easily.
8. Aesthetic and minimalist design:
    a. I am not given too much or too little information to complete my task.
    b. I like the way the system looks.
    c. I do not feel overwhelmed by the information presented.
    d. The presentation is not confusing.
9. Help users recognize, diagnose, and recover from errors:
    a. When there is a problem, the system shows an error message and suggests an action.
    b. I understand the error message and know what I need to do to recover.
    c. If I make a mistake or find an error, I do not think it is my fault.
10. Help and documentation:
    a. I understand the instructions and documentation.
    b. I can search for information about a topic or action I don't understand.
    c. Information or help is available for the action I am working on.
    d. I can find step by steps instructions for what I need to do to complete a task.
    e. The instructions and help documentation is not too long or overwhelming to read.

Policies: See Communications

Data transactions: See Interfaces

End-to-end processes: See Interfaces

Remediation: Remediation is defined in the literature as bringing a website into compliance or remedying errors like broken links and accessibility issues. (citation)

While it's not called remediation, Nielsen Norman offers an approach in guideline 9 of their ten usability heuristics:

8. Help users recognize, diagnose, and recover from errors: Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
http://www.nngroup.com/articles/ten-usability-heuristics/

I found a patent that describes remediation as "a method for resolving a problem in a user interface." Seemed pretty succinct to me, but strange that I had to dig into a patent to find a definition. http://www.patentsencyclopedia.com/app/20160041899

From hhs.gov: "The Remediation Framework outlines a course of actions to bring HHS Web sites and content into compliance with Section 508."
http://www.hhs.gov/web/section-508/compliance-and-remediation/framework/index.html

Much of the references to remediation are in the context of accessibility so may be found in accessibility literature. Either that or it is assumed to be a remedy for compliance to an accessibility standard or guideline.

USABLE-2. USABILITY ASSESSMENT

Entities MUST assess the usability of the communications, interfaces, policies, data transactions, and end-to-end processes they conduct in digital identity management functions.

SUPPLEMENTAL GUIDANCE

Entities may satisfy this Requirement by confirming that they have conducted a usability assessment of their digital identity management functions. Other Requirements and best practices in this set address their duty to mitigate issues identified in that assessment.

REFERENCES

Consult the UXC Guidelines and Metrics page. An archived version as of October 2015 is stored

at:https://workspace.idesg.org/kws/public/download.php/58/User-Experience-Guidelines-Metrics.docx

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

Usability Guidelines for Usable-2

Usable-2 requires performing usability assessments of digital identity service.

Reference to Usability Methods

- Expert Reviews
    - Cognitive Walkthrough
    - Heuristic Evaluation
- User Testing
    - Think Aloud User Test
    - Interviews
        - In lab observation
        - Field observation
        - Guerilla testing
    - Diary Study
    - Surveys

USABLE-3. PLAIN LANGUAGE

Information presented to USERS in digital identity management functions MUST be in plain language that is clear and easy for a general audience or the transaction's identified target audience to understand.

SUPPLEMENTAL GUIDANCE

Instructions for use of the system should be visible or easily retrievable whenever appropriate.

Help and documentation information should be easy to search, focused on the users' task, listing concrete steps to be carried out, and be concise.

Platform conventions for words, actions, and situations are consistent across the platform. Example: users should not have to wonder whether different words, situations, or actions mean the same thing across the platform.

The system should speak the users' language, following real-world conventions and making information appear in a natural and logical order. Example: Systems should use words or phrases and graphics or icons familiar to the user rather than system-oriented terms. Example: although the phrase "privacy enhancing technology" is widely in use in industry, research suggests that "privacy protection" is more readily understood and used by real users.

Error messages should be expressed in plain language, without codes, clearly indicating the problem and constructively suggesting a solution.

The user's identity status on a system should be clear to the user. Example: It should be clear to the user whether their identity is anonymous, pseudonymous or verified.

Any change in identity status should be presented in clear language to the user. Example: If a process requires a user to switch to a verified identity from a more anonymous state, the user should be clearly prompted to change their identity status.

Descriptions of states of identity (verified, anonymous, pseudonymous) should be linked to clear, easy to read, understandable and concise definitions.

If standard definitions are available, they should be used.

The design of the website should eliminate information that is irrelevant or rarely needed.

Layout and look/feel/branding, in addition to language, should also eliminate information that is rarely needed.

REFERENCES

None.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

CHOICE, CLARITY, LANGUAGE, OPTIONS, USABILITY

Usability Guidelines for Usable-3

Usable-3 requires use of plain language.

See guidelines for designing communications above. Eg no jargon, average English speaker versus users familiar with identity services.

Include glossary for commonly used terms.

USABLE-4. NAVIGATION

All choices, pathways, interfaces, and offerings provided to USERS in digital identity management functions MUST be clearly identifiable by the USER.

SUPPLEMENTAL GUIDANCE

Systems should provide clear and easy to use pathways to help users recognize, diagnose, and recover from user-made errors.

The information needed by the user to understand any choice should be clearly visible in a single, visible window. Dialogues should not contain information that is irrelevant or rarely needed.

To mitigate the risk of errors, systems should allow the user the option to cancel, skip or decline, before they commit to a pathway action as well as provide a confirmation notice after they commit.

If an entity decides an action is required, and a user chooses to skip or decline this action, the entity's system should state clearly to the user if the transaction will not be completed and present a pathway for redress.

If a user accepts, skips or declines an option, the entity's system should state clearly to the user the transaction was or was not completed.

An entity's systems should allow users the choice to proceed anonymously, pseudonymously or with any chosen / assigned identity where appropriate.

An entity's systems should allow the user choice and clear options for changing the status of their identity. For example: switching to anonymous browsing.

