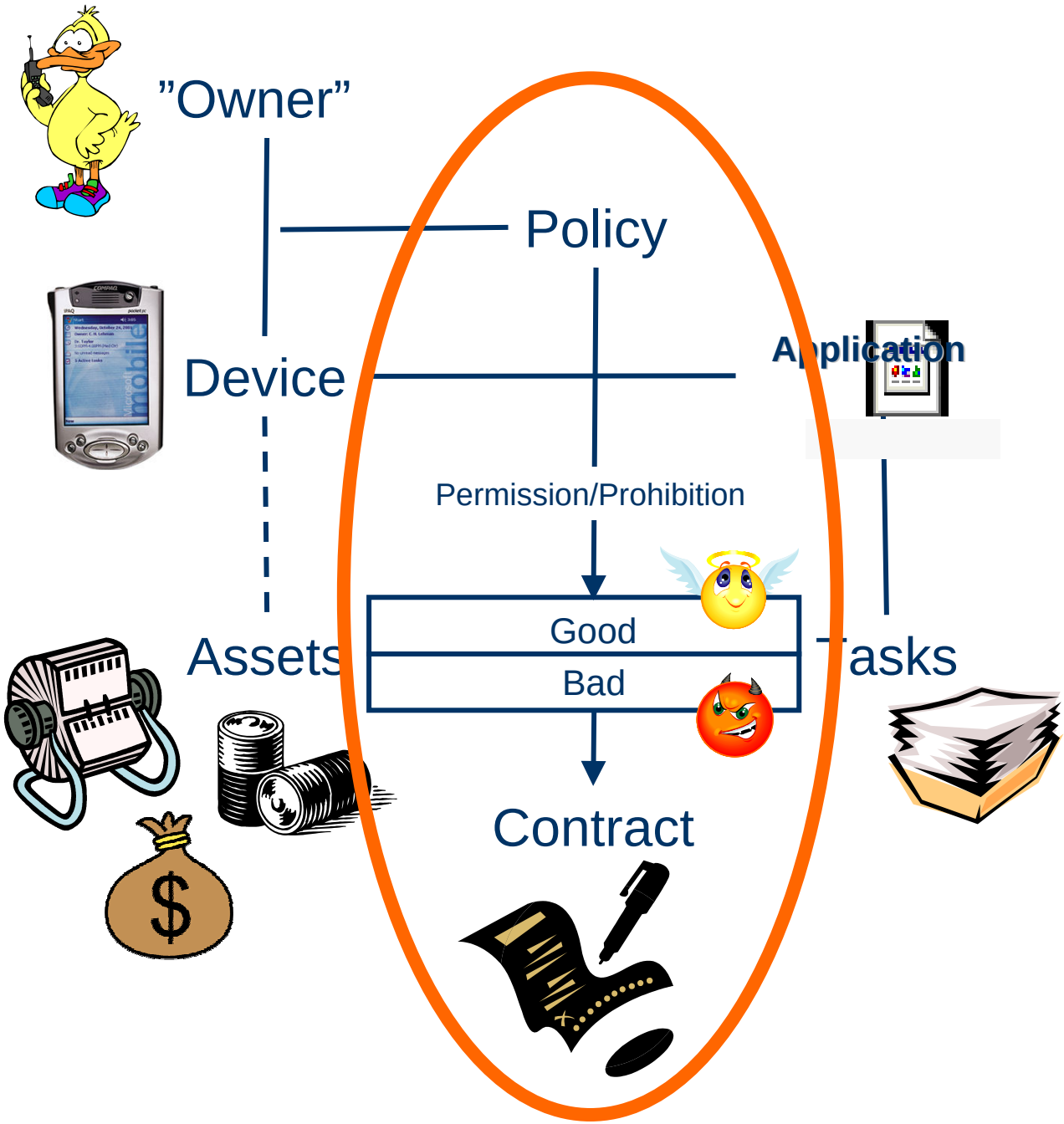
# Håndheving av sikkerhetspolicies i mobile applikasjoner

Folker den Braber
SINTEF
23. november 2006


"Owner"
Policy
Device
Application
Permission/Prohibition
Good
Bad
Assets
Tasks
Contract

