27 February 2018 Study · E-Government · Digital Identity

Demonstrator IBE for Key Management

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Version 2018-02-27
Source https://technology2.a-sit.at/en/publications/demonstrator-ibe-for-key-management/

The project demonstrates an alternative approach of managing cryptographic keys in organisations (by using concepts of identity-based encryption).

Key management in organizations is complex, prone to error and slow. An example is email and S/MIME. Future employees cannot receive encrypted email because there exists no cryptographic key (yet), expired keys forecloses sending encrypted email as well. The aim of this very project is to use ideas and concepts of identity-based encryption (IBE) to construct a centralized key management infrastructure. That infrastructure is able to automate and simplify the management processes and thus, besides speeding up the process, can implement features that can overcome the restrictions stated above. In the end, the approach overcomes a set of hurdles on the way to totally encrypted communication in organisations.

Links

CrySIL-Demo Site (deactivated)

Webapplikation Demonstrator (deactivated)