
SECURE
SIMPLE
EFFICIENT

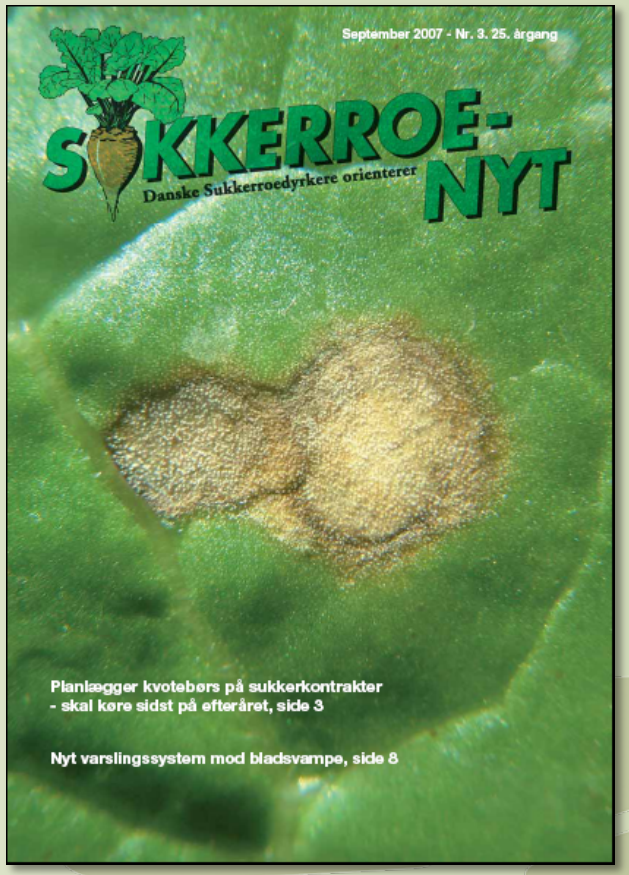
Jakob I. Pagter

# USING MARKET DESIGN AND CRYPTOGRAPHY TO ENABLE NEW BUSINESS

# Cryptography meets Economy

# 5 (five!) years later

- Three PC's on LAN computes clearing price based on apx. 2400 encrypted bids which are *never* decrypted.
- Finally – a market clearing price and the amount of quota that each farmer must sell/ buy – the result is decrypted
- Following, the production rights (quota) for 25000 tons of sugar changes hands

