Lightweight Identity-Based Signature

Description

Identity-based cryptology allows a user to use his or her identity as a public key, simplifying encryption and authentication tasks. But some parts of these tasks are computationally heavy-weight.

An online/offline signature allows a signer to outsource the signing part to an external but untrusted party. This is particularly useful if the signer is using a lightweight device, such as a wireless sensor or smart card that lacks substantial computing power. The heavy parts of the computation can be delegated.

Our identity-based solution eliminates the costly process of certificate verification, and allows a lightweight device to carry out signature generation and verification.

Features

- Identity-based – no certification verification
- Efficient – no pairing operation
- Lightweight – for resource-constrained device

Applications

- Mobile Device
- Smart Card
- Wireless Sensor

Features Diagram:

- **Identity Based**
- **Trusted Key Generator**
- **Lightweight Device**
- **Untrusted Server**
- private key confined on smart card
- signature

References


Department of Infocomm Security, Institute for Infocomm Research (http://icsd.i2r.a-star.edu.sg)
1 Fusionopolis Way, #21-01 Connexis (South Tower), Singapore 138632
Contact: Eunice Pee (IDM) Tel: (65) 64082180 Email: eunice-pee@i2r.a-star.edu.sg