Information users need to make decisions should be readily available and transparent to the user.

The identity of the entity and entity's systems with which the user is interacting should be clearly visible and understandable to users at all times. This includes third parties and changes between entities and users during sessions.

When a new user chooses an identity provider, the available options should be clearly presented so that a user can make an informed decision. When a new user visits a relying party site, the user should be presented with information about the request for identity proofing, verification or attributes and the types of identity providers or frameworks that are acceptable.

Clear pathways should exist for users to procure desired services.

The user should be presented with pathways to the identity services they desire, such as: privacy options, identity caching, etc.

Organizations should operate in a manner that allows individuals to easily switch service providers if the organization fails to meet user expectations, becomes insolvent, is incapable of adhering to policies, or revises their terms of service. See also INTEROP-BP-A (RECOMMENDED PORTABILITY).

REFERENCES

None.

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

CHOICE, CLARITY, CONTROLS, CORRECTION, DESIGN, OPTIONS, USABILITY

Usability Guidelines for Usable-4: Navigation

Usable-3 requires that all choices, pathways, interfaces, and offerings provided to users must be clearly identifiable by the user.

This requirement focuses on clear way-finding practices. The supplemental guidance indicates that error mitigation and risk management should be available when the user takes a wrong turn. General guidance may be covered by communications and plain language principles and NNGroups 9th heuristic. Usable-3 Supplemental guidance contains prescriptive guidance for identity services.

Useful tests:

- Cognitive walkthrough
- NNG Heuristics, 2 and 9
- User observation: wayfinding tasks

USABLE-5. ACCESSIBILITY

All digital identity management functions MUST make reasonable accommodations to be accessible to as many USERS as is feasible, and MUST comply with all applicable laws and regulations on accessibility.

SUPPLEMENTAL GUIDANCE

Entities should review all accessibility standards and apply what they deem feasible to their sites based upon their legal and regulatory environment.

All entities, when feasible, should provide equivalent access to and use of information and systems to users with disabilities that is comparable to the use and access by those who are users without disabilities.

All sites should provide all feasible functionality to any user with a compatible internet connected device as those available to individuals without disabilities.

User with disabilities should have access to documentation tailored to their needs, as is feasible.

User-Centered Design that accounts for accessibility issues should be used whenever possible.

The specific requirements applicable to particular vertical industries (health, finance, etc.) should also be reviewed and applied when relevant.

REFERENCES

Some existing relevant standards and regulations include:

Section 508 contains information about accessibility: https://www.section508.gov/

For example, see ISO 9241 (2010) "Human-centered design processes for interactive systems" and ISO/IEC 40500 (2012) Information technology — W3C Web Content Accessibility Guidelines (WCAG) 2.0

Consult the UXC Resources page for examples of non-normative UX practices. An archived version as of October 2015 is stored at:https://workspace.idesg.org/kws/public/download.php/60/UXC-Resources.docx

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ACCESSIBLE, ACCOMMODATION , DESIGN, USABILITY

Usability Guidelines for Usable-5: Accessibility

Usable-5 requires reasonable accommodation, as feasible and as required by law. Section 508 serves as a minimum requirement for services provided by the federal government and represents minimum best practices for all other services.

ISO 9241 (2010) "Human-centered design processes for interactive systems"
ISO/IEC 40500 (2012) Information technology
W3C Web Content Accessibility Guidelines (WCAG) 2.0
http://www.w3.org/standards/webdesign/accessibility

USABLE-6. USABILITY FEEDBACK

All communications, interfaces, policies, data transactions, and end-to-end processes provided in digital identity management functions MUST offer a mechanism to easily collect USERS' feedback on usability.

SUPPLEMENTAL GUIDANCE

All websites should provide a mechanism to gather feedback from users on site usability, adjusting the site design in response when appropriate.

Users should be provided equitable choices where possible around the mechanisms they can use to express their feedback to entities. Parameters, risks and benefits for those choices should be clear to the user.

REFERENCES

Additional information on collecting USER feedback can be found in our UXC Guidelines and Metrics page. An archived version as of October 2015 is stored at:https://workspace.idesg.org/kws/public/download.php/58/User-Experience-GuidelinesMetrics.docx

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ASSESSMENT, DESIGN, FEEDBACK, USABILITY

Usability Guidelines for Usable-6: Usability Feedback

Usable-6 requires a mechanism for collecting usability feedback from users. NNGroup's heuristic 9 and 10 discuss error recovery and help but do not provide for full remediation and reporting by users to the service provider.

USABLE-7. USER REQUIREMENTS

Wherever public open STANDARDS or legal requirements exist for collecting user requirements, entities conducting digital identity management functions MUST offer structured opportunities for USERS to document and express their interface and accessibility requirements, early in their interactions with those functions. Entities MUST provide a response to those user requirement communications on a reasonably timely basis.

SUPPLEMENTAL GUIDANCE

Any entity "collecting personal data," whether they are first or third parties, would mean that the entity is interacting with USERS directly and therefore should provide a response to user requests early on in the interaction or collection. Website USER do-not-track requests are an example of a USER request. An example of a site that handles responses to Do Not Track

(DNT) requests in this manner is Medium.com which sends a single popup to new users, whether or not they are registered, about how they will handle the DNT request.

As a general principle, consent choices or other similar must-see-this-first information should be exchanged in a first encounter, and then honored in and presented in a consistent manner thereafter.

Suggested ways for User Experience mitigation includes using pop-up boxes or email responses to user requests. Links to information regarding additional use should provide adequate time for users to read the information presented to them.

The entity gathering requests should state whether identity information is being used, and the user must be notified.