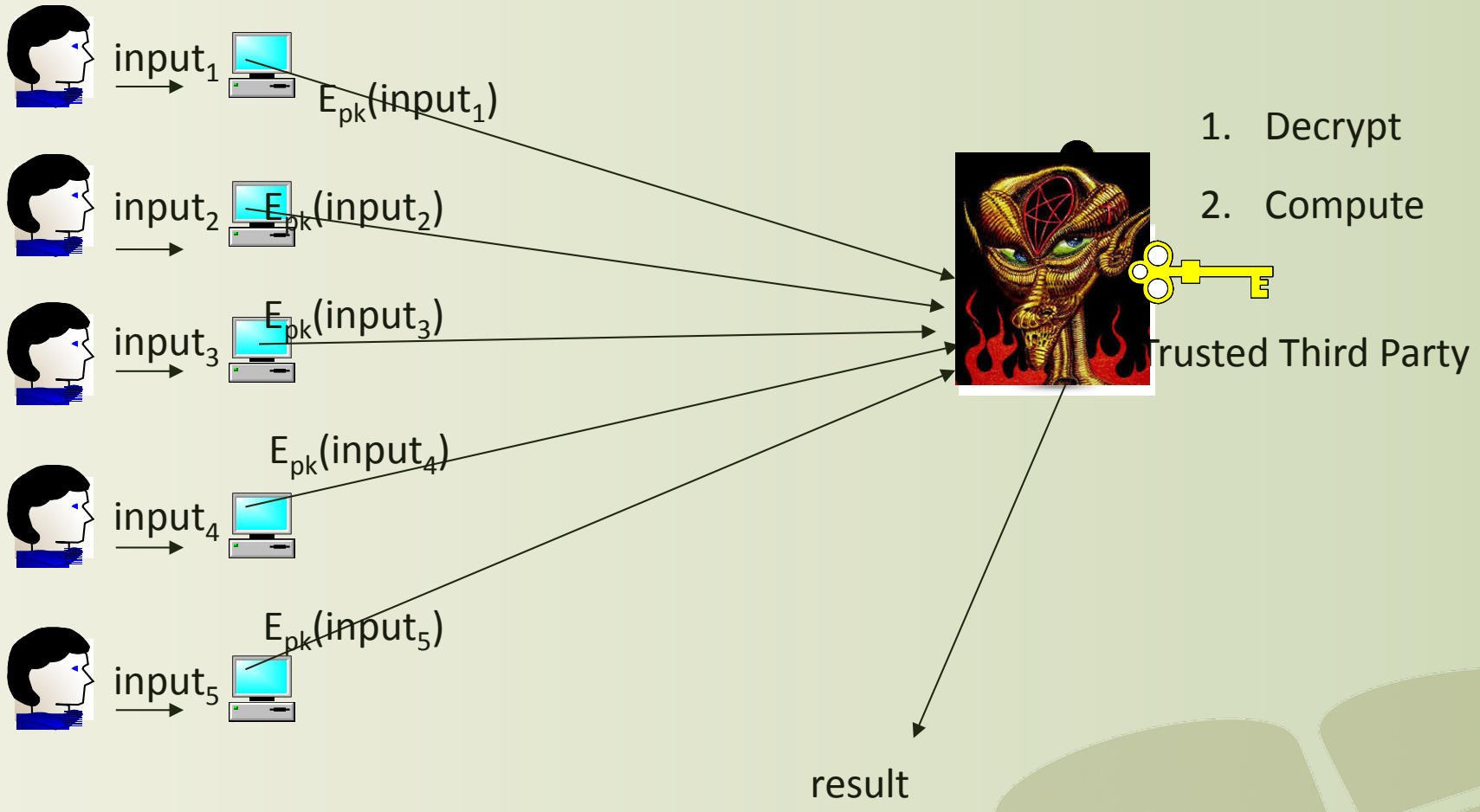


# Public-key cryptography

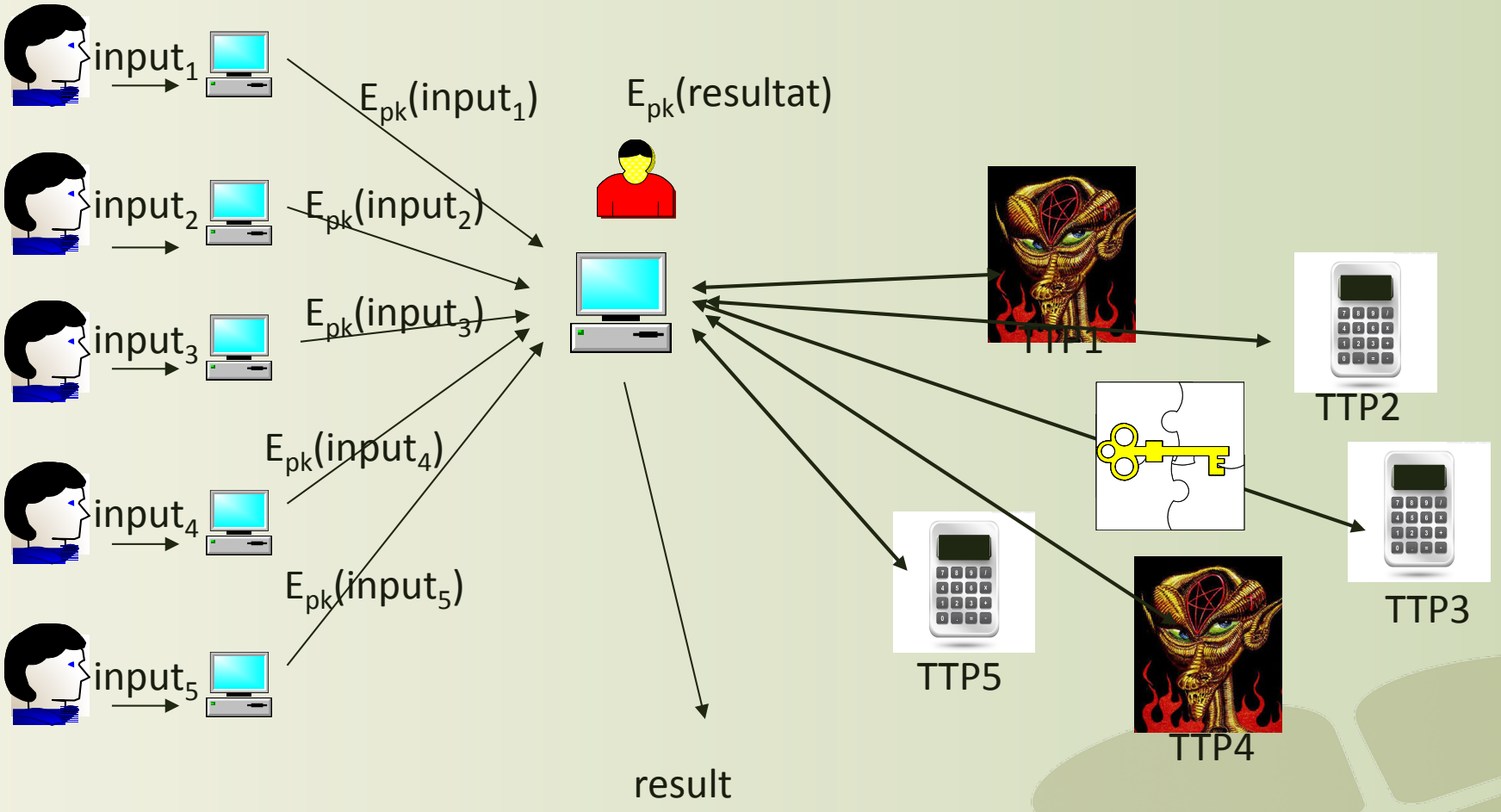
- Sender and receiver has key pair: one for encrypting and one for decrypting

