

JASON: A Generic Architecture for Secure Remote Management

Security of Systems group,
Radboud University Nijmegen
Chess IT, Haarlem

Goals

To design a *secure, object oriented, distributed* programming platform for *smart cards and embedded systems* that provides

- separation of concerns: application programmer only needs to specify the security properties, not implement them, and
- generic secure access to objects and their methods, irrespective of their current location.

Design decisions

- Java based (J2EE ... JavaCard).
- Smart cards and embedded devices (like PC's) are real nodes in an IP network, each containing a collection of objects.
- Objects communicate through Remote Method Invocation (RMI).
- Role based access control.
- Security requirements specified by additional keywords in the object interface.
- Platform provides secure remote method invocation (SMI) to satisfy these requirements.

Example

The following piece of code shows the use of additional keywords in a Java interface to specify the security requirements of an electronic purse.

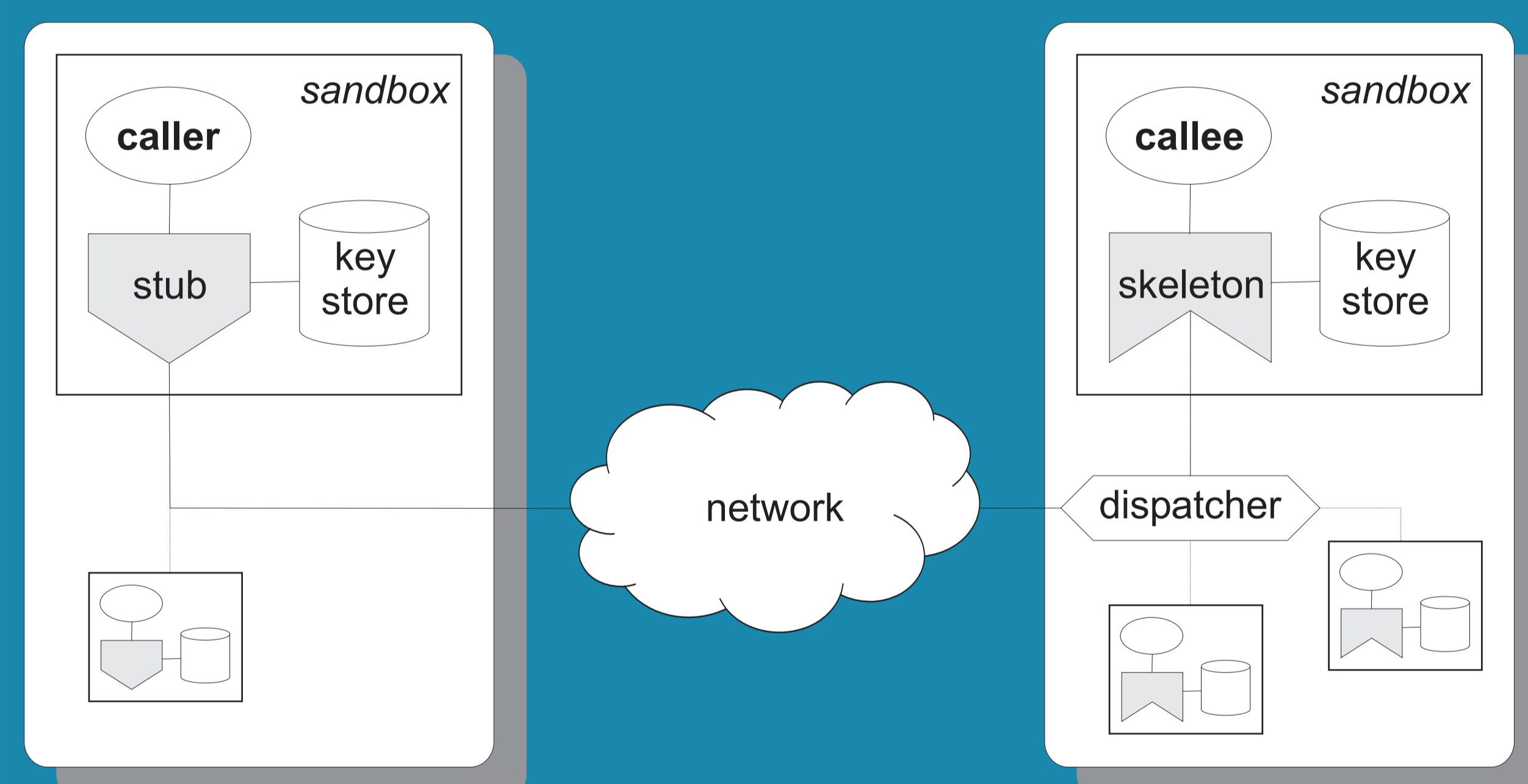
```
public interface Purse
{
    roles BANK, MERCHANT, OWNER;

    accessible to ALL
    authentic short
    getBalance();

    accessible to BANK
    authentic short
    increaseBalance(confidential
                    authentic short amount);

    accessible to MERCHANT
    authentic short
    decreaseBalance(authentic
                   short amount);
}
```

The interface is used to construct stubs and skeletons. SMI requests are sent from caller to callee through a stub (securing outgoing requests), and received by the skeleton (performing access control decisions, and securing outgoing return values).



Contact

For more information, contact
dr. Jaap-Henk Hoepman (jhh@cs.ru.nl,
telephone: 024 3652710). See also
<http://www.cs.ru.nl/jason>