Please note that the IDESG Privacy Requirements apply to these interactions and the data they generate.

REFERENCES

More information about Do Not Track can be found at these links: FTC website on Do Not Track:
https://www.ftc.gov/news-events/media-resources/protectingconsumer-privacy/do-not-track
Do Not Track standard work at the W3C: http://www.w3.org/2011/tracking-protection/

APPLIES TO ACTIVITIES

REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, INTERMEDIATION

KEYWORDS

ACCESSIBLE, ACCOMMODATION, ACCOUNT, CHOICE, CONSENT, FEEDBACK, OPEN-STANDARDS, USABILITY

Usability Guidelines for Usable-7: User Requirements

Usable-7 requires structured opportunities to provide interface and accessibility requirements. Supplemental guidance provides a suggested ways to allow this interaction to take place in cases of privacy and consent to use supplied user data. In addition, accessibility requirements

can be mitigated by addressing these issues through standard accessibility testing and remediation.

Identity Ecosystem Scenarios

We have identified three prospective scenarios in which an ID Provider or Relying Party may wish to perform user testing. Note: These are sample scenarios and do not represent all possible activities and processes that may occur within an individual identity ecosystem product or service. We are providing these scenarios as an example of ways you may wish to test your products and services.

In Sundar et al, "Six Ways to enact Privacy by Design: Cognitive Heuristics that predict Users' Online Information Disclosure" (2016), the authors note that heuristics around user privacy can be used in expert or observational testing. In expert testing, the expert can ask if there is a visible trustmark or brand name, if data management practices are outlined in detail and easy to find, whether data is stored briefly or via a third party. For mobile situations, users can be tested to identify whether they are aware when they have established a secure connection and whether they trust the network with which they are connecting to the product.

The following sections present possible scenarios for study at Identity Providers and Relying Parties. There are many other scenarios that can be tested to ensure optimal usability of identity systems.

Identity Provider Scenarios

IdP Scenario 1: The user navigates to an identity provider (IdP) to acquire an account that will be able to support their concerns for privacy. Until the user has been informed in a clear way about the information that will be required to meet the assurance levels required by the IdP, and the user has positively accepted the terms, no information about the user will be stored on the site or on the user's device.

Issues: Data Privacy, Account Setup, Privacy Policy

Expert Testing Procedures

Cognitive Walkthrough of account setup process:

- Will the user achieve the right affect? (User thinking at the beginning of the action)
    - Are the login and account setup functions visible?
    - Is there information about setting up an account, for example, a how-to video/slidedeck or benefits of an account.
    - How does the user know they can create an account?
- Will the user notice that the correct action is available (Locating the command, navigation)?

    - Are the login and account setup functions visible or easy to find?
    - Are the terms of service or privacy policy visible or easy to find?
    - When an account is created can the user access account or privacy settings?
- Will the user associate the correct action with the effect that user is trying to achieve (Identifying the command, visibility, and feedback)?
    - Do the login and account setup functions operate as expected?
    - Are the functions of the account settings clear?
- If the correct action is performed, will the user see that progress is being made toward solution of the task (Interpreting the feedback)?
    - Is there a message or other indication that the account has been setup, with text indicating the either the privacy policy or how identity data will be handled?
    - Does the user receive an email or other notification that the account has been set up?

Heuristic Analysis: Expert evaluates whether the account setup process meets the requirements of NNGroup Heuristic #1, #3 and #10:

- Heuristic 1: Visibility of system status:
    - In each step of the account setup process, the Expert notes whether an operation appears to be triggered and what evidence of the operation exists, such as a change in URL or graphic, animation effect, popup box or other state change.
    - For any function that collects data, expert notes whether there is an indication that this is occurring. Is it explicit, as in a user filling out a form?
    - Questions you can ask:
        - At each point in the system, I am aware of whether or not I am logged into the system.
        - I know what data or other input is being accessed and what will happen to it.
        - I can see how and whether private information is kept private.
        - I can see when the system is processing an action.
        - I can see how long a process will take.
        - I can see when a process is completed.
- Heuristic 3: User control and freedom:
    - Expert notes what information is being requested of the user, if any.
    - Questions you can ask:
        - I can stop or decline the process at any time.
        - I can return to where I left off.
        - I can return to the previous state and make changes.
        - I can leave the system knowing that my data will be saved or deleted according to my expressed wishes.
- Heuristic 10: Help and documentation:
    - Expert walks through the steps of the account setup process noting any errors or missing information.

    - Expert notes copy indicating how the IdP meets required privacy assurance.
    - Expert notes whether a notice of terms and conditions for use of the system is provided.
    - Expert notes whether privacy policy exists and whether it covers preference settings, data storage and deletion.
    - Questions you can ask:
        - I understand the instructions and documentation.
        - I can search for information about a topic or action I don't understand.
        - Information or help is available for the action I am working on.
        - I can find step by steps instructions for what I need to do to complete a task.
        - The instructions and help documentation are not too long or overwhelming to read.

<u>User Testing Procedures</u>

Observation Method:

- Participant completes Pre-Test Questionnaire (see Appendix B for examples)
- Before each task, participant completes a Pre-Task Questionnaire.
- Task 1: Set up a new account.
- Task 2: Find and read the privacy policy.
- During the tasks and without prompting, note whether the participant shares any data privacy concerns. For example:
    - Does the participant express any concerns about data privacy?
    - Does the participant comment on the type of data collected?
    - Is the participant able to find the privacy policy and user settings.
- After completing each task, participant completes a Post-Task Questionnaire. Some questions may include the following, in addition to the more general SUS questions:
    - I understand the type of data that is required to login.
    - The handling of my personal data is explained sufficiently during the signup process.
    - I provided permission for my personal data to be stored on the website or on my device.
    - I am confident that the requested personal data is protected.
    - I am confident that the requested personal data is used appropriately.
    - The privacy settings are easy to find and understand.
    - I was able to find the help documentation and privacy policy easily.
    - I am confident that the service provider does not share my personal data or shares it only with named entities with my explicit permission.
- After completing these tasks, participant completes a Post-Test Questionnaire. Some questions may relate specifically to the tasks, in addition to the more general SUS questions.