# HappyBirthdaySMS - Introduction

- Application running on a mobile device
- Offering a semi-automatically service that sends a personal written congratulating message to contacts in the contact list having their birthday

- Possibility to specify different categories of contacts
- Possibility to specify different policies for each category

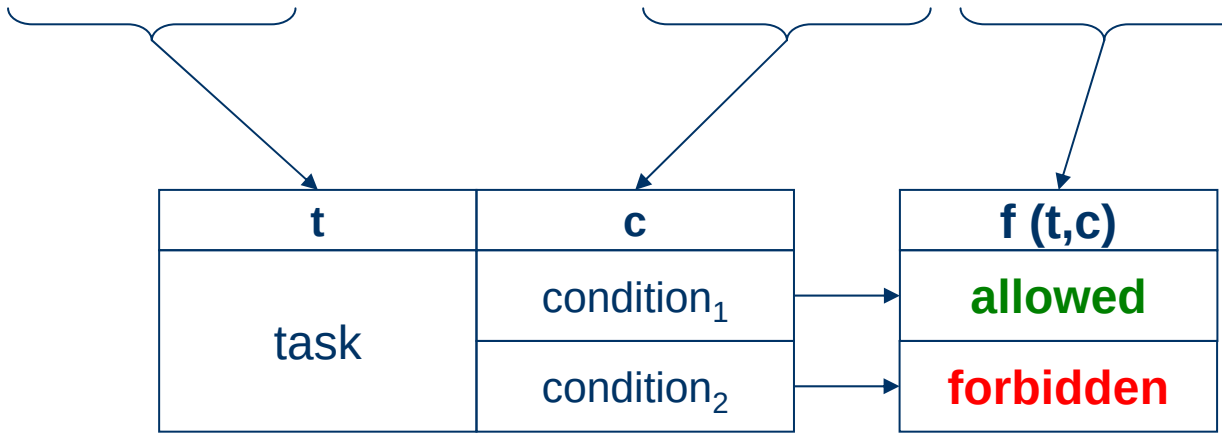
| | Always | Ask me | Never |
|---|---|---|---|
| **Friend** | x | | |
| **VIP** | | x | |
| **Normal contact** | | | x |

# HappyBirthdaySMS – General Security policies

- Do not read contact information for contacts without permission
  - name
  - birthday
  - mobile phone number
- Do not send SMS to any contact category before requiring permission when necessary

