Location-sensitive File AccessControl

Atsushi Ito, Yasunari Harada

2011.12.10

An International Workshop on Linguistics of BA and The 11th Korea-Japan Workshop on Linguistics and Language Processing

Background

- For study of linguistics, we have to use books, DVDs, CDs etc.
- It is prohibited to copy them by copyright act.
- It is only allowed to use copies for education at a class.

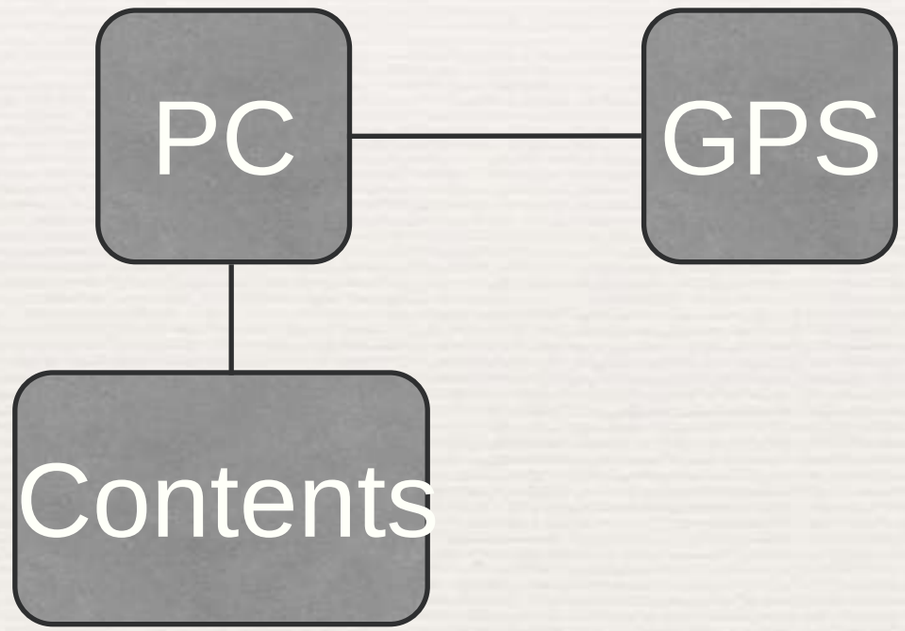
Problems

- Students are allowed to use contents in a school, university.
- Students have to study at home.

Solution

- Provide access control to contents for study
- Requirements: It should be allowed to use contents at registered location.
- Ideas to solve this problem.
  - (1) access contents server from home by on-line => problem of huge number of access and security to protect illegal access
  - (2) bring the contents to home => how to know the location?