Source: Kolter, Jan Paul, “Chapter 5: User Centric Privacy Architecture.” In *User-centric privacy: a usable and provider independent privacy infrastructure*, 2010. https://www.ics.uci.edu/~kobsa/phds/kolter.pdf

True-Intent Study:

Site visitors are randomly asked what their goal or intention is upon entering the site, via a popup or similar mechanism. Visitors may decline participation or agree to continue with the understanding that a process will be triggered that measures their subsequent behavior during the current session, and whether they were successful in achieving their goal upon exiting the site. All identifying data will be removed from the study. A follow up survey can ask questions about their experience with the handling of personal data and privacy.

To determine if a true-intent study or other live user survey is appropriate, you may wish to review current and previous survey studies and response rates. Avoid survey-fatigue by limiting the number of survey campaigns within a given period or filtering prospective respondents to logged in users, based on specific criteria in their user profile. Declining to participate should be a simple process.

IdP Scenario 2: The user wishes their identity on the IdP system to be destroyed, the site will use every lawful means to eliminate any information about the user and avoid reusing the identity that previously was associated with that user for one full year. No request for information about that identity, including the fact that it was previously in use, will be revealed.

Issues: Privacy, remediation

<u>Expert Testing Procedures</u>

Since destruction of user data is a backend process, it would be difficult to evaluate whether the destruction occurs during a user test. As above, an expert or user can note if help documentation or site copy references the ability to request that an ID be destroyed. Additional assurances can be included in confirmation notices, privacy policy and help documentation.

Cognitive Walkthrough of Account Deletion:

- Will the user achieve the right affect? (User thinking at the beginning of the action)
    - Do the instructions or other copy clearly indicate what the system will do with regard to account cancellation or deletion?
    - Are there actionable elements, such as links, icons and buttons, on the page that the user can identify for account management?
    - Do the actionable elements clearly represent the action they will initiate, e.g., the account will be deleted?

    - Are there elements that may distract the user from the task?
    - Is help available for the task?
- Will the user notice that the correct action is available (Locating the command, navigation)?
    - Are actionable elements for account deletion, such as icons and buttons, clearly visible?
    - Are the account management form fields and settings visible? Do they appear to be editable?
    - Are there elements that distract the user from noticing the correct action?
    - Is there a statement in the privacy policy, data policy or terms of use indicating that it is possible to delete an account or remove all personal data from the system?
- Will the user associate the correct action with the effect that user is trying to achieve (Identifying the command, visibility and feedback)?
    - Are icons and button labels representative of account deletion and the related actions they perform?
    - Are actionable elements, such as buttons and links, located near the instructions or icons they are associated with?
    - Are incorrect or unavailable actions visible?
- If the correct action is performed, will the user see that progress is being made toward solution of the task (Interpreting the feedback)?
    - When the action is performed, does the system change? For example, does the copy include confirmation that an action has been performed? Does it go on to the next step in the process?
    - Is there a progress bar or a next/back buttons visible to indicate the user's position within the process?
    - Does the privacy policy, data policy or terms of use indicate what happens to identity data when an account is deleted?

Heuristic Evaluation: Expert evaluates whether the account cancellation process meets the requirements of NNGroup Heuristic #1, #2, #3, #9 and #10:

- Heuristic 1: Visibility of system status:
    - Expert notes whether user can edit privacy and/or account settings.
    - Questions you can ask:
        - At each point in the system, I am aware of whether or not I am logged into the system.
        - I can see when the system is processing an action.
        - I can see when a process is completed.
- Heuristic 2: Match between system and the real world: The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.

    - Expert cancels account and attempts to log back in, noting whether the ID is recognized, for example, via password reminder or other process.
    - Expert notes any language describing account deletion that does or does not fit the users' mental model of deletion.
    - Expert notes whether cookies related to the deleted account are still saved to the local computer
    - Questions you can ask:
        - I am unable to log into a deleted account.
        - I am unable to obtain a password reminder for a deleted account.
        - Cookies related to my account have been removed.
- Heuristic 3: User control and freedom:
    - Questions you can ask:
        - I can stop or decline the process at any time.
        - I can return to where I left off.
        - I can return to the previous state and make changes.
        - I can leave the system knowing that my data will be saved or deleted according to my expressed wishes.
- Heuristic 4: Consistency and standard: Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
    - Expert notes the terms used when canceling or deleting the account.
    - Questions you can ask:
        - I understand that performing the action for cancelling, deleting or removing my account, in each case means that my personal information is also deleted from the system.
- Heuristic 9: Help users recognize, diagnose, and recover from errors: Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
    - When attempting to cancel an account, Expert notes whether a dialog or warning appears noting the account cancellation and requesting confirmation.
    - After canceling the account, Expert attempts to create a new account with the same ID.
    - Questions you can ask:
        - If I cancel or delete my account by accident, I am able to reverse the action before the account is deleted permanently.
        - I have to confirm that I wish to cancel an account.
- Heuristic 10: Help and documentation:
    - Expert accesses the product or service via signup and notes whether any communication of the ability to destroy an ID is included.
    - Expert reviews privacy policy for language on ID storage and removal.
    - Expert reviews "Cancel Account" process for language on identity, what happens to data associated with the account (this is often in the form of a warning that all data associated with the account will be deleted).
    - Questions you can ask:

        - I understand the instructions and documentation.
        - I can search for information about how to delete my account.
        - Information or help is available for deleting my account.
        - I can find step by steps instructions for what I need to do to delete my account and all personal data.
        - The instructions and help documentation is not too long or overwhelming to read.