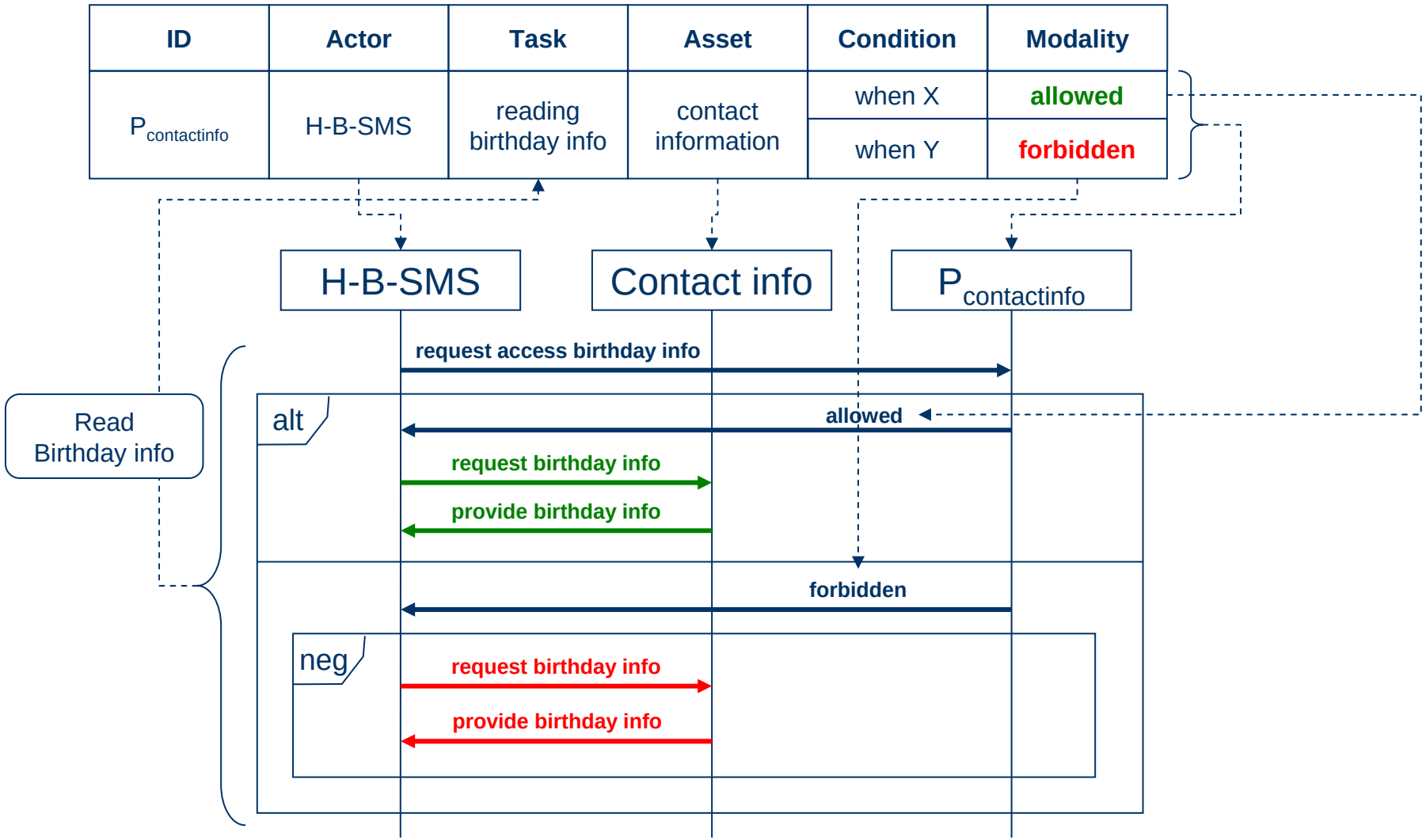
# Policy specification language

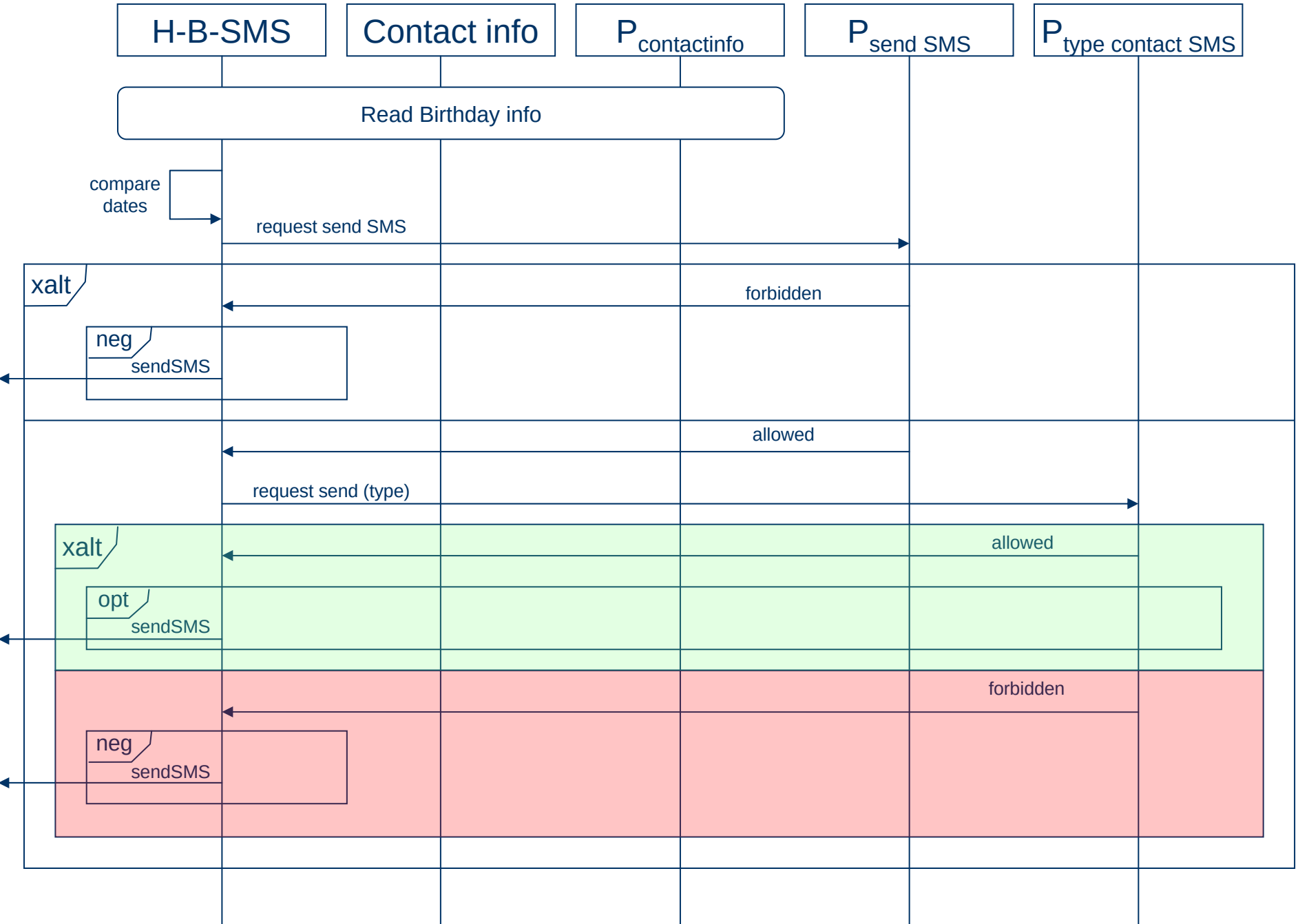
| ID | Actor | Task | Asset | Condition | Modality |
|---|---|---|---|---|---|
| $P_{contactinfo}$ | H-B-SMS | read contact info | contact info | when A | **allowed** |
| | | | | when B | **forbidden** |
| $P_{sendSMS}$ | H-B-SMS | send SMS | account credit | when X | **allowed** |
| | | | | when Y | **forbidden** |