Basic Idea



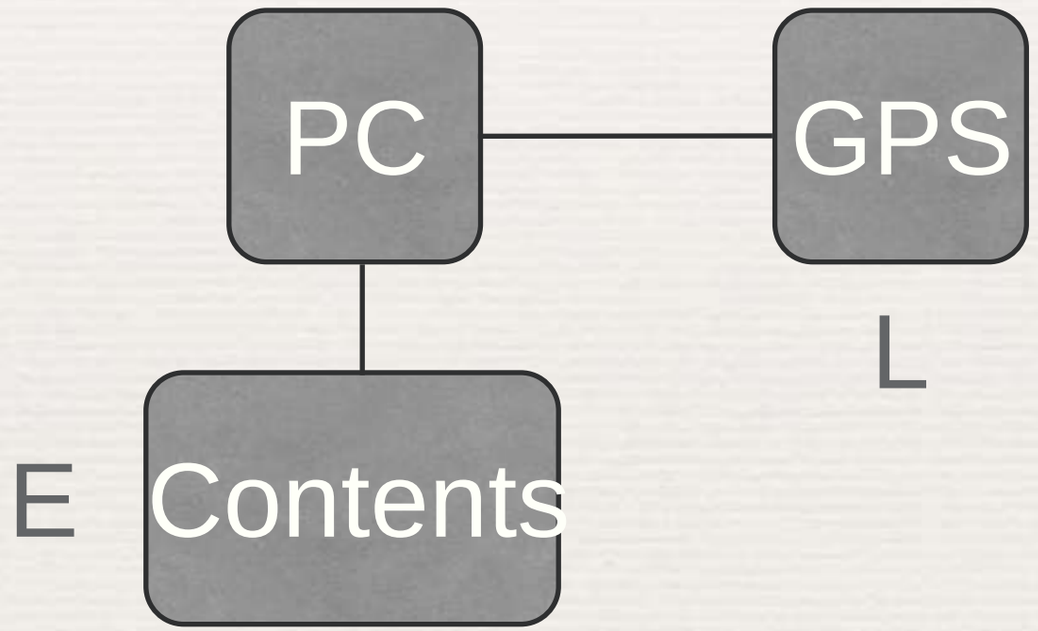
Detail of encryption

- E　a file　(contents)
- E　encrypted F
- L　location

- A(y,x)　y is encrypted by x
- Q(v,u)　decode v by u

- E = A(F,L)
- F = Q(E,L) = Q(A(F,L),L)