User Testing Procedures

Observation Method:

- Participant completes Pre-Test Questionnaire (see Appendix B for examples)
- Before each task, participant completes a Pre-Task Questionnaire
- Task 1: Find and read the privacy policy.
- Task 2: Create a new user account.
- Task 3: Locate the user privacy or account settings.
- Task 4: Delete the account.
- Task 5: Try logging into the deleted account.
- Before each task, participant completes a Pre-Task Questionnaire
- During the tasks and without prompting, note whether the participant shares any data privacy concerns. For example:
    - Does the participant express any concerns about data privacy?
    - Does the participant comment on the type of data collected?
    - Is the participant able to find the privacy policy and user settings.
    - After deleting the account, does the participant express any concerns about user data.
- After completing each task, the participant completes a Post-Task Questionnaire.
- After completing all of the tasks, participant completes a Post-Test Questionnaire. Some questions may relate specifically to the tasks, in addition to the more general SUS questions.
    - I knew what I needed to do to delete my account.
    - I was able to find information on account deletion easily.
    - After deleting my account, I was confident that my personal data was removed from the system.

Relying Party Scenario

RP Scenario 1: The user navigates to a relying party (RP) that follows the principles of the IDEF. The site respects the user's intents by avoiding any information collection from the user until the user understands what information about them is required and why. No cookies are

placed on the user's device until the user accepts the terms under which the data is to be used. The site may use existing cookies on the device as proof of the user's intent.

Since user tasks performed at a RP may be similar to those at an IdP, some of the expert and user tests may be similar. The main difference is that a RP does not store the identifying login account data, but only uses data (for example, a unique OAuth token) from an IdP to authenticate or verify user credentials. A RP may or may not require the user to supply information in addition to the information held by the IdP.

Issues: Navigation, communication, privacy, data collection

Cognitive Walkthrough of a Relying Party website:

- Will the user achieve the right affect? (User thinking at the beginning of the action)
    - Does the RP require a login to use its services?
    - If so, are the login and account setup functions visible?
    - Is it possible to access the RP system via an external IdP?
    - Is there information available about accessing the RP services via a third party authenticator or other IdP—such as a how-to video/slide deck or account help documentation..
- Will the user notice that the correct action is available? (Locating the command, navigation)
    - Is there a login or create account button/link?
    - Is the user access function (login/create account) visible or easy to find?
    - Are the terms of service or privacy policy visible or easy to find?
    - If the user does not have an account at one of the IdPs listed by the RP, are there instructions on how to create one?
- Will the user associate the correct action with the effect that user is trying to achieve (Identifying the command, visibility and feedback)?
    - Are the RP and any IdP account access functions clearly delineated?
    - Is the relationship between the RP and any IdP services that they use on the site clear? E.g., would the user understand the role of the IdP?
    - Are the terms and functions of the RP account settings and site access clear?
    - Will the user understand that collection and use of data consistent with IDEF privacy requirements.
- If the correct action is performed, will the user see that progress is being made toward solution of the task (Interpreting the feedback)?
    - Do the login and account setup functions operate as expected?
    - Does the user have access to the Relying Party site?
    - Does the user see a notice or receive an email or other notification that the account access has been approved?
    - Is the RP listed in the list of connected applications or sites at the user's IdP account?

Heuristic Analysis: Expert evaluates whether the process of accessing the RP site via IdP meets the requirements of NNGroup Heuristics #1, #3, #9 and 10:

- Heuristic 1: Visibility of system status:
    - In each step of the account access process, the Expert notes whether an operation appears to be triggered and what evidence of the operation exists, such as a change in URL or graphic, animation effect, popup box or other state change.
    - For any function that collects data, expert notes whether there is an indication that this is occurring. Is it explicit, as in a user filling out a form? Or is it more passive, such as via a third party authenticator, in which case, a notice that a third party authenticator is being used, or request to use an IdP, would be appropriate.
    - Questions expert can ask:
        - At each point in the system, I am aware of whether or not I am logged into the system.
        - At each point in the system, I am able to see a way to log out.
        - I know what data or other input is being accessed and what will happen to it.
        - I can see how and whether private information is kept private.
        - I can see when the system is processing an action.
        - I can see how long a process will take.
        - I can see when a process is completed.
- Heuristic 3: User control and freedom:
    - Expert notes what information is being requested of the user, if any.
    - Experts notes if documentation outlining the RP contractual relationship with IdP(s), particularly as it relates to user data, is available.
    - Questions expert can ask:
        - I can stop the process at any time.
        - I can return to where I left off.
        - I can return to the previous state and make changes.
        - I can leave the system knowing that my data will be saved or deleted according to the privacy policy and terms of use.
        - Collection and use of data is consistent with IDEF privacy requirements.
        - I can easily discover how to remove my account.
- Heuristic 9: Help users recognize, diagnose and recover from errors (remediation)
    - System error messages are appropriate, easy to read, use clear language and provide clear instructions for recovery.
    - Questions expert can ask:
        - Documentation and notification exists telling me what I can do if a change in the relationship with an IdP occurs (e.g. delete account, remove IdP, edit settings, etc).