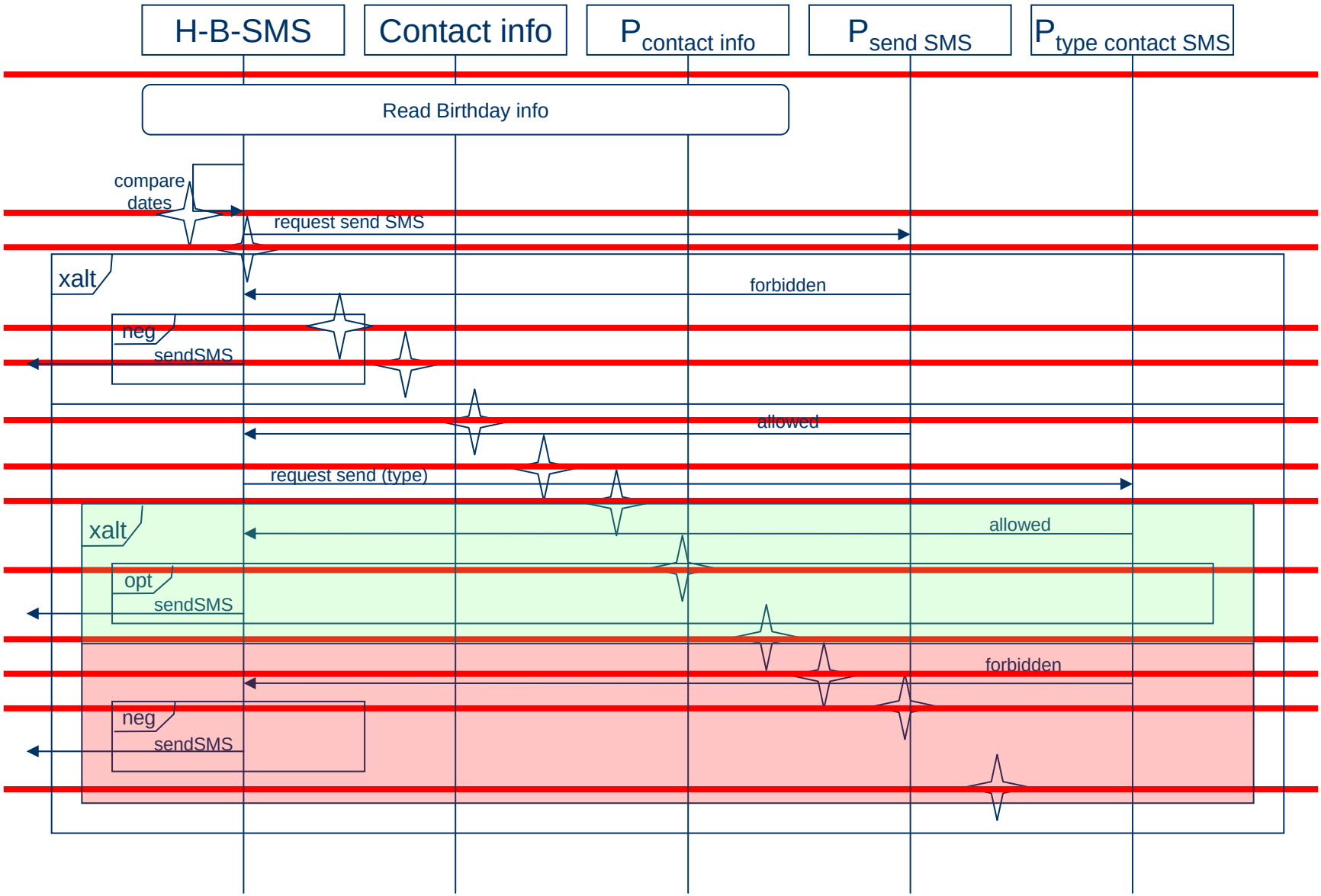
# Sequence diagrams

| ID | Actor | Task | Asset | Condition | Modality |
|---|---|---|---|---|---|
| $P_{contactinfo}$ | H-B-SMS | reading birthday info | contact information | when X | **allowed** |
| | | | | when Y | **forbidden** |

