Veilig & Betrouwbaar

ICTDELTA 2012

Risks and Gains in Green ICT

Outline

- Who is that guy?
- Risks and Gains: two sides of one and the same medal
- Smart Design = … + … + …
- Smart Homes
- Smart Energy Infrastructure
- Smart Metering
- The future of Green ICT

Who is that guy?

- Open University: Professor Software Technology (0.3 fte)
- Radboud University: Digital Security Department (0.7 fte)
- Scientific Director of LaQuSo Nijmegen
  - Security and Privacy Assessments and Advice
  - Responsible for many security and privacy risk assessment projects in the areas of smart meters, smart grids and smart homes.
- Programme Leader of OU Master Software Engineering
  - Distance education, 60 EC, Academic Master of Science
- Research in Sustainability, Security and Correctness
- Member of the Scientific Advisory Board of IIP Sustainable ICT
- NEW: Scientific director of SIEnergyLab
  - Sustainable ICT and Energy Research Laboratory

SIEnergyLAB

SUSTAINABLE ICT & ENERGY RESEARCH

- Initiative of 5 yr old IIP Sustainable ICT (with Roel Croes)
- Operate on national level based in location Nijmegen, RU
- Initiate and perform research on Sustainable ICT and Energy
- Focus on research applicable in practice
- Collaboration between Science, Government, & Industry
- Improve image and visibility of ICT for sustainability
- www.sienergylab.nl

Risks and Gains
Two sides of one medal!

ICT for Sustainability
- New intelligent ways to control systems using ICT
- Based on newly collected data

High Gains:
- more intelligent control, less energy consumed

High Risks:
- cyberwar, terror, blackmail, more global impact of incidents, security risks, privacy risks

Gains, and Risks…?

- Intrinsic-ID, key to securing your digital life
- Planning and Control in Smart Grids
- De groene auto is slim!
- A global hydrological model for real-time flood management
- Zelforganiserende ICT Systemen
- Intelligent Robots: Cyberphyisical systems for the future
- Onze digitale samenleving is op het niveau van het Wilde Westen

The need for Smart Systems

We need safe (secure and reliable) sustainable systems:
high energy gains and low security and privacy risks

1. Green by Design
   - Decrease energy consumption
2. Secure by Design
   - Safe to use, well secured, NO security through obscurity
3. Privacy Friendly by Design
   - NOT: first collect, then protect; BUT: first select, then protect!
   - Clever crypto-protocols

SMART DESIGN = GREEN + SECURE + PRIVACY FRIENDLY

Preferably also correct by design: formally proven algorithms

Smart Homes

GoGreen
- *Rody Kersten, Sjaak Smetsers, Marko van Eekelen*
- Greener house through a self-learning, privacy-aware user-centric energy-aware wireless monitoring and control system
- AgentschapNL IOP Generieke Communicatie
- Collaboration of RU Nijmegen with UTwente, TU Delft, Saxion, Novay, Ambient Systems and iSensus

Go-Green

Monitoring

•Read sensors (light, movement, temperature, CO2, …)

•Gather information from on-line agendas, GPSs, …

Learn

•Who lives in a house, who is where, doing what, what are their preferences, …

Control

•Heating, ventilation, air-conditioning, lighting, sunscreens, appliances, ...

Smart, Secure, Wireless

- Secure communication between wireless sensor nodes
- Encryption requires key distribution or agreement for new sensors (*pairing*)
- Wi-Fi Push-Button Configuration (PBC)
  - User presses a (virtual) button on one device
  - Then presses the button of the other device within 120 seconds
  - Security lies in physical access to the devices
  - Vulnerable to several attacks:
    - collision, capture effect, timing control

Solution: Tamper-Evident Pairing?

*MIT, **Secure In-Band Wireless Pairing**. Usenix Security, 2011*

•Sending a packet of fixed (large) length, means energy on channel

•Not sending a packet means no energy, unless others are transmitting

•On/Off slots, can be used as bits

Done:

•Verify security of simplified version using Uppaal model-checker

Current work:

•More thorough formal verification using SPIN model-checker and ACL2 theorem prover