        - I have a way to request help or recourse to correct any errors (e.g. if I am unable to authenticate or if I have changed my password or other credentials at a linked IdP).
        - If authentication fails, it is clear to the user which party was responsible for the failure.
        - If an error originates from the IdP, the RP provides actionable information to allow the user to correct the failure (e.g. explain single versus 2 factor authentication, link to IdP account management, etc).
        - Add any other questions you may want an expert to investigate.
- Heuristic 10: Help and documentation:
    - Expert walks through the steps of the account access, noting any errors or missing information.
    - Expert notes copy indicating how the RP meets required privacy assurance.
    - Expert notes whether a notice of terms and conditions for use of the system is provided.
    - Expert notes whether privacy policy exists and whether it covers preference settings, data storage and deletion.
    - Experts notes if documentation outlining the RP contractual relationship with IdP(s), particularly as it relates to user data, is available.
    - Questions expert can ask:
        - I understand the instructions and documentation.
        - I can search for information about a topic or action I don't understand.
        - Information or help is available for the action I am working on.
        - I can find step by step instructions for what I need to do to complete a task.
        - The instructions and help documentation is not too long or overwhelming to read.
        - Documentation fully explains all third parties that process a user's personal information and their relationship with the RP.
        - I am able to locate documentation regarding privacy, redress of any failure, unauthorized data storage, or disclosure or change in a relationship with any third party that may provide or receive personal information.

Observation Method:

- Participant completes Pre-Test Questionnaire (see Appendix B for examples)
- Before each task, participant completes a Pre-Task Questionnaire.
- Task 1: Browse the RP site.
- Task 2: Attempt to log into the RP site using an IdP.
- Task 3: Find and read the privacy policy.
- During the tasks and without prompting, note whether the participant shares any data privacy concerns. For example:

    - Does the participant express any concerns about data privacy?
    - Does the participant comment on the type of data collected?
    - Is the participant able to log into the RP site using an IdP?
    - Is the participant able to find the privacy policy and user settings?
- After completing each task, participant completes a Post-Task Questionnaire. Some questions may include the following, in addition to the more general SUS questions (the information presented is clear and understandable, I would recommend this site to a friend or colleague, etc):
    - Task 1: Browse the RP site.
        - When browsing the RP site, without logging in, I am confident that my personal data is safe.
    - Task 2: Attempt to log into the RP site using an IdP.
        - When logging into the RP website with an IdP, I understand what data if any is shared between the RP and IdP.
        - The handling of my personal data is explained sufficiently during the login process.
        - I am confident that I have control over how and with whom my personal data is shared.
    - Task 3: Find and read the privacy policy.
        - I understand that a cookie may be placed on my device or a token created at the IdP account that allows me to use the RP site.
        - I am confident that the requested personal data is protected and used appropriately.
        - I am confident that the service provider does not share my personal data without my explicit permission.
    - Task 4: Find user privacy and notification settings.
        - I was able to find the privacy settings easily.
        - I understand what the choices in the privacy settings mean.
        - All user settings are easy to find and understand.
- After completing these tasks, participant completes a Post-Test Questionnaire. Some questions may relate specifically to the tasks, in addition to the more general SUS questions.

Appendix A: Defined Terms

This IDEF Glossary Version 1.0 is intended specifically to support the IDEF Registry program. It was approved by the IDESG Plenary by electronic ballot on May 13, 2016.

Citations for the primary source of each definition are given in brackets, and link to IDEF Glossary References, where titles and Internet links are provided.

These definitions will be harmonized as a single normative glossary in a future edition of the Requirements. In this document, they are informative but not normative, and may be considered part of the Supplemental Guidance to The IDEF Requirements set. Some meanings may vary from Requirement to Requirement based on context.

https://wiki.idesg.org/wiki/index.php?title=IDEF_Glossary

ACCESSIBLE

A product, service, environment or facility which is usable by USERs with the widest range of capabilities. [ISO 9241-210]

ACCOUNTABILITY

The property of a system or system resource that ensures that the actions of a USER or AGENT may be traced uniquely to that USER or AGENT, which can then be held responsible for its actions. [RFC4949]

AGENT

A non-human application or service acting in the digital environment on behalf of a human USER. Synonymous with "non-person entity" (NPE). See USER

ANONYMOUS

An INTERACTION designed such that the data collected is not sufficient to infer the identity of the USER involved nor is such data sufficient to permit an ENTITY to associate multiple INTERACTIONs with a USER or to determine patterns of behavior of a USER. [IDESG IDEF] [UXC-Dict] See PSEUDONYMOUS

ASSERTION

A statement from an ATTRIBUTE provider to a RELYING PARTY. [NIST SP 800-63-2] NOTE: ASSERTIONs may be used to communicate CLAIMs, ATTRIBUTEs, IDENTIFIERs, or DIGITAL IDENTITIES. See CLAIM

ATTRIBUTE

A named quality or characteristic that is claimed to be inherent in or ascribed to someone or something. [IDESG Taxonomy]

AUTHENTICATION (FM)

"AUTHENTICATION" is defined in the IDEF Functional Model in part as a "Process of determining the validity of one or more CREDENTIALs used to claim a DIGITAL IDENTITY." [FM] CREDENTIAL AUTHENTICATION: Process of determining the validity of one or more CREDENTIALs used to claim a DIGITAL IDENTITY. [IDESG Taxonomy] DIGITAL IDENTITY AUTHENTICATION: Process used to achieve sufficient confidence in the binding between the USER or AGENT and the presented DIGITAL IDENTITY. [OpenID Connect]

AUTHORIZATION (FM)

"AUTHORIZATION" is defined in the IDEF Functional Model in part as a "Process of granting or denying requests for specific access to resources." [FM]

CLAIM

A statement about the USER or AGENT asserting a property of the USER or AGENT without necessarily containing identity information. NOTE: CLAIMs refer to the content of an ASSERTION rather than the specific source and destination. See ASSERTION

CONTROL

SECURITY CONTROL

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [SP 800-37]

PRIVACY CONTROL

The administrative, technical, and physical safeguards employed within an entity to ensure compliance with applicable privacy requirements and manage privacy risks.

