Mobile Adventure

Non-repudiation for service accounting in ad hoc networks

Gina Kounga and Christian Schaefer

ASWN 07

DoCoMo Communications Europe GmbH
Landsbergerstr. 312
80687 Munich Germany

Outline

- Motivation
- Requirements
- Scenario
- Assumptions
- Accounting and Charging process
  - Registration
  - Selling/buying process
  - Authentication problems in ad hoc networks
  - A novel authentication solution
  - GenCAp solution
  - Generation of evidences
  - Discussion
- Conclusion

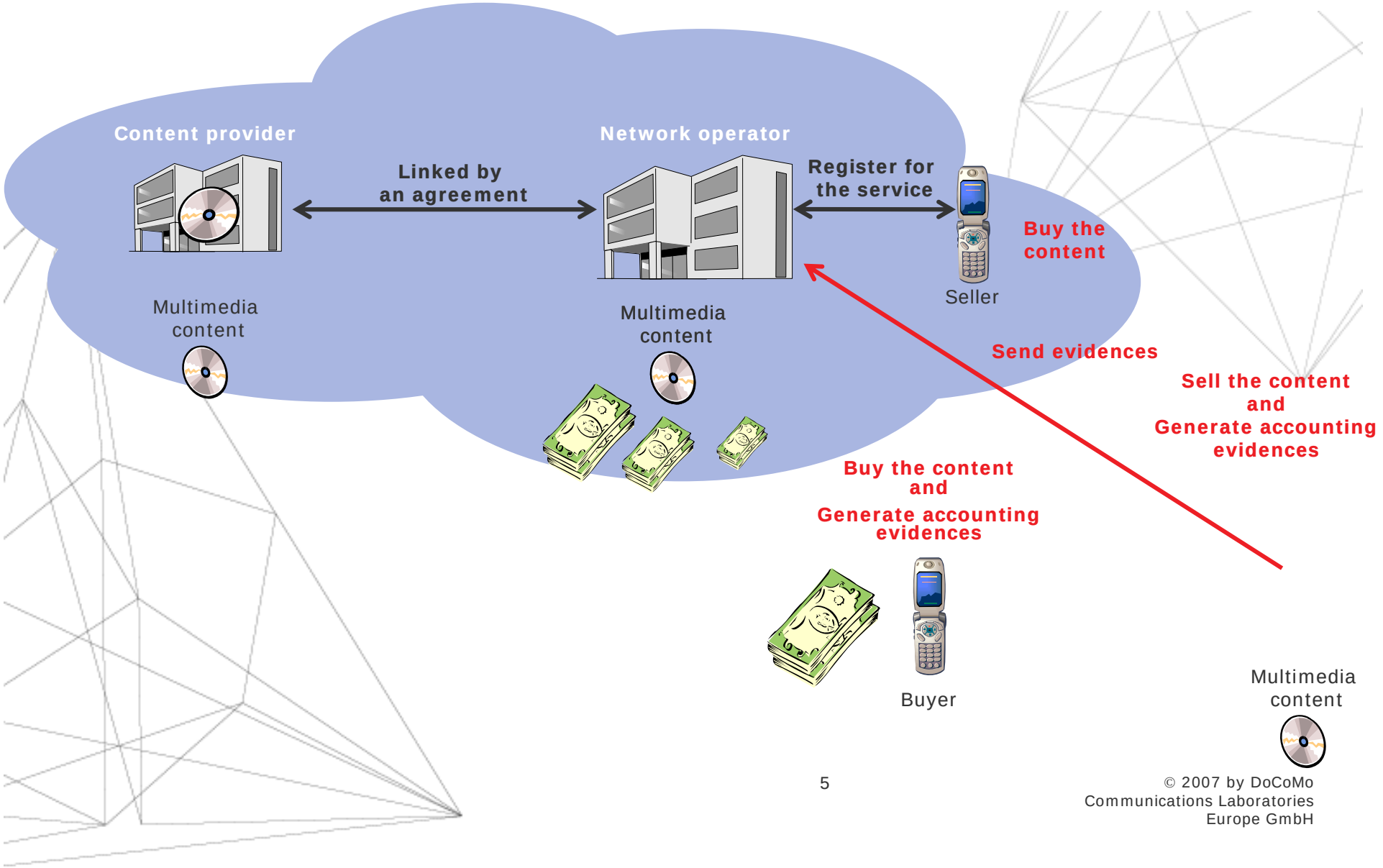
Motivation

- Millions of multimedia resources (songs, videos) are sold each year
- New distribution channels are defined to sell even more resources
  - Online stores, mobile networks, etc.
  - E.g. iTune Music Store : more than 2 billions of songs sold since launching in 2003
  - E.g. NTT DoCoMo Chaku-Uta, Vodafone live, etc.
- Ad hoc networks offer a new channel of distribution
  - Mobile user = potential buyer/seller
  - Multimedia resources can be bought
    - Everywhere
    - At any time
    - From anybody

Requirements

- Multimedia resources are often protected by property rights
  - Property rights should be obeyed
  - Owner of resource should be remunerated each time that a copy of the resource is sold
- User's interest is to be able to play the resource as soon as it is bought
  - A solution to provide authentication, authorization and accounting (AAA) must be defined
  - The selling and buying process must not rely on a trusted third party (TTP)

Scenario



Assumptions

- Ad hoc networks may not be connected to a fixed infrastructure
- Accounting evidences are
  - Generated in the ad hoc network and stored by devices
  - Transferred to the operator when a connection is available
- Multimedia resource Exchange System (MES) is installed in each device that :
  - Generates a copy of a resource
  - Generates a new license out of an existing one for that copy
  - Manages the resource encryption and transfer
  - Acts as a meter for the AAA system on the device
  - Transfers the accounting data to the AAA server
- Resource bought only after it has been completely received
- MES and AAA system are not in the scope of this work
  - They operate correctly
  - User can not change their behavior

