Cryptology ePrint Archive: Report 2011/029

Outline of a proposal responding to E.U. and U.S. calls for trustworthy global-scale IdM and CKM designs

Benjamin Gittins

Abstract: In 2007, the E.U. FP6 SecurIST called for trustworthy international identity management (IdM) that was user-centric. In 2009, the U.S. Department of Homeland Security (DHS) called for trustworthy global-scale IdM and the U.S. National Institute of Standards and Technology (NIST) called for new cryptographic key management (CKM) designs. In this paper we outline the core architecture for (apparently) the first globally scalable, post quantum secure, symmetric key based platform for provisioning IdM, key distribution/agreement and inter-enterprise CKM services. Our proposal employs a decentralised trust model that exploits compartmentalisation, redundancy and diversification simultaneously across service provider, software developer, hardware vendor, class of cryptographic primitive, and protocol axis. It employs behavioural analysis techniques and supports the collaborative management of international name spaces, management of client transactions using public identifiers and supports user-centric cross-cutting control mechanisms. Our proposal is suitable for use with commercial off the shelf hardware and is designed to wrap-around and protect the output of existing security deployments. The platform addresses the U.S. Networking and Information Technology Research and Development Program (NITRD) call to create a digital immune system (multi-layered protection, decentralised control, diversity, pattern recognition), the DHS call for combating insider attacks and malware, achieving survivability and availability, and NIST managers' call for a CKM design supporting billions of users without the use of public key technologies. This proposal has been designed as part of our Trustworthy Resilient Universal Secure Infrastructure Platform project.

Category / Keywords: secret-key cryptography / identity management, key management,

Publication Info: This work is based on an earlier work: "Overview of SLL's proposal in response to NIST's call for new global IdM-CKM designs without Public Keys", in Proceedings of the 6th Annual Workshop on Cyber Security and Information Intelligence Research (April 21-23, 2010) (C) ACM, 2010.

Date: received 17 Jan 2011, last revised 14 Mar 2011

Contact author: cto at pqs io

Note: Minor clarifications made throughout the text. Change outdated references to Trustworthy Cloud Compute Platform (TC2P) in the text to reflect new project name: Trustworthy Resilient Universal Secure Infrastructure Platform (TruSIP).