Applicable area: Transparency and alternative certification, distribution or confirmation of key information;

Title: Usable Trust Anchor Management

Authors: Scott Rea, Dr. Massimiliano Pala

Abstract:

Security in browsers is based upon users trusting a set of root Certificate Authorities (called Trust Anchors) which they may know little or nothing about. Browser vendors face a difficult challenge to provide an appropriate interface for users. Providing usable Trust Anchor Management (TAM) for users, applications and PKI deployers is a complex task. In this paper we describe how Trust Anchor Management is a central point for PKI usability. We advocate that by adopting a more dynamic approach to PKI services, in particular within browsers, both PKI and Application vendors can benefit from easier to use services and more flexible infrastructure. In particular we detail different approaches to linking different PKIs and recommend a hybrid trust model for doing so.

Our tests show that a hybrid trust model, which combines the flexibility of cross-certification with the ease of deployment typical of the hierarchical trust model, is supported by many available applications. The proposed solution also addresses trust management issues by reducing the number of trust anchors needed by applications to a minimum. Still further investigation is required to better understand all the possibilities provided by the usage of this model but we are currently in discussions with potential live PKI based communities for conducting a limited proof-of-concept pilot. We believe that operational experience will be important in validating the usability of this approach and its adoption in specific environments (e.g. research networks and grid communities) where simple trust management of certificates and linking of isolated PKIs is required. We expect that our work will provide valuable feedback for the implementation of TAMP and provide a useful use-case to further promote the standardization of PRQP.