Smart Energy Infrastructure

Secure and Privacy Friendly Smart Grids

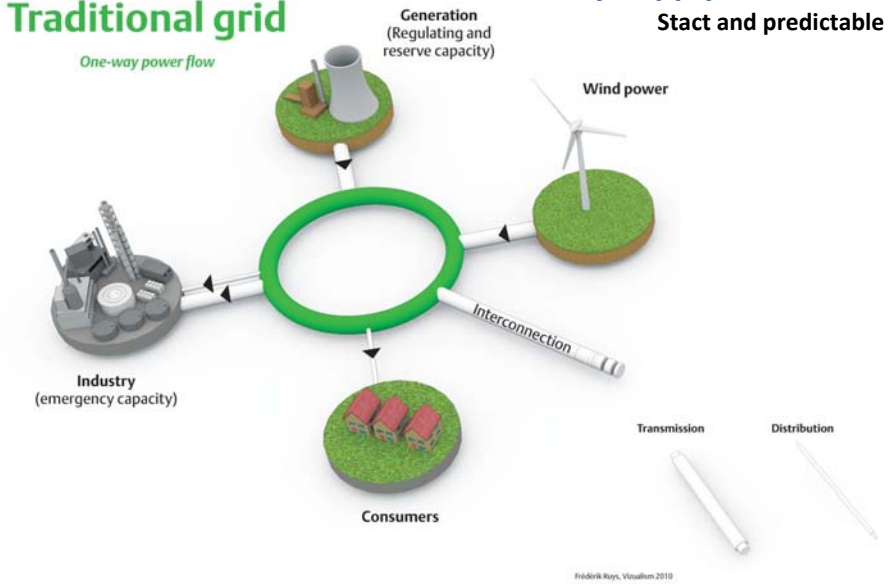
•Carlos Montes Portela (Enexis), Marko van Eekelen