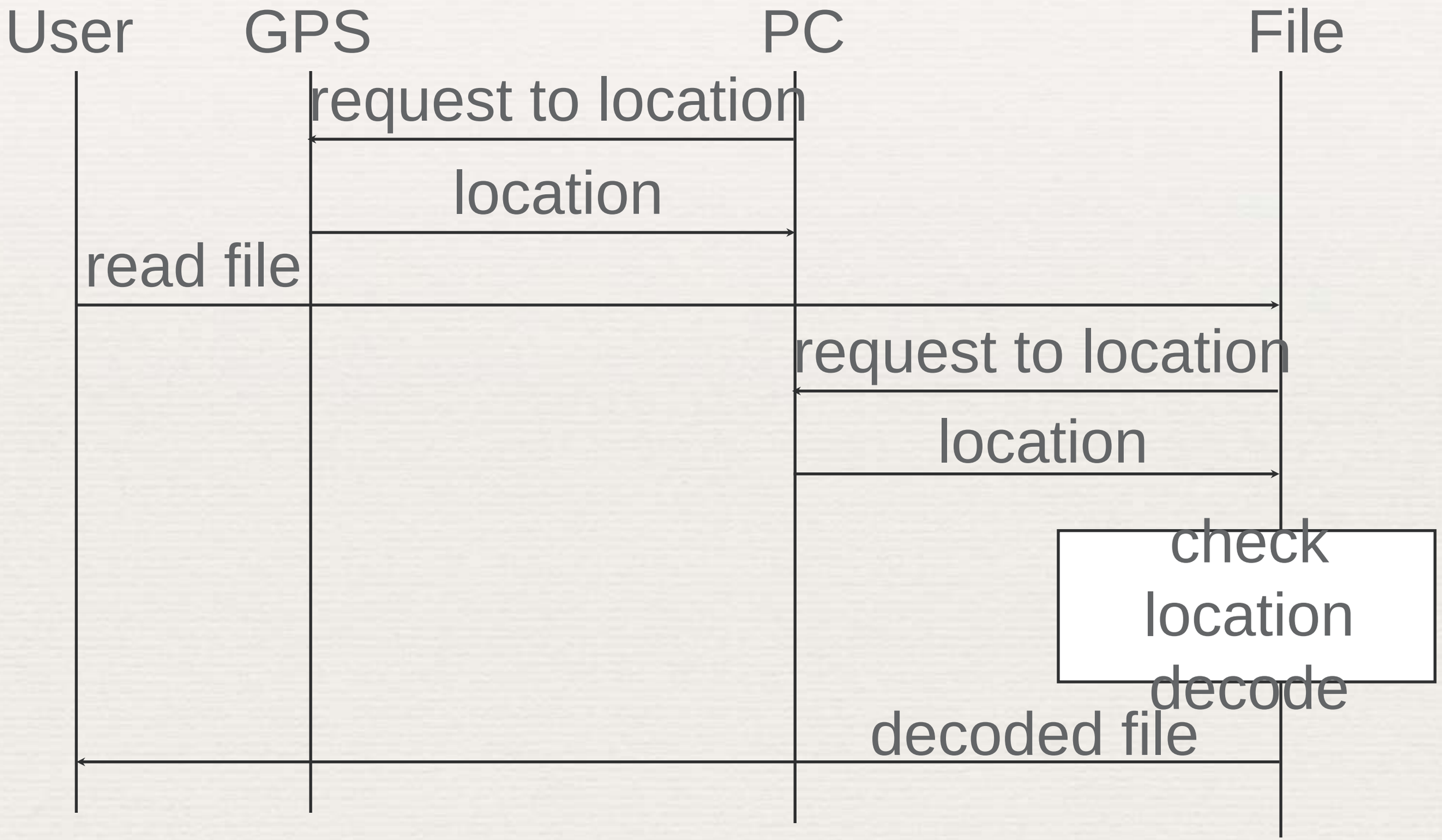
Basic Idea



Example

- Location (x,y)
- x=140.30.15 (longitude) y=40.10.30 (latitude)
- Key = f(x,y)
- f = x + y
- Key = 1403015401030
- E = A(F,L) = A(F, Key)

