User Engagement

From IDESG Wiki

Contents

Full Title or Meme

This topic takes the concept of User Experience as a deep interaction with the user over time. The intent is to help Kantara plan for the next phases of development.

Context

A proposal is in process to extend the Service Assessment Criteria for NIST SP 800-63 into a Trust Registry API for Mobile Applications that act as the User Agent. The existing proposal addresses the first phase of a user experience in acquiring a User Agent that will honor their intent.

The next phase will be the development os specification to the the current set of specification together into a complete package of all of the user attributes, and only those attributes that are required to establish and retain a relationship between one user and one relying party.

What this is NOT about

- **User Engagement** is also a term used by marketers to mean user manipulations. This is a technical discussion about the interaction of users with their technology choices.
- Patient Empowerment is about asserting what a healthcare patient CAN do. This is a discussion about what a user SHOULD do.

Actors

- User
- User Delegate
- Technology vendor - provider (eg EHR)
- Technology vendor - user (eg Phone App)
- Primary Provider (original RP accessed by the user)
- Other Providers (Other web sites that were not on the user's original agenda)

The objective is to focus the discussion between the user and the site that the user wants to access.

Proofs

Context

is a statement of the set of rules that apply to the current interchanges. (eg US Healthcare HIPAA, aka federation)

User Authentication

is the traditional role for an Identifier provider (IdP). In some ways it becomes an anachronism as we disassemble, enhance and reassemble the parts below into a complete **User Engagement**.

Identity Proofing

is the process of binding an identifier to a real-world person. At its core Identity Proofing is just a comparison of biometric factors of the real-world person to some subset of the user credentials that are accumulated over a user's life-time.

User Informed

- The Relying Party has give the user the information needed to decide to proceed with engagement.
- The Relying Party lets the user know of any changes before they occur if possible.
- Where breach or other unforeseen problems evolve the Relying Party will promptly notify the users and possibly the authorities.

User Agent Integrity

- The application code actually running on the phone is the code that was certified
- The configuration of the phone meets the assurance level requested. For example if a lock screen feature is enabled.
- Report on the level of security of user secrets (e.g. Private keys and other credentials). Hardware versus software protection.

User Intent

Consent to share data to achieve objectives.

Proof of Presence

- Typically this will be real-time identity proofing against biometrics attributes performed in the user agent application software.

Proof of Possession

- This merely affirms that the user has access to the private key that can create a signature (or similar crypto.)

Liveness

- The user reamains engaged in the session and is not replaced by someone else.

Currency

- Proof that user attributes (claims) are still valid.

Notice and Consent

- How is the patient informed of the transfer of information between providers with a frequency and level of detail that understands the user's expectations.
- Notice can be contemporaneous with the interaction, or can occur later if an event occurs at the RP or in a receipt of some sort that the user can view if questions about the interaction arise later.

Problems

- The biggest challenge is to adequately address the preservation of User Rights in digital interchanges.
- If the user expectations are not met because of the actions of some bad actors, the users will reveal against the technology and demand better treatment.

Problem Remediation

- The User Rights will include the ability to cancel or seek redress for descrepancies.

Fraud Detection

Let us not forget that the attacker is one user of the system. They can imitate either party in the transaction to divert assets to their own use. It is to be expected that the RP will use techniques to detect fraud and that is beneficial to the health of the ecosystem. The user needs to understand what these are, in broad terms, and consent to the functioning.

Sovereign Surveillance

Governments have a duty to protect both parties to an internet transaction. But they can destroy trust by those actions and must be held to account. For example, if a state insists on the use of only their app in the smart phone to enable the mobile driver's license, and then uses that for surveillance, the users may lose trust in the system an fall back to using paper cards rather they electronic replacements.

User Agent Trust

- The application that is interactive with the RP on the user's behalf is know to protect the user's secrets and intent.

Soltuions

Kantara already has a deep reservoir of experience in the development os specification on the User Experience that can serve as a basis for the next steps.

1. User Managed Access
2. Consent Receipt
3. Mobile Authentication Assurance Statement.
4. Privacy and Identity (https://docs.kantarainitiative.org/PImDL-V1-Final.html) in Mobile Driver's License

The path forward

If the existing projects are considered as phase one, which is still in active development, the following items could be considered as phase two.

The objective is to ensure that **User Engagement** works to the benefit of both the user and the RP. Each party must feel that their needs are adequately met and that one side is not taking advantage of the other.

1. The consent receipt is being expanded into
    1. a consent record.
    2. a generalized notification.
2. The MAAS is being bound, in-real-time, into:
    1. proof that the user is present at the device
    2. proof that the software running on the device is same code that received the MAAS
    3. current device configuration that describes security settings (not user settings.)

References

Research

- What is user engagement? A conceptual framework for defining user engagement with technology (https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.20801)

    > The purpose of this article is to critically deconstruct the term engagement as it applies to peoples' experiences with technology. Through an extensive, critical multidisciplinary literature review and exploratory study of users of Web searching, online shopping, Webcasting, and gaming applications, we conceptually and operationally defined engagement. Building on past research, we conducted semistructured interviews with the users of four applications to explore their perception of being engaged with the technology. Results indicate that engagement is a process comprised of four distinct stages: point of engagement, period of sustained engagement, disengagement, and reengagement. Furthermore, the process is characterized by attributes of engagement that pertain to the user, the system, and user-system interaction. We also found evidence of the factors that contribute to nonengagement. Emerging from this research is a definition of engagement—a term not defined consistently in past work—as a quality of user experience characterized by attributes of challenge, positive affect, endurability, aesthetic and sensory appeal, attention, feedback, variety/novelty, interactivity, and perceived user control.

This exploratory work provides the foundation for future work to test the conceptual model in various application areas, and to develop methods to measure engaging user experiences.

Categories: User Experience | Trust
