Identity-Based Encryption / Private Key Generator

Der Private Key Generator (PKG) berechnet als Teil eines "Identity Based Encryption Systems" die privaten Schlüssel
der Empfänger. Ein Empfänger muss ein eindeutiges Identitätsmerkmal (bspw. eine KVNR, TID, E-Mail-Adresse besitzen).

Mit dem PKG kann man ebenfalls einen Hashwert inkl. Zeitinformationen von beliebigen Nutzerdaten
bestätigen lassen (quasi als Fernsignatur-Light).

Beispiel-Implementierung: https://bitbucket.org/andreas_hallof/pkg/

Vorträge:

Toller Vortrag von John Tate allgemein über die Arthmetik von elliptischen Kurven:

https://www.youtube.com/watch?v=RtiVaALdqX0

Super Vortragsreihe: https://www.youtube.com/playlist?list=PL8Vt-7cSFnw2V2Wpf4MpwtSJvLvZo1ADB, The 3rd BIU Winter School: Bilinear Pairings in Cryptography

---

Revision #1
Created 15 February 2026 14:21:56 by Admin
Updated 15 February 2026 14:24:54 by Admin