Mobile Adventure

Accounting and Charging process

DoCoMo Communications Europe GmbH
Landsbergerstr. 312
80687 Munich Germany

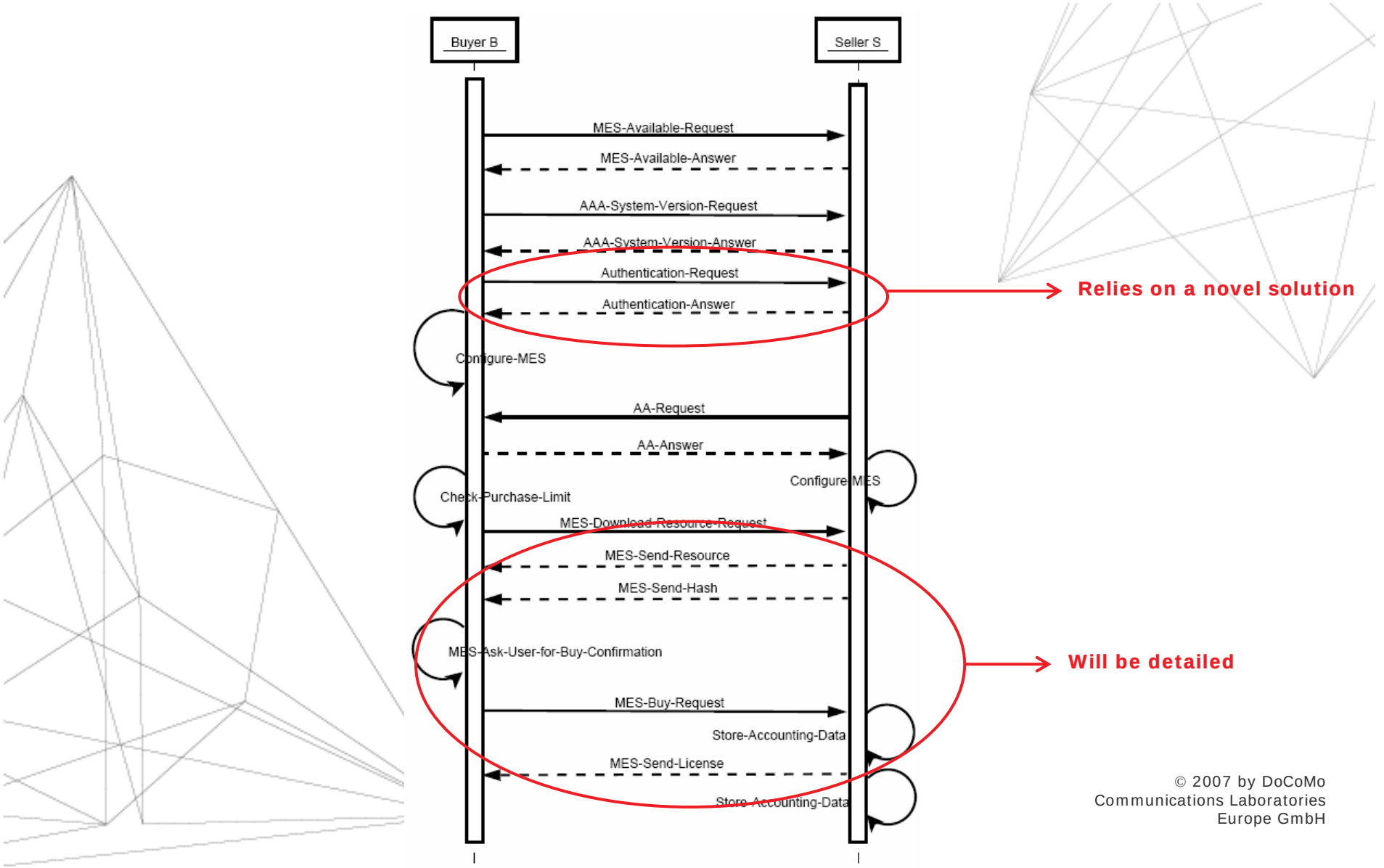
Registration

- Done once in the fixed network
- User concludes a contract with the operator that specifies
  - Whether user can sell, buy or sell and buy some multimedia resources
  - The purchase limit of the user
- User presents identification information that is verified by the operator
  - A unique ID is associated to the user
  - The required parameters are transferred to user's device

User's Certificate	Configuration data
• User identifier • User check value • Issuance time of the certificate • Identifier of the provider at which the user subscribed • Digital signature of the provider at which the user subscribed • Is user allowed to sell/buy multimedia resources	• Public key of the provider at which the user subscribed • Public keys of the other trusted providers • Which accounting information needs to be collected • Addresses of network operators AAA server • Is user allowed to sell/buy multimedia resources • Limit for buying resources

