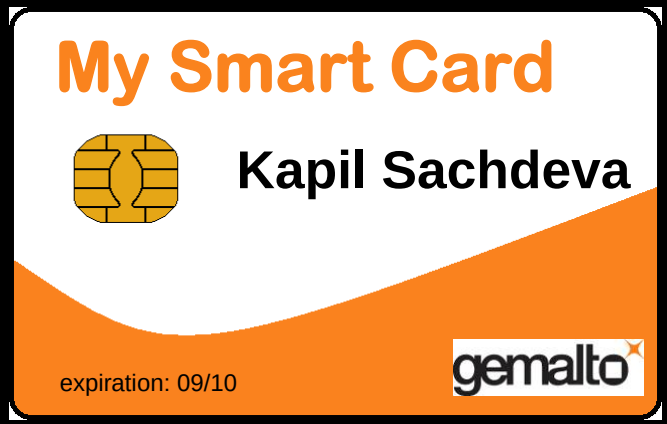
Browser based approach for Smart Card Connectivity



Karen Lu
Ksheerabdhi Krishna

CSP

Sign ??

PKCS#11

Certificates

Encrypt??

CDSA

Middleware

Select &
Propagate
Certificate

Challenges

- **Installing crypto providers**
  - **Breaks mobility**
  - **Breaks ubiquity of web**
  - **Configurations hard for end user**
- **Supporting implementations compliant to various arch./browser/OS combination is painful**
- **User interface decoupled (and not controlled) through web application**
- **All crypto arch abstractions are leaky**
  - **Do not utilize all the functionalities offered by security device**

SConnect

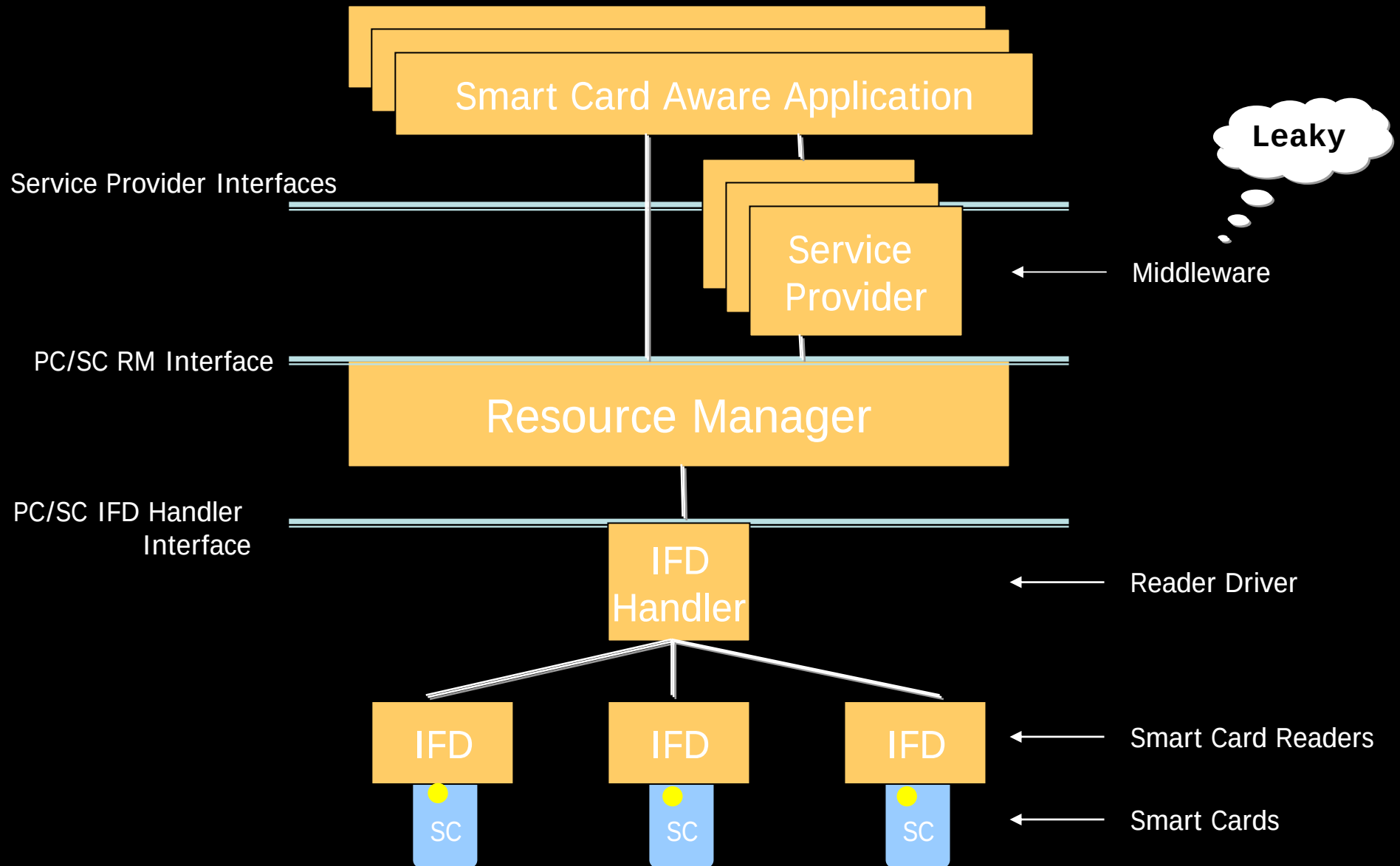
- **Web apps drive the user interface**
  - **Enable the possibility of continuous improvement**
- **Implementation for a particular smart card access comes from server (as JavaScript)**
- **Enable other functionalities:**
  - **Alternative auth mechanisms**
  - **Digital signature & encryption for web content**
- **Consistent interfaces across browsers/os**

SConnect security mechanisms

- **HTTPS Required**
- **Override user’s decision to ignore SSL errors shown by browser**
- **Connection key to only allow authorized sites**
- **User Consent**

Questions?

Leaky Abstraction



Abstraction that works