Dustin O'Hara
University of California, Los Angeles
dustin.ohara@gmail.com
February 2015

User Experience Research / Design for the NDN Identity Manager Application

One of the core aims of the ID manager is to enable users to manage the public keys for their encrypted data. In this sense, the ID manager falls into the broad category of public key infrastructure (PKI). The adoption of PKI systems has largely taken place within "coherent" organizations, echoing the longer history of encryption happening under the management of nation states, armies, and more recently corporations. Whitfield Diffie, a key figure in the development of public key cryptography, was in the 1970s a self described "young radical" who was interested in "protecting the individual." Subsequently, in the decades since Diffie's initial public key work, PKI has been taken up by some individuals, but their numbers are limited. Recently, some research has gone into why there has been such low adoption of end-to-end PKI (Renaud, et all). This research has pointed to two main points: 1. most internet users don't understand how the internet works, nor do they feel the need for personal security, and 2. the user experience of current encryption tools requires a high degree of technical skill. In Jean-François Blanchette's words, "people want privacy, but they don't want to practice privacy."

If internet users aren't willing to "practice" privacy, what are they practicing? What skills do they regularly perform? It turns out about 42% of interest users know how to "friend request." According to Google, out of the 2.92 billion internet users, 1.23 of them are active on Facebook. It's a statistic that reaffirms the well known fact that the Facebook user experience of "friend requesting" and "liking" pages and posts, has effectively entered, if not dominated, the popular vernacular of internet usage. The two-way authentication process of friend requesting, coupled with its wide spread familiarity, became the impetus for conducting a close reading of the Facebook user experience. The analysis was primarily focused on the friend requesting process, and the design choices that support authentication and trust. This analysis, then helped inform a series of guiding principles for the user experience of the NDN ID Manager.

Principles for the User Experience of the NDN ID Manager

1. Articulating one's place within the network is often foundational to social practices involving trust.

2. The ID Manager is about the management of context & trust, rather than the direct management of public keys.

3. Trust & context are first established by situating and understanding one-another's place within the network, which is mirrored by the nature of the exchange.

The Ontology of the ID Manager User Experience

The Identity Manager, is defined by "*users*," "*apps*," and "*data types*." The networked configuration of these are then clustered into self defined "*identities*," that correspond with the various aspects of the user's life.

Identities: enable the user to quickly cluster their tasks, into self described identities (i.e. home & utilities, family, work, social, media, etc). Each identity is defined by the particular networking of users, apps, and data types, constituting the specific tasks and performative norms of that identity.

Data Types: allow the user to quickly understand what data, or public keys, the various apps and users have access to. Rather that managing specific public keys, the user authorizes clusters of public keys, for present and future exchanges. These clusters of public keys are the "*data types*."

Users: are understood as other individuals or groups that the user is actively, or potentially, exchanging data with. Before a connection authorized (or public keys are shared), the user is vetted by reviewing the user's "*mutual apps*," "mutual users," and the "*data types*" associated with their common apps.

Apps: function as a trusted context for a given exchange, and are understood by their necessary "*data types*" and "*mutual users*." Apps are identified and associate with a wide range of institutions and groups, whose branding and functionality inform the affective experience of the user, and by extension the choices in how they categorize the app in relationship to their "*identities*."