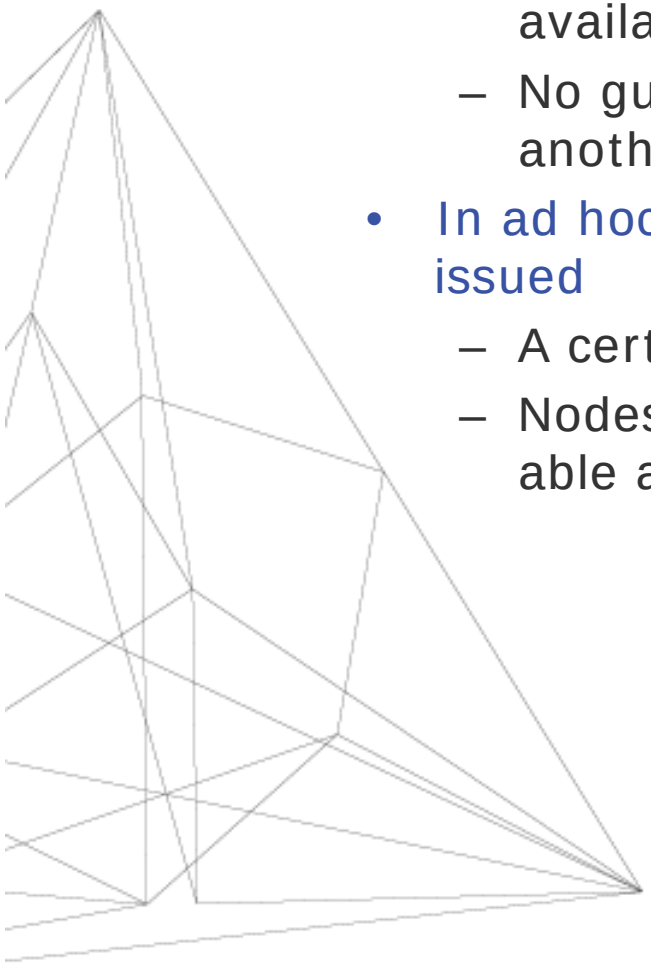
Mobile Adventure

Selling/buying process



Authentication problems in ad hoc networks

- In ad hoc networks, no guarantee that a public key was not revoked
  - Certificate revocation lists (CRLs) not always available
  - No guarantee that a certificate was not revoked in another ad hoc network
- In ad hoc networks, new certificates can not always be issued
  - A certification authority (CA) is not always reachable
  - Nodes that have revoked their certificates may not be able anymore to use public key cryptography



A novel authentication solution

GenCAp* solution is used

- It defines a one time password approach for public/private key pairs
- Public/private key pairs are only valid if they are used at the right time
- Nodes can generate valid certificates from a unique certificate issued at registration by the CA
- The authenticity of these certificates can be verified with the CA's public key

* Generating CA-authenticated public keys in ad hoc networks (G. Kounga, C. Mitchell, T. Walter)

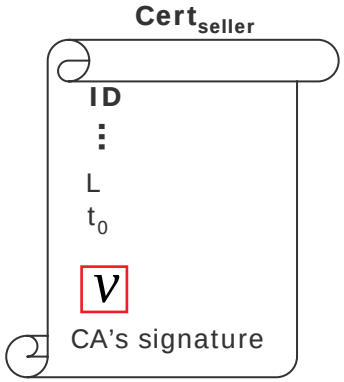
GenCAp solution (1/2)

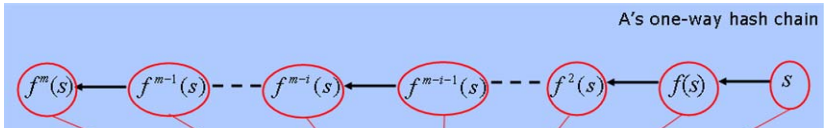
Public values

- m
- g
- f
- h

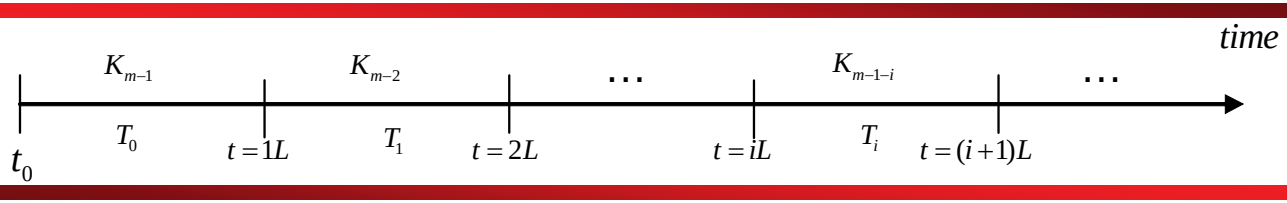
Secret s is generated from a pass-phrase