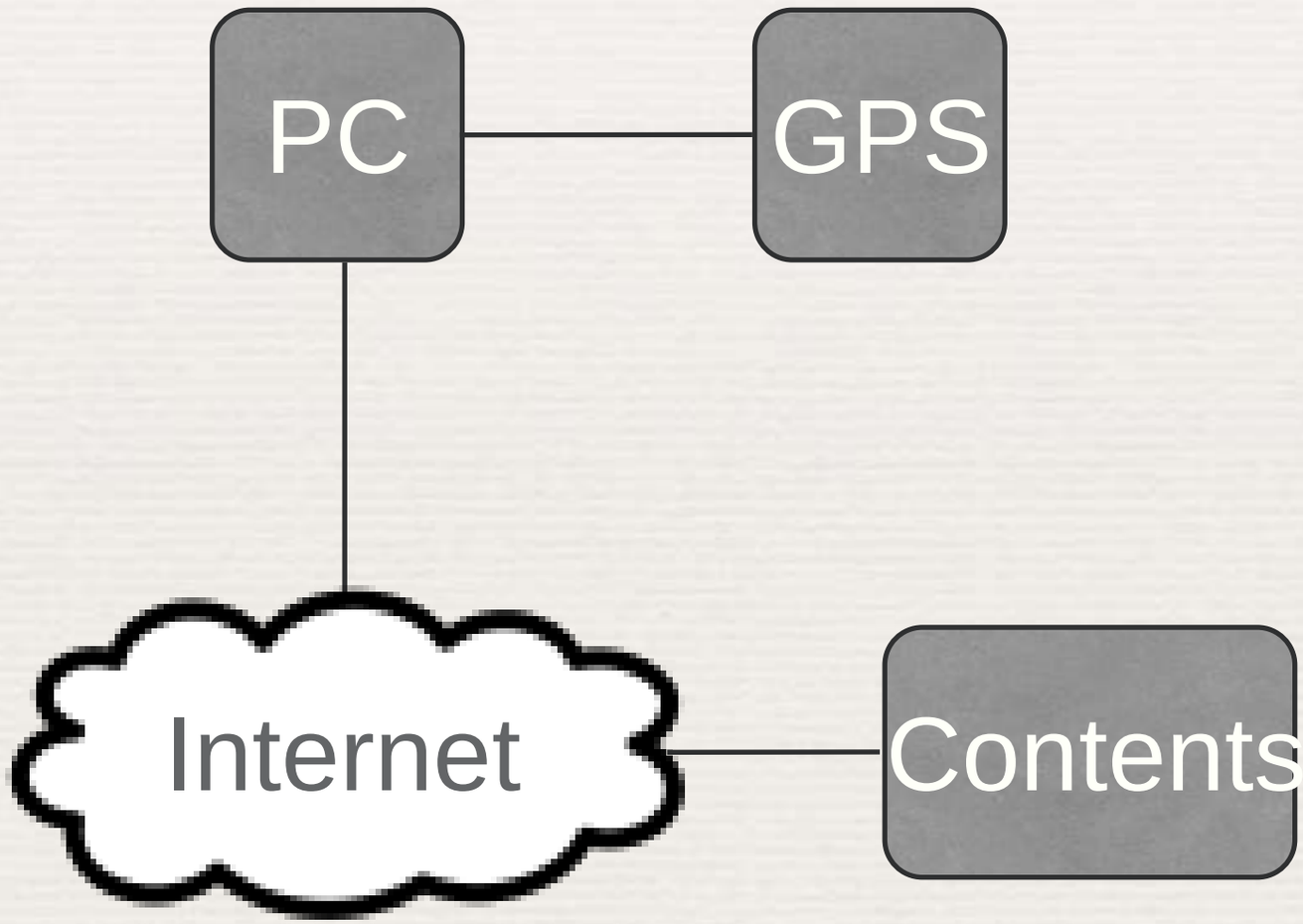
Sequence Chart



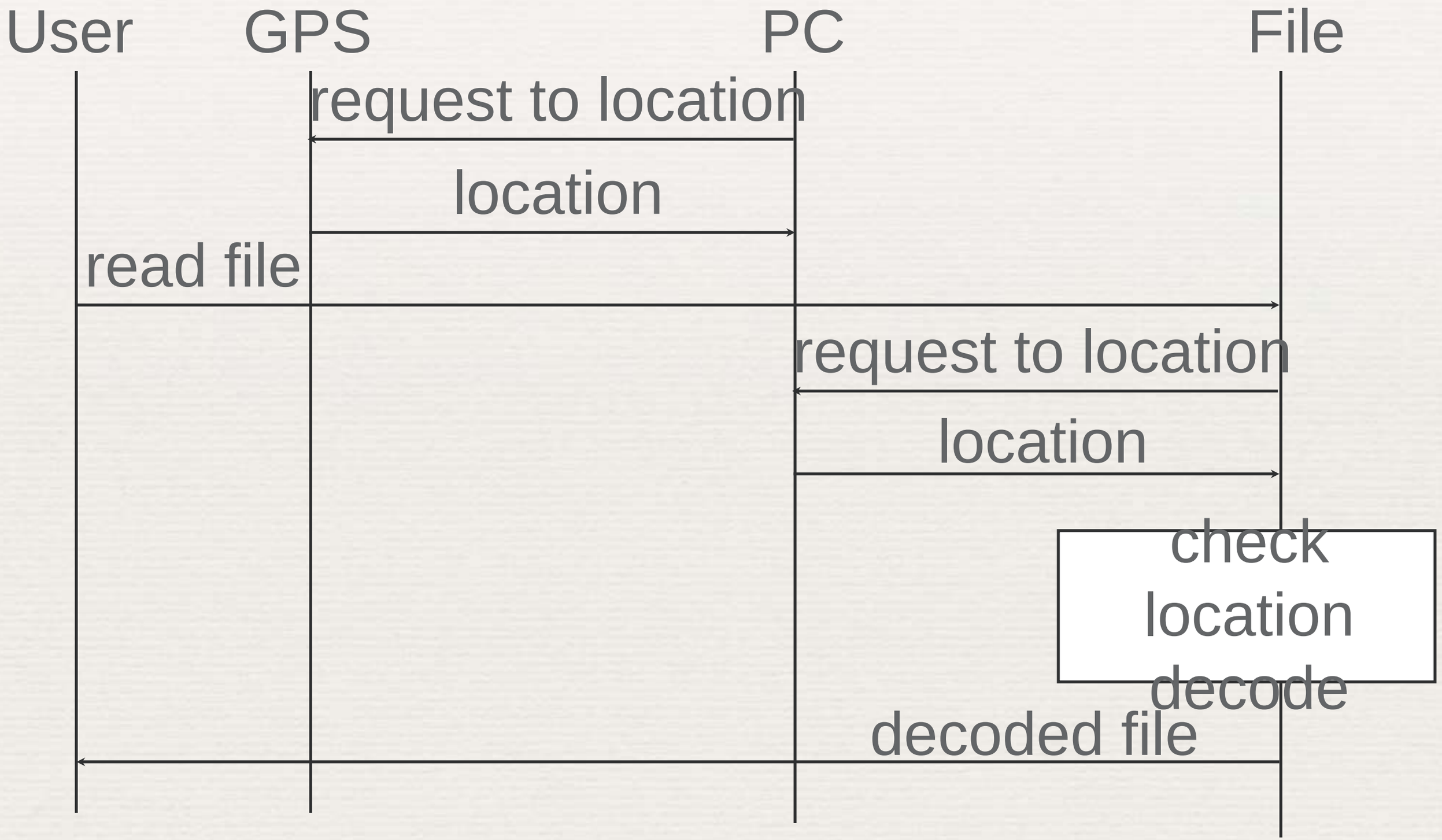
Multiple Location

- Li(i＝1∽n)
- Example:
- 3 locations　L1,L2,L3
- Encrypted key K＝G(L1)＝G(L2)＝G(L3)
- file E is encrypted by E＝A(F,K)
- decode by F＝B(E,K)