CREDENTIAL

A set of data presented as evidence of a claimed DIGITAL IDENTITY. [IDESG Taxonomy]

CREDENTIALING (FM)

"CREDENTIALING" is defined in the IDEF Functional Model in part as a "Process to bind an established DIGITAL IDENTITY with a CREDENTIAL." [FM]

DATA INTEGRITY

The property that data has not been inappropriately altered.

DIGITAL IDENTITY

An ATTRIBUTE set that can be uniquely distinguished in a given context and can be used for a digital interaction. [IDESG Taxonomy]

DIGITAL IDENTITY MANAGEMENT FUNCTIONS (FM)

The functions described in the IDESG Functional Model (REGISTRATION, CREDENTIALING, AUTHENTICATION, AUTHORIZATION, and INTERMEDIATION), which also encompass enrollment, identity proofing, identity vetting, access control, attribute management, transaction processing, and identity data maintenance.

ENTITY

Any organization providing or using identity services. [IDESG IDEF][UXC-Dict] NOTE: The correct usage of ENTITY is “Organization providing or using identity services”; synonymous with Service Provider in the ID Ecosystem. USER should be used for persons. AGENT should be used for non-persons. NOTE: The word “actor” has been employed in this Glossary to replace the term “entity” previously used in some definitions, where ENTITY (as an organization) is not exclusively intended.

FEDERATION

An association comprising any number of service providers and IDENTITY PROVIDERS. [SAML v2.0] NOTE: This definition concerns IDENTITY and CREDENTIAL FEDERATIONs

IDENTIFIER

ATTRIBUTE or value that can be used to distinguish a DIGITAL IDENTITY. [IDESG Taxonomy]

IDENTITY

see DIGITAL IDENTITY

IDENTITY PROVIDER

An ENTITY that creates, maintains, and manages trusted identity information. [NSTAC]

INTERACTION

An event involving two or more actors. See TRANSACTION

INTERACTION DESIGN

A term given to a set of design areas that focuses on the INTERACTION value of content, as opposed to its presentation or information value. The INTERACTION topics include USER interface controls, error handling, and feedback systems. The term “INTERACTION DESIGN” is intended to differentiate these topics from other topics for purposes of evaluation and development. [Human Factors]

INTERMEDIATION (FM)

"INTERMEDIATION" (or "Transaction Intermediation") is defined in the IDEF Functional Model in part as "Processes and procedures that limit linkages between TRANSACTIONs and facilitate CREDENTIAL portability." [FM]

INTEROPERABILITY

The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together to mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate. [NSTAC]

MINIMIZATION

See the IDESG Baseline Requirement “PRIVACY-1. DATA MINIMIZATION” [Reqts]

MULTIFACTOR

MULTIFACTOR AUTHENTICATION

AUTHENTICATION using two or more different factors to achieve AUTHENTICATION. Factors include something one knows (e.g., password/PIN), something one has (e.g., cryptographic identification device, token), or something one is (e.g., biometric). [SP 800-53]

NONPROPRIETARY PUBLISHED FORMAT/SPECIFICATION

A known and consistent format that is published and transparent to all RELYING-PARTIES and IDENTITY PROVIDERS in the relevant network, and is not controlled by a commercial interest. [IDESG IDEF]

PATHWAY

A route or routes of events, actions or INTERACTIONs leading to a defined result. [UXC-Dict]

PERSONAL INFORMATION

Any information about or linked to a USER that is collected, used, transmitted, or stored in or by DIGITAL IDENTITY MANAGEMENT FUNCTIONS. [IDESG IDEF]

PROVISIONING

Creating USER access accounts and assigning privileges or entitlements within the scope of a defined process or INTERACTION; providing USERs with access rights to applications and other resources that may be available in an environment; may include the creation, modification, deletion, suspension or restoration of a defined set of privileges. [ABAC]

PSEUDONYMOUS

An INTERACTION designed such that the data collected is not sufficient to allow the ENTITY to infer the USER involved but which does permit an ENTITY to associate multiple INTERACTIONs with the USER's claimed identity. [IDESG IDEF] [UXC-Dict]

REGISTRATION (FM)

"REGISTRATION" is defined in the IDEF Functional Model in part as a "process that establishes a DIGITAL IDENTITY for the purpose of issuing or associating a CREDENTIAL." [FM]

RELYING PARTY

Actor that relies on an identity ASSERTION or CLAIM. [ISO/IEC 29115]

STANDARD

OPEN STANDARDS are standards made available to the general public and are developed (or approved) and maintained via a collaborative and consensus driven process. OPEN STANDARDS facilitate INTEROPERABILITY and data exchange among different products or services and are intended for widespread adoption. (ITU-T) See also: IDESG Standards Adoption Policy v2.0 [SAPv2]

TOKEN

Something that the claimant possesses and controls that is used to authenticate the claimant's DIGITAL IDENTITY. [IDESG Taxonomy]

TRANSACTION

A specialized form of INTERACTION that involves an exchange of some kind. See INTERACTION

USABILITY

Extent to which a system, product or service can be used by USERs to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. [ISO/IEC 9241-210]

USER

An individual human being. See AGENT

USER-CENTRIC

Systems, design and/or program processes that put the individual human being at the center of the activity. Equivalents and related terms may include: USER, user-centered, human-centered, end user, individual user, user-friendly. [IDESG IDEF] [UXC-Dict]

USER EXPERIENCE

A USER's perceptions and responses resulting from the use of an ENTITY's services as rendered by expected USER AGENTs.