- Ex: padlock
  Everybody can shut the lock (encrypt) but only the holder of the matching key can open the lock (decrypt)

# “Shallow” confidentiality



# “Deep” confidentiality



# Back to the sugar beets

- Grown and sold to Danisch based on EU quotas (like fish, milk, etc.)
- Untill 2007/2008 trading of quotas has been done by bilateral trades facilitated through paper ads, personal connections etc.

- One out three factories shut down and guaranteed prices lowered => a lot of growers near shut down factory who wishes to sell
- Theoretical analysis indicate that a central exchange could
  - Increase turnover with as much as 400%
  - Ensure almost full use of entire national quota (less than 50% use without re-allocation)

# An exchange (double auction)

- All growers submit one or more bids on the form
  - Buy (maxprice, volume)
  - Sell (minprice, volume)


- Aggregated demand (supply): Total volume bought (sold) at given price

- Market Clearing Price: the price where supply equals demand

- *This auction design and market size makes it optimal to bid truthfully, which ensures that all preferred trades are realised.*

# Tillidsproblem

- Optimalt for dyrkerne at byde ”sandfærdigt” i henhold til deres indtjeningsevne
- Danisco kan potentielt udnytte viden om dyrkernes indtjeningsevne
- Danisco ønsker samtidigt at kontrollere handlen med kvoter, pga. udestående gæld mv.

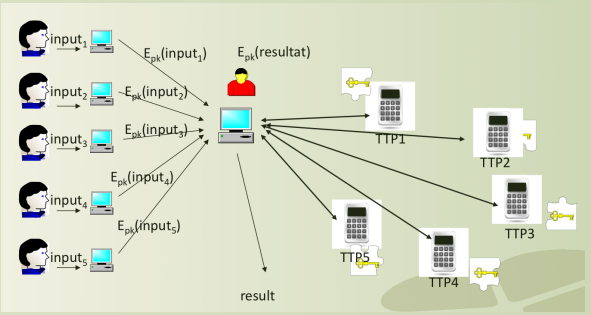
**Modstridende interesser!!**

  - Dyrkerne ønsker ikke at Danisco kan se bud
  - Danisco har behov for at kontrollere budene

- Hvordan kan gevinsterne ved en central børs realiseres?!