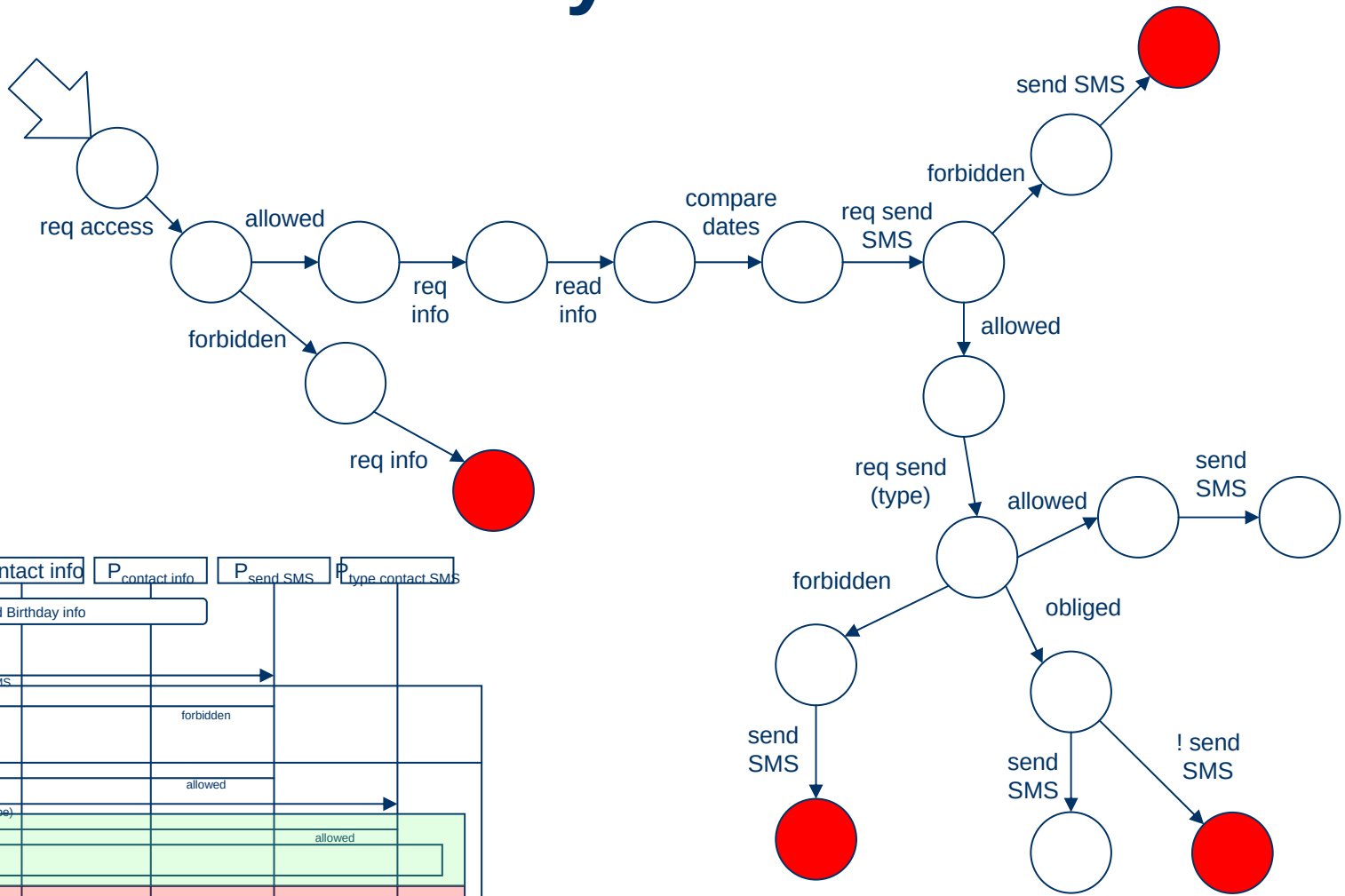



H-B-SMS
Contact info
P contactinfo
P send SMS
P type contact SMS
Read Birthday info
compare dates
request send SMS
xalt
forbidden
neg
sendSMS
allowed
request send (type)
xalt
allowed
opt
sendSMS
forbidden
neg
sendSMS

# Finding states in the Sequence diagram



# Generated Security Automaton



# From Policy to Contract

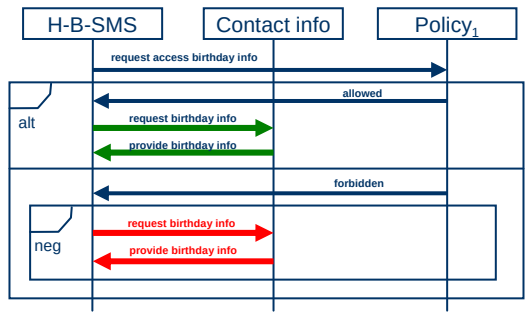
Specific Policy Specification

Policy structuring

| Actor | Task | Asset | Condition | Modality |
|---|---|---|---|---|
| H-B-SMS | read contact info | contact info | contact info opened for reading | **allowed** |
| H-B-SMS | send SMS | account credit | explicit permission from user | **allowed** |

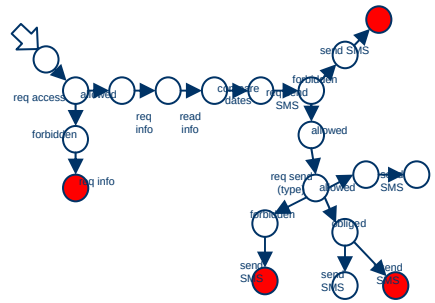
Policy Table

Modelling behaviour




Sequence Diagram

Semi-automatic generation




FSA

- Inline monitoring
- Static Analysis
- Proof carrying code

**”Contract”**

# Goals for the work

- Development of a framework for developers of mobile applications
- Security Policies shall be:
  - easy to identify and specify during the development process
  - alive and satisfied during the entire development process
- Quick and easy approval of finalised developed applications
- Increase trust in mobile applications developed by 3rd party companies

# Background


- S3MS-project
  - Subsidised by the EU
  - 12 partners:
    - Italy, Spain, France, Germany, Netherlands, Belgium and Norway
  - Duration:
    - March 2006 – Februar 2008
  - Budjet:
    - 4 M€
  - Website
    - www.s3ms.org