Registration



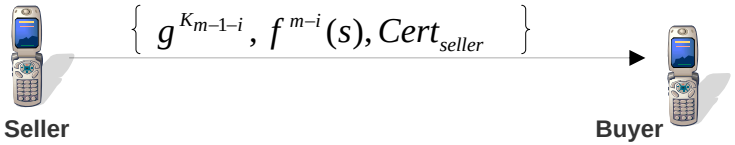


$$v = h(g^{\prod_{j=0}^{m} f^j(s)})$$



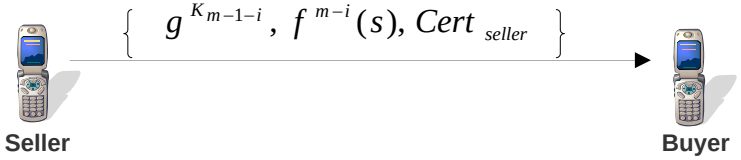
Authentication message

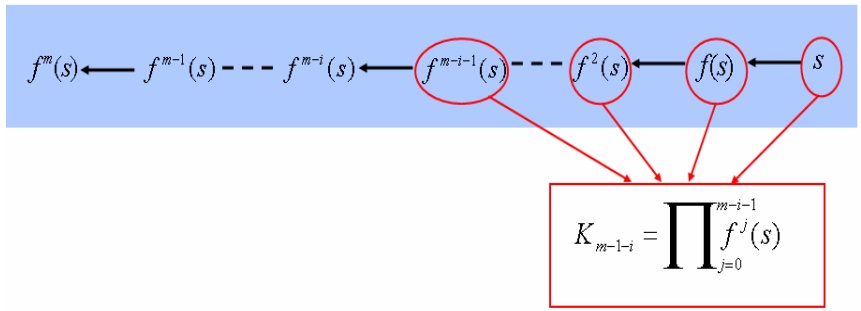
In time interval $T_i, 0 \le i < m$



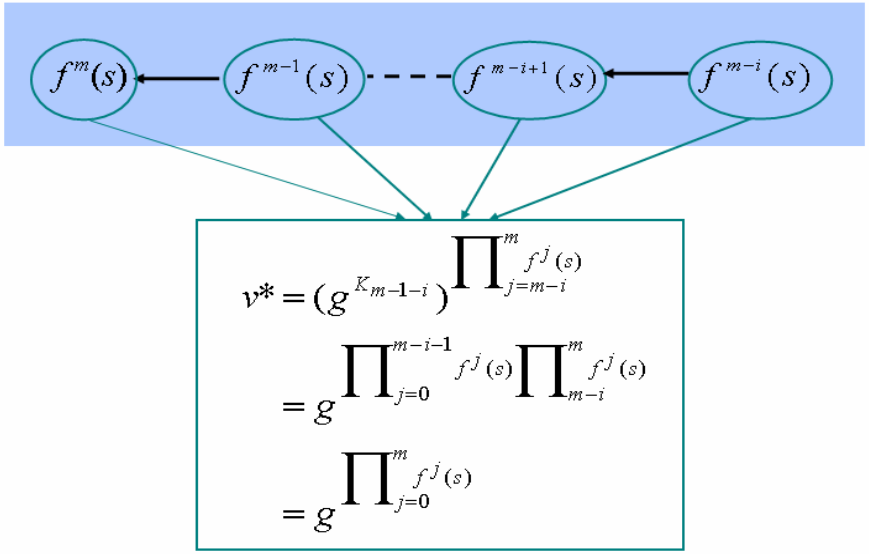
GenCAp solution (2/2)

