Basic Idea

• Use identity as the key for encryption and signature verification.
  – No key directory needed.
• Trusted key generation center (KGC)
  – Give each user a smart card when user first joins the network.
  – Each user uses the secret key in smart card for decryption and signature verification.
  – KGC can be closed after all cards are issued.

Basic Idea (Cont’d)
The security of underlying cryptographic functions.

• The secrecy at KGC.
• Identity check before issuing cards to users.
• The loss, duplication and unauthorized use of cards.

Implementation of Signature Scheme

• KGC chooses three public parameters. The factorization of $n$ is only known by KGC.
  – $n=pq$, $p$ and $q$ are large primes
  – $e$, which is relatively prime to $\phi(n)$
  – $f$, which is one way function
• The secret key corresponding identity $i$ is $g$
  – $g^e = i \pmod{n}$
  – KGC can compute $g$ easily. Why?
    $$ ed \equiv 1 \pmod{\phi(n)} $$
    $$ p' = (g^e)^i \pmod{n} - g $$
Signature Generation and Verification

• Signature generation
  1. Choose random number $r$
  2. $t = r^e \pmod{n}$
  3. $s = g \cdot r^f(t,m) \pmod{n}$
  4. Signature is $(t, s)$

• Signature verification
  $se = i \cdot t^{k_i} \pmod{n}$
  $s^e = g^e \cdot r^e \cdot f(t,m) \pmod{n}$

Misc

• Multiplicative relationship between the identities will introduce same relationship between secret key.
  – Expand identity to pseudo-random string

• $r$ cannot be reused or revealed