Author: Phillip Hallam-Baker, Principal Scientist Comodo Inc.
Title: The Omnibroker
Areas: Revocation, Trust evaluation, User Interfaces

The Web PKI has been subject to numerous criticisms since its inception. Complaints made include that the criteria for obtaining a certificate are too strict and that they are too lax, that number of Certificate Authorities is too large and that the small number of Certificate Authorities represents an unacceptable concentration of trust.

Various proposals have been made to 'remedy' the operation of Certification Authorities. It should however be noted that when considering a proposal for an entirely new Public Key Infrastructure, the criteria against which it is judged should not be merely whether the new proposal addresses the defects the proposer sees in the existing CA infrastructure, any new proposal must also satisfy all the requirements that the existing infrastructure is designed to meet. Assuming that network administrators will never make a mistake affords a considerable simplification in design as the 'Sovereign Keys' proposal illustrates. But since real world administrators make mistakes rather frequently, the result is merely an academic exercise.

The Omnibroker mechanism is designed to address two particular criticism of the existing Web PKI: That large CAs are 'too big to fail' and that since CAs are engaged by certificate holders, they are a poor proxy for safeguarding the interests of relying parties. To address these defects a new class of PKI third party is introduced, the 'trust curator' and a new protocol, Omnibroker is defined to mediate communication between a relying application and the Trust curator.

In contrast to the earlier notion of a 'validation authority', the scope of a trust curator covers all trusted network infrastructures including PKI, DNS, time, security policy and reputation. A competitive market for such services is envisaged as a logical extension of existing anti-virus products.

--
Website: http://hallambaker.com/