In time interval $T_i, 0 \le i < m$



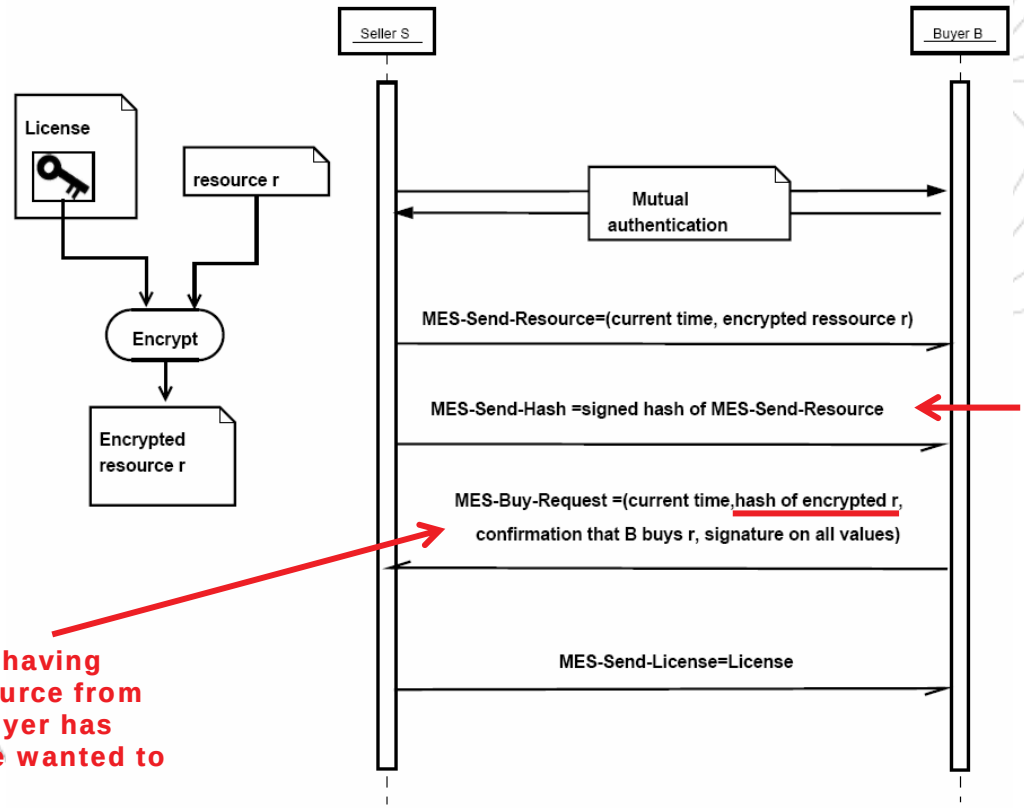


Verification of the public key's validity



If $v = h(v^*)$, then $g^{K_{m-1-i}}$ is a valid public key

Generation of evidences



The buyer can check that he received the complete encrypted resource from the seller

Proves that after having received the resource from the seller, the buyer has confirmed that he wanted to buy the resource

Discussion: What if ...

- The buyer claims not having received the license
  - To receive his remuneration, the seller must send a copy of the license to the operator
  - The buyer can request the license from the operator
- The buyer claims that he did not agree to buy the resource
  - The confirmation message received by the seller is signed with the buyer's private key
  - The buyer needs to enter his pass-phrase to generate his private key
- The seller does not report to the operator that he has sold a resource
  - Seller is only paid if he reports that he has sold a resource
  - The remuneration should be interesting enough to increase seller's incentive to be honest

Conclusion

- Non-repudiation for service accounting in ad hoc networks
  - Selling/buying of multimedia resources
  - Accounting and charging for the service
- Additional interesting features
  - Buying process does not rely on any third party
  - Relies on GenCAp novel solution that extends one time password to public/private key pairs
  - Permits the instant use of bought multimedia resource
  - Can be used for Selling/Buying other digital resource, e.g.:
    - Tickets (Concerts, Movies, etc.)
    - e-Books and e-newspapers

Mobile Adventure

Thank you for your attention!

DoCoMo Communications Europe GmbH
Landsbergerstr. 312
80687 Munich Germany