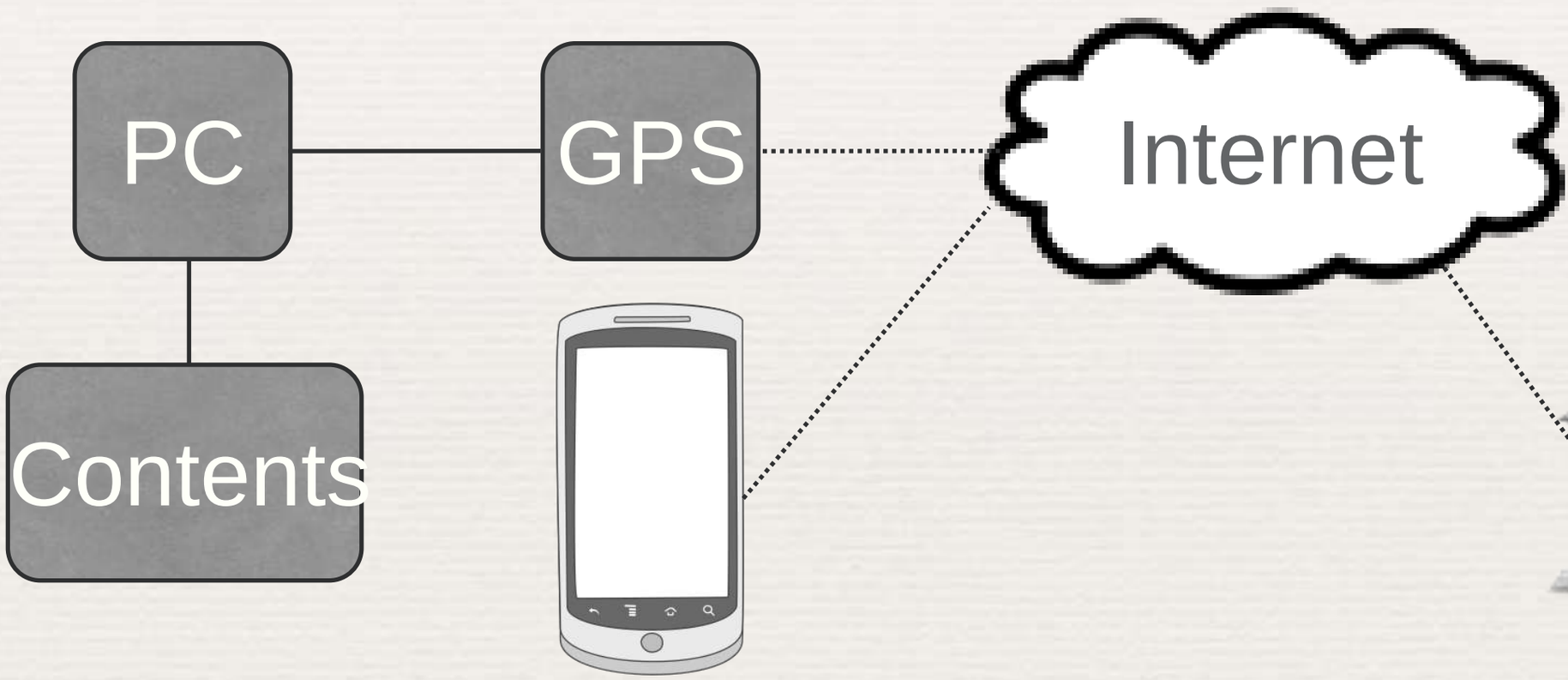
Remote Access



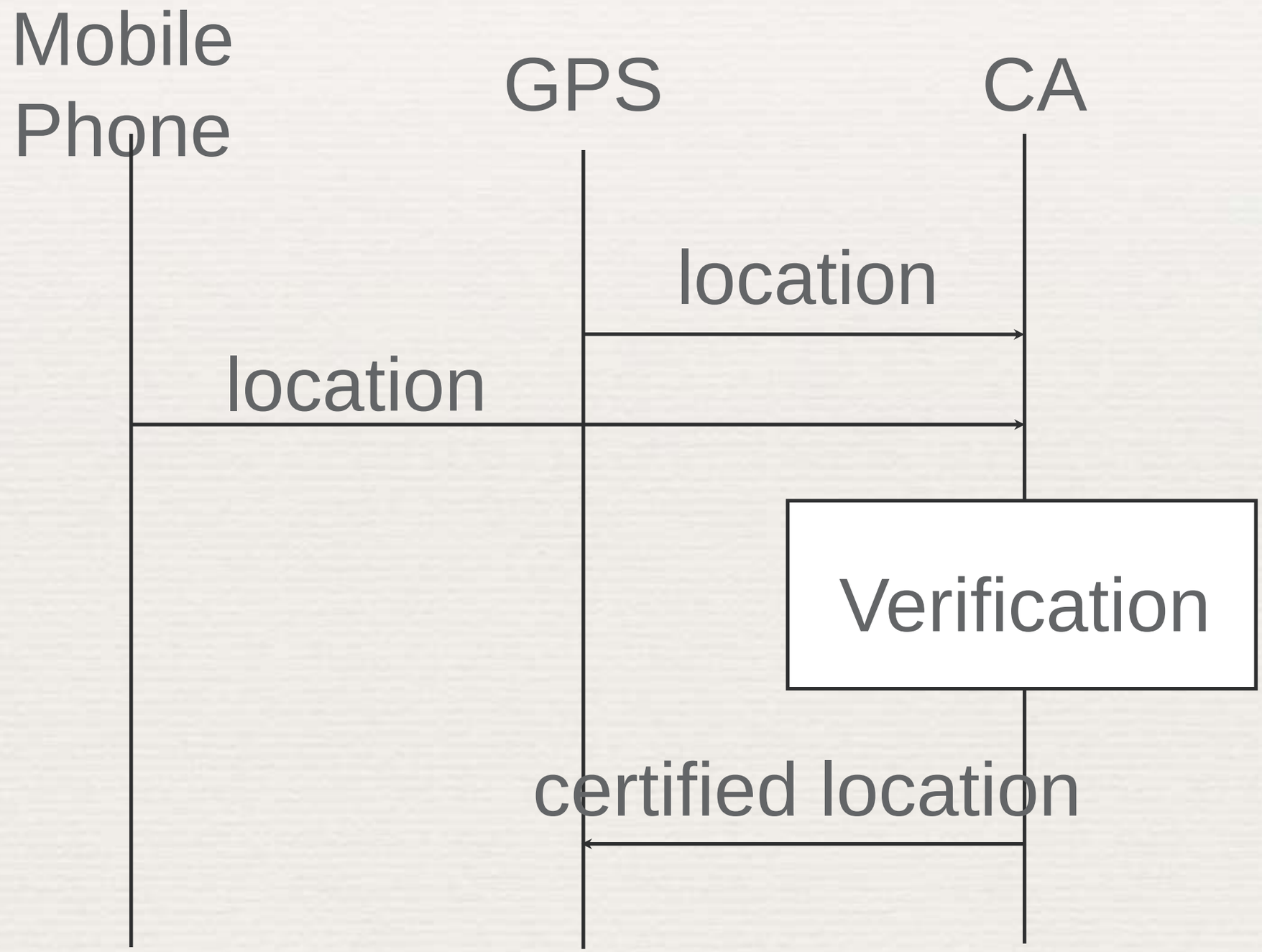
Sequence Chart



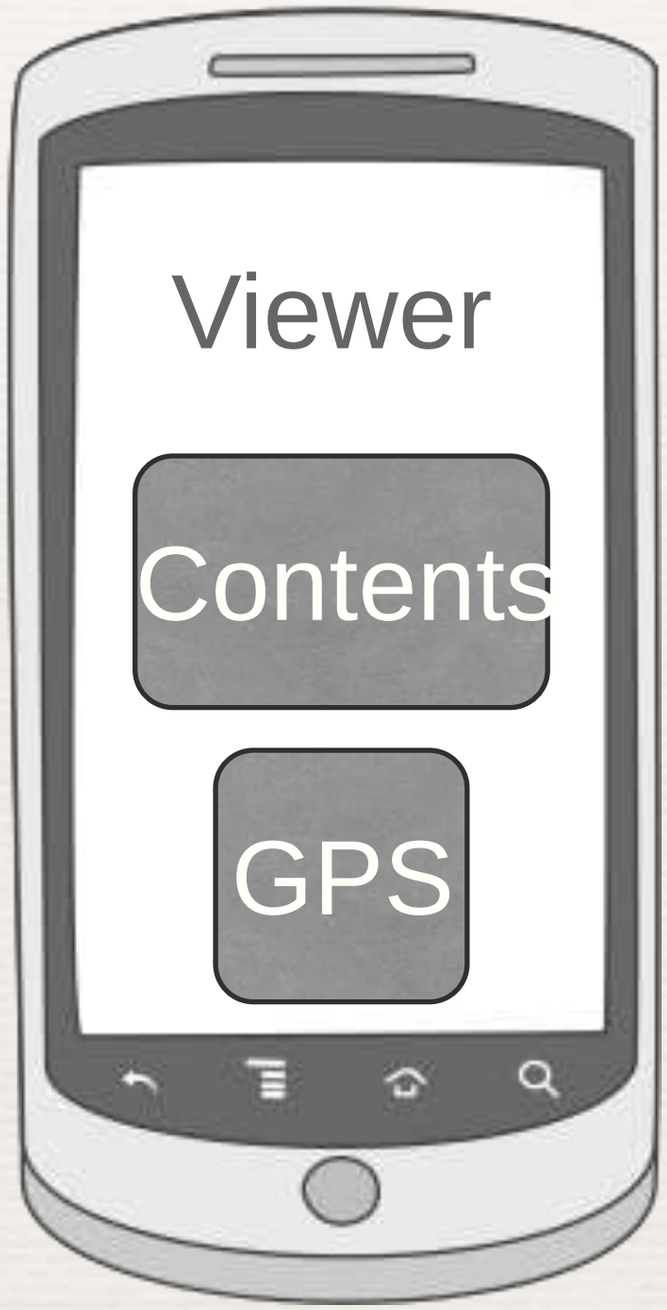
Safer System



Sequence Chart 2



Variations



Problems of ICT society

- A lot of information is stored as files.
- It is easy to access information.
- Problems of security and privacy

Other Applications

- Documents for secret meeting
- Medical Information
- Diplomatic documents
- Judicial documents
- Customer Information

- Thank you
- Q & A