# Trust problem

# Systems architecture




Danisco

SIMAP web-server

DB

session

log-in

Java-applet

Encrypted bid(s)

grower

**bidding**

Us

DB

LAN

DB

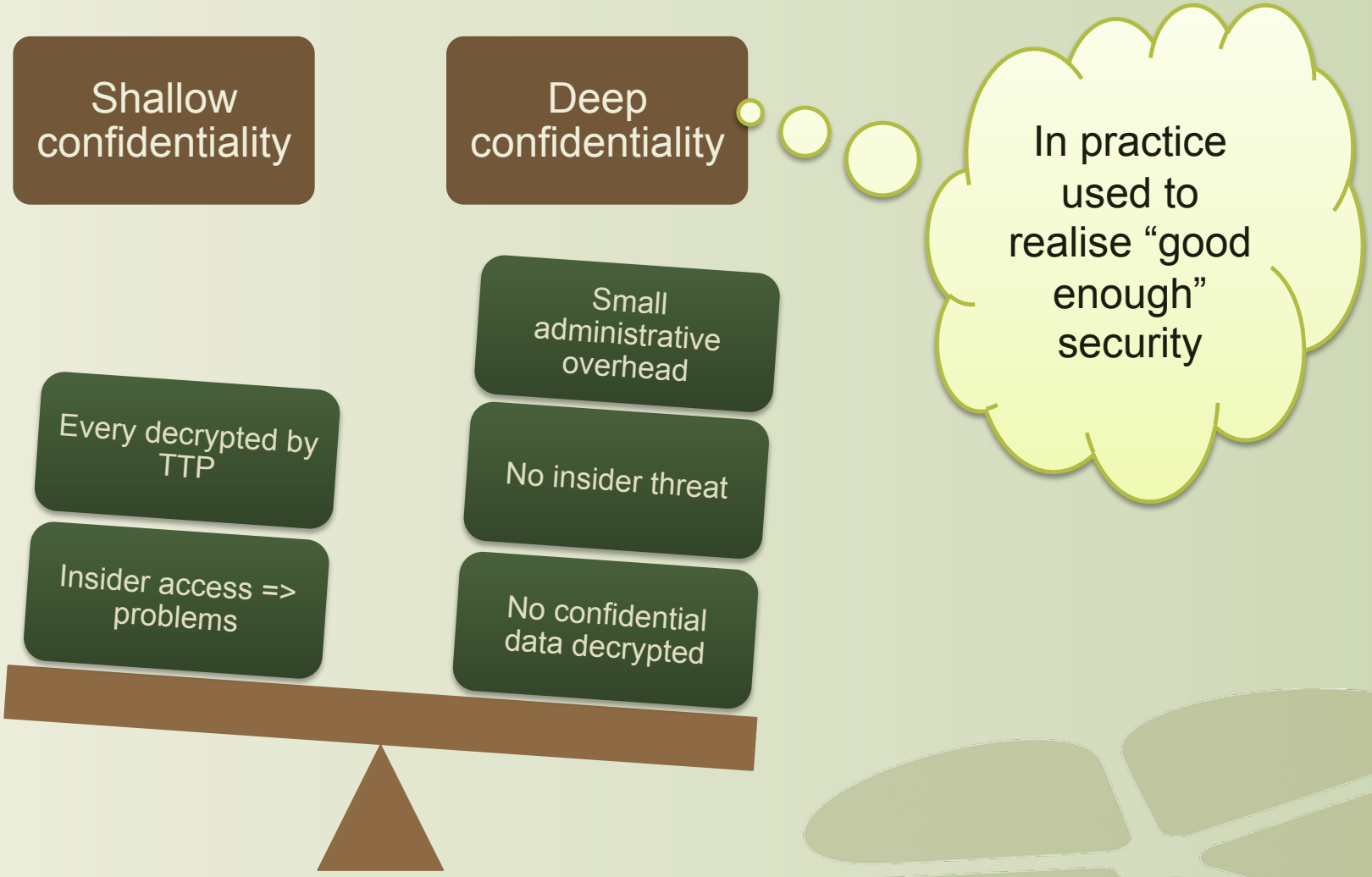
Grower representative

Danisco

