Abstract Title: Reducing the Tail Risk of CA Compromise by Enabling Trust in Regional CAs Using Language Community and Locale Annotations

Author: Brad Hill, PayPal Inc.

Technology Space: Trust Store Partitioning, User Interface

Abstract Body:

That all Certificate Authorities are equally trusted to assert all names contributes greatly to the perceived insecurity of the market by creating many single points of failure and expanding the scope of trust beyond what many users are comfortable with. 99% of certificates are issued by just the top 8 global CAs. Many other CAs in the "long tail" of issuance do not need to be trusted by any given user in their common activities, as they serve distinct geographical and language communities or are operated by foreign sovereign governments. Partitioning this trust can greatly reduce this tail risk, and might be partially accomplished by a simple system of annotating the target market of CAs and matching that to a given user's locale and/or language communities. Users could then be prompted the first time they encounter an assertion by a CA targeting a different market or language community. A similar heuristic is used today by some browsers to reduce spoofing risks in the display of international domain names - users only see native renderings if they have installed the relevant language support.

If standardized, such annotations could be populated in several ways. Annotations could be voluntary added by CAs themselves, to reduce their value as a target. For example, this could have prevented DigiNotar, a CA serving almost exclusively the Dutch language community, from being targeted in order to attack members of the Persian language community. Annotations could be enforced by trust store operators, perhaps to accommodate differential audit regimes and requirements. Or, annotations could be chosen by users from lists curated by special-interest communities. This system would preserve local sovereignty in the context of the Internet, reduce the risks to the global Internet community of localized trust frameworks, and empower user choice in personal trust decisions.