

Smart Cards

Carrying certificates around

How do you use your [digital] identity?

- Install your certificate in browser
- On-computer keychain file

Need there be more?

Smart cards

- Smart card
 - Portable device
 - credit card, , key fob, button with IC on it
- Communication
 - Contact-based
 - Contactless
 - Near Field Communication (NFC)
 - Communication within a few inches of reader
 - May draw power from reader's EMF signal
 - 106-424 kbps
 - Hybrid: contact and contactless

Smart cards

- Capabilities
 - Memory cards
 - Magnetic stripe: stores 125 bytes
 - Smart cards typically store 32-64 KB
 - Optional security for data access
 - Microcontroller cards
 - OS + programs + cryptographic hardware + memory

Smart card advantages

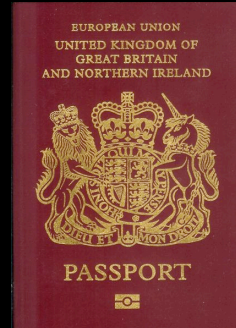
- Security
 - on-board encryption, hashing, signing
 - data can be securely transferred
 - Store biometric data & verify against user
 - key store
 - store public keys (your certificates)
 - do not divulge private keys
 - perform digital signatures on card
- Convenience
 - more data can be carried on the card
- Personalization
 - e.g. GSM phone card

Smart card applications

- Stored-value cards (electronic purses)
 - Developed for small-value transactions
 - Mid 1990s in Europe and Asia
- GSM phone SIM card
- Credit/Debit
 - Stored account numbers, one-time numbers
 - EMV System (Europay, MasterCard, VISA)
- Passports
 - Encoded biometric information, account numbers
- Toll collection & telephone cards
 - Account number (EZ-Pass) or stored value (mass transit)
- Cryptographic smart cards
 - Authentication: pin-protected signing with private key

Example: Passport

- Contactless communication
- Stores
 - Descriptive data
 - Digitized facial image
 - Fingerprints, iris scan, etc. optional
 - Certificate of document signer & personal public key
- Basic Access Control (BAC)
 - Negotiate session key using passport #, date of birth, expiration date
 - This data is read optically
 - Generates 3DESS "document basic access keys"
 - Fixed for life
 - German proposal to use Diffie-Hellman key negotiation



Example: Octopus

- Stored value card - contactless
 - Provision for automatic replenishment
 - Asynchronous transaction recording to banks
 - Two-way authentication based on public keys
 - All communications is encrypted
- Widely used in Hong Kong & Shenzhen
 - Buses, stores, supermarkets, fast food, parking
 - Logs \$10.8 million per day on more than 50,000 readers
- Available in:
 - Cards, fobs, watches, toys