DB

**clearing**

# Enabling new business with SMC



# Cloud computing

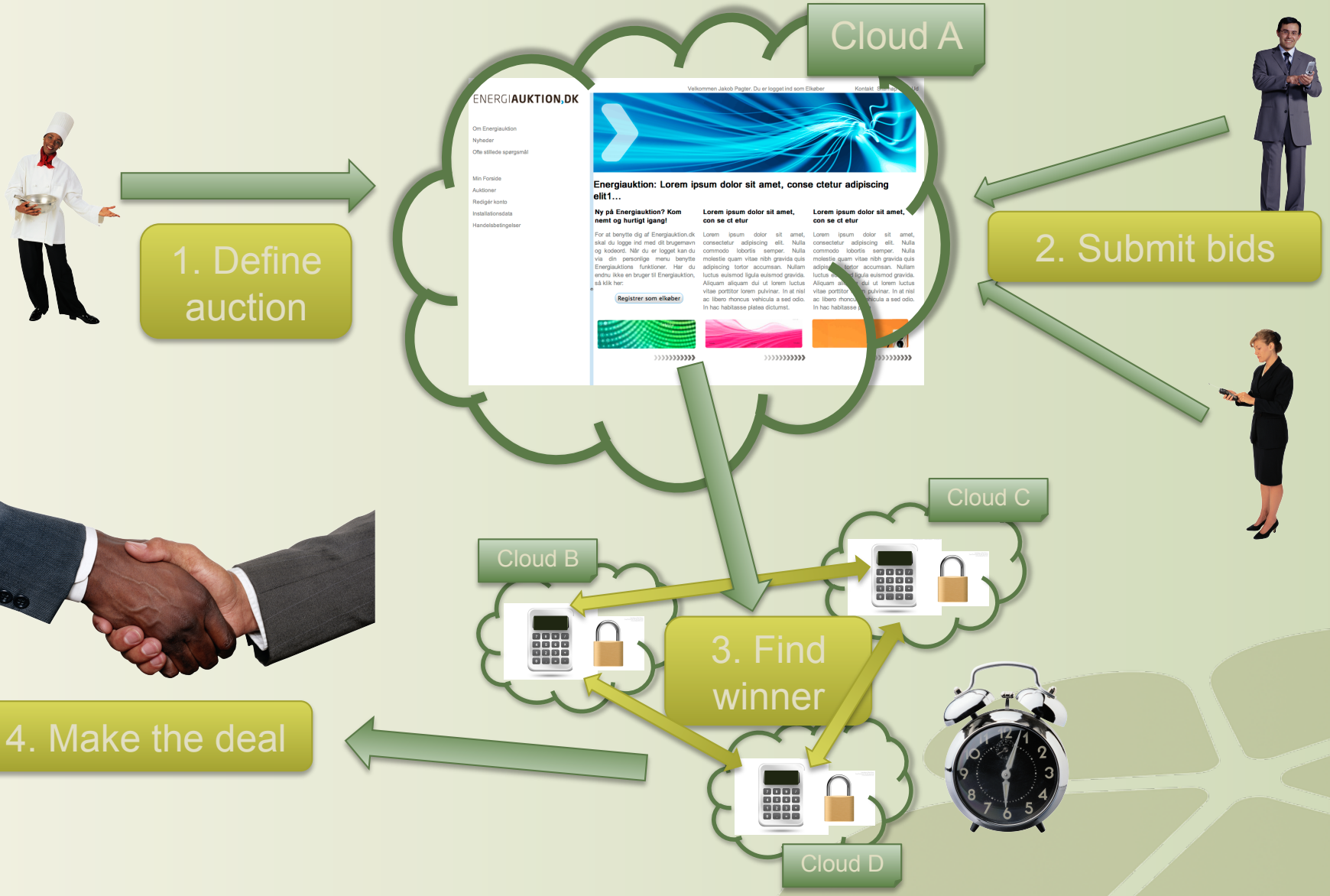
## Cloud Computing

- Cheap (economies of scale/pay-by-the-drink)
- Elastic
- Innovation catalyst
- Maybe more secure…?

