Company Background

P3KI GmbH was founded in 2014 by Felix ‘FX’ Lindner as a subsidiary of Recurity Labs GmbH, a spin-off of Recurity Labs’ research & development program. P3KI is the culmination of eight years of research into alternatives to existing PKI approaches, initially based on the automotive ISO 20828:2006 (Road vehicles – Security certificate management) standard.

PKI

Existing Public Key Infrastructure approaches are mostly based on X.509 certificate schemes. Certificates are commonly issued by intermediate certificate authorities which in turn are backed by root certificate authorities which are ultimately trusted by the mere fact that their certificates are declared trusted by being included in the default trust stores of major operating systems, browsers, and mobile devices.

Shortcomings of these systems are plenty and range from difficulties in the key distribution during provisioning of large numbers of devices, regular maintenance-related key distribution due to certificate expiration, to often overlooked cases where things go wrong: compromised root or intermediate certificate authorities or active attacks, such as Denial-of-Service attacks targeting central infrastructures required by these systems (e.g. key distribution, online certificate status protocol servers, certificate revocation lists, etc).

P3KI offers an alternative approach and the required technology to tackle the following key issues:

- Separation of identity and permission delegation data
  - Update intermediate permission delegations without affecting leaf nodes (no need to roll out new client certificates)
  - Update intermediate permission delegations at minimal cost and high frequency (certificate lifetimes measured in minutes instead of days)
- Arbitrarily precise expression of permission levels
  - Vastly improved risk management capabilities
  - Easier damage assessment in forensic scenarios
  - Ability to refine permission expressions while already in the field
  - Evaluation of permissions via pure mathematics (clear provability)
  - Safe permission delegation semantics
- Graceful degradation
  - Offline capable
  - No central infrastructure required
  - Fully transport agnostic (seamlessly switch from central database to distributed peer-to-peer to offline verifiable permissions exchanged via near-field communication)
- Forward web-of-trust definition
  - No inherently trusted root certificate authorities required
  - Multi-path permission delegation links as native features
- Easy & safe to use
  - Off-the-shelf integrations and extensions for PAM, X.509, VPN solutions
  - Background service (daemon) for easy server-based deployments
  - C-ABI multi-platform library (targeting x86_64, ARM, MIPS, and more)
  - Straight forward, minimal API
  - Trust data fully opaque to application- and transport layer
  - Full-stack and full life-cycle consulting and support (assessment, planning and design, implementation and customization, rollout, operations)

Contact P3KI GmbH at +49 711 22051252, +49 30 695399933, contact@p3ki.com, or via p3ki.com.