Appendix B: Sample User Research Study

https://docs.google.com/document/d/1ATxHnQzVftlgtK_Omsjq2LgK4SMnoRY1JyawKVYK-Lg

Appendix C: Other Resources

Review of Existing Design Guidelines

UXC Resources, October 2015

https://workspace.idesg.org/kws/public/download.php/60/UXC-Resources.docx

Government Resources

United States

Usability.gov

- What and Why: Benefits of User Centered Design

U.S. Digital Service Digital Playbook

U.S. General Services Administration: Research-Based Web Design & Usability Guidelines
https://www.usability.gov/sites/default/files/documents/guidelines_book.pdf

United Kingdom

UK Government Digital Services Design Principles
UK Government Services Design Manual includes standards and user evaluation from planning, initial design, alpha/beta releases and ongoing development
UK GDS Good Practice Guide: Requirements for Secure Delivery of Online Public Services - Chapter 2 and 3 addresses user expectations
UK GDS Good Practice Guide: Annex A: Stakeholder Expectations

European Union

Usabilitynet.org (EU Funded guidelines)

British Columbia

UX Toolbox: Better Web for Citizens
Accessibility 2024

Other Usability Resources

NNGroup: Articles

Industry Associations and Publications

UX Matters

Boxes and Arrows

Information Architecture Institute: IA Library

Interaction Design Foundation Encyclopedia

UXPA: Usability Body of Knowledge

Common Practices

General usability guidance

- Morville Honeycomb: http://semanticstudios.com/user_experience_design/
- Jesse James Garrett's Elements of User Experience diagram: http://uxdesign.com/assets/Elements-of-User-Experience.pdf

Usability Methods

- Expert Reviews
    - Cognitive Walkthrough
        - Wharton, C., Rieman, J., Lewis, C. & Polson, P. (1994). The Cognitive Walkthrough: A practitioner's guide. In J. Nielsen & R. L. Mack (Eds.), Usability inspection methods (pp. 105-140). New York: Wiley. http://www.colorado.edu/ics/sites/default/files/attached-files/93-07.pdf
    - Heuristic Evaluation
        - Nielsen, Jakob. (1995). "How to Conduct a Heuristic Evaluation." Web. https://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/
- User Testing
    - Thinking Aloud User Test
        - Barnum, Carol M. (2011), *Usability Testing Essentials*. Burlington, MA: Morgan Kaufmann.
    - Interviews
        - Laboratory observation
        - Field observation
        - Guerilla testing
    - Diary Study
        - Rieman, John. (1993), The Diary Study: A Workplace-Oriented Research Tool to Guide Laboratory Efforts. http://dl.acm.org/citation.cfm?id=164935
    - Surveys
        - Brooke, John. (1986). "SUS - A quick and dirty usability scale." http://www.usabilitynet.org/trump/documents/Suschapt.doc

Accessibility Guidelines

ISO 9241 (2010) "Human-centered design processes for interactive systems"

ISO/IEC 40500 (2012) Information technology

W3C Web Content Accessibility Guidelines (WCAG) 2.0

http://www.w3.org/standards/webdesign/accessibility

Remediation Guidelines

"The Remediation Framework outlines a course of actions to bring HHS Web sites and content into compliance with Section 508."
http://www.hhs.gov/web/section-508/compliance-and-remediation/framework/index.html

Usability Guidance for Identity Services

IDEF Registry User Research Methodology
https://docs.google.com/document/d/1ATxHnQzVftlgtK_Omsjq2LgK4SMnoRY1JyawKVYK-Lg
Includes sample user test script

IDESG Identity Design Patterns:
https://wiki.idesg.org/wiki/index.php?title=Identity_Design_Patterns

Kantara: The Design Principles of Relationship Management V1.0 Report (identifies design principles for identity management - possible resource for prescriptive guidance)
https://kantarainitiative.org/confluence/display/irm/Home
https://kantarainitiative.org/confluence/download/attachments/69273830/Kantara%20Initiative%20IRM%20Laws%20of%20Relationship%20Final%20Report%20v1.0.pdf?version=1&modificationDate=1425408854000&api=v2 (PDF)

A Comparative Usability Study of Two-Factor Authentication
http://www.internetsociety.org/sites/default/files/01_5-paper.pdf

NIST Interagency Report (NISTIR) 8080, Usability and Security Considerations for Public Safety Mobile Authentication, has been approved as final & is now available from the NIST CSRC website.
http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8080.pdf

Usability Studies in Privacy, Security, Identity, etc.

Kolter, Jan Paul, User-Centric Privacy – A Usable and Provider-Independent Privacy Infrastructure. Dissertation, University of Regensburg
https://www.ics.uci.edu/~kobsa/phds/kolter.pdf

Sundar et al. Six Ways to enact Privacy by Design: Cognitive Heuristics that predict Users' Online Information Disclosure. Conference Paper. CHI 2016, May 7 - 12, 2016, San Jose, CA.

https://networkedprivacy2016.files.wordpress.com/2015/11/sundar-et-al-final_chi-pbd-workshop-161.pdf

Usable Security (USEC), Internet Society (papers on usability in security products)
http://www.internetsociety.org/events/ndss-symposium-2016/usable-security-usec-workshop-programme
https://www.internetsociety.org/events/ndss-symposium-2015/ndss-2015-usec-programmesion3

Wang, Y.D., and Emurian, H.H. An overview of online trust: Concepts, elements, and implications. Computers in Human Behavior, 21, 2005:105-125.
http://userpages.umbc.edu/~emurian/cv/TrustCHB.pdf