## Types (NIST)

- IaaS – Infrastructure-as-a-Service
  - Amazon Web Services
- PaaS – Platform-as-a-Service
  - Microsoft Azure
- SaaS – Software-as-a-Service
  - Google Apps

# Auctions-as-a-Service (“SaaS”)



# Mechanism design with SMC

## Security

- Confidential data never decrypted
- “Good enough”-security

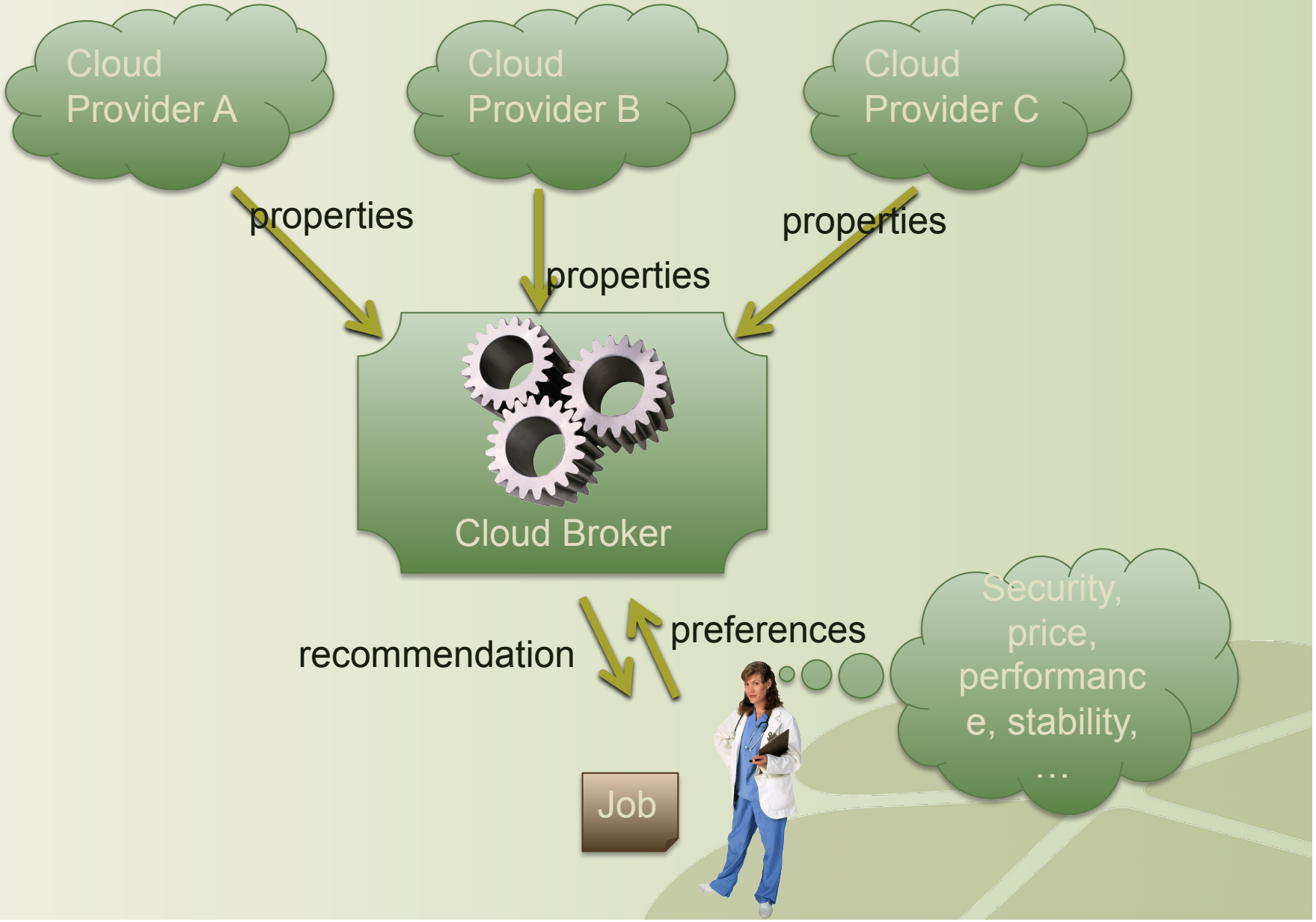
## Simplicity

- Security policy reduced to “protect your key”
- Small TCB!

## Efficiency

- Manuel procedures replaced by computers
- Cloud-enabled

# Cloud brokering (a CFEM-topic?)



# Questions?

jip@partisia.com
www.partisia.com