•Smart Designs of Smart Grid Infrastructures

•Collaboration of Enexis and Open University of the Netherlands

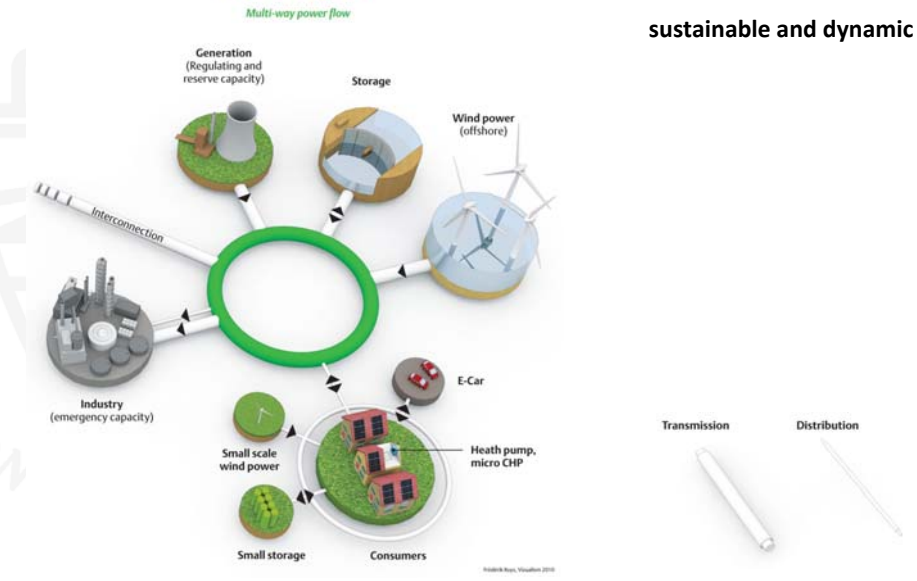
Electricity Supply anno 2012

Stact and predictable



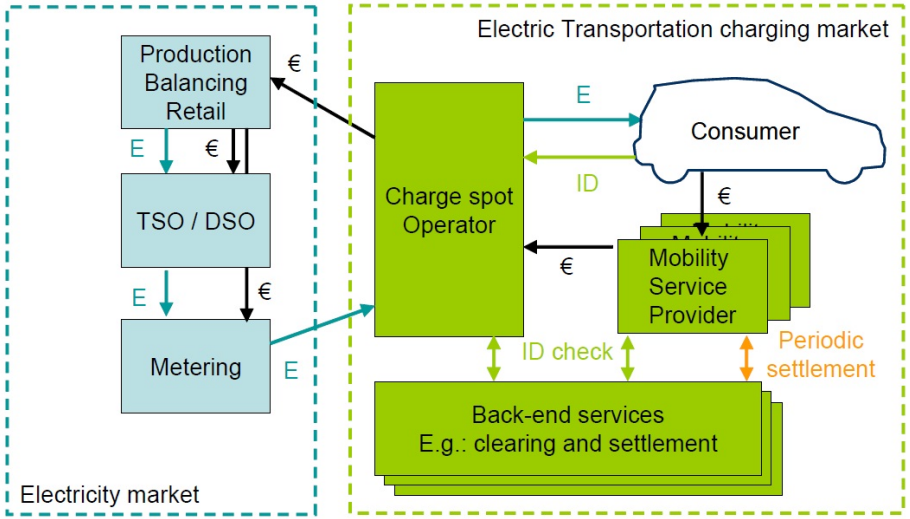
Electricity Supply in the Future

sustainable and dynamic

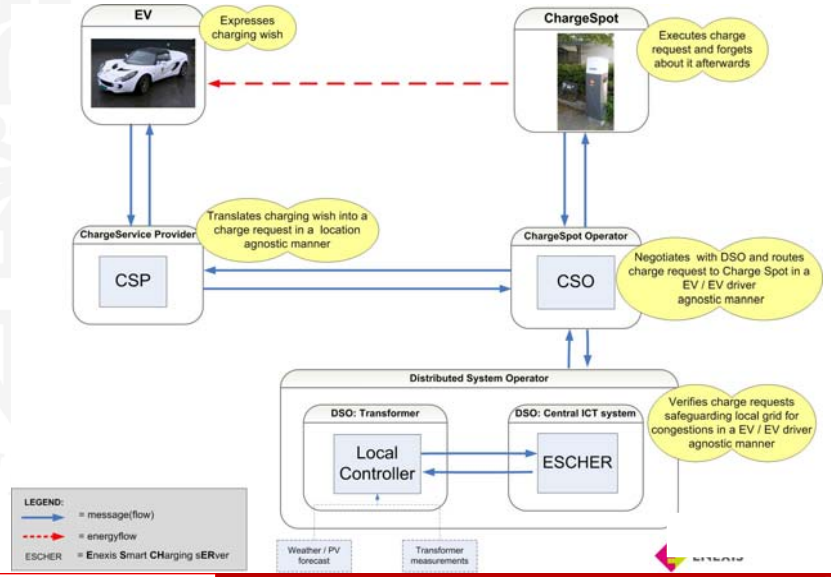


Smart Charging of EV's

Possible new Market Model



Smart Charging of EV's IT-Architecture, privacy *by design*



Smart Metering

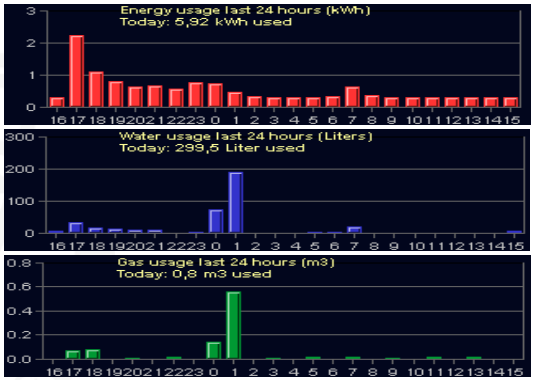
- *Flavio Garcia, Bart Jacobs, Eric Verheul, Marko van Eekelen*
- Sentinels (RDW, Alliander, RU)
- Secure and Privacy Friendly Metering Applications (electricity, road pricing)
- Focus on smart use of cryptographic protocols

Smart Electricity Metering??

(1880's technology) (today's technology)

Privacy	☺	☹
Integrity	☺	☹
Availability	☺	☹
Functionality	☹	☺

Privacy issues



In 2009 the Dutch Senate refused a bill that made it compulsory for consumers to accept e-meters in their homes

SLIMME METERS

MIJN BROERTJE GAAT LANGER DOUCHEN IN DE HOOP DAT DE CONTROLEURS DENKEN DAT HIJ EEN VRIENDINNETJE HEEFT

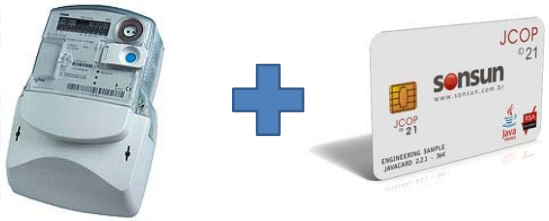
Loesje

Postbus 1045
6801 BA Arnhem www.loesje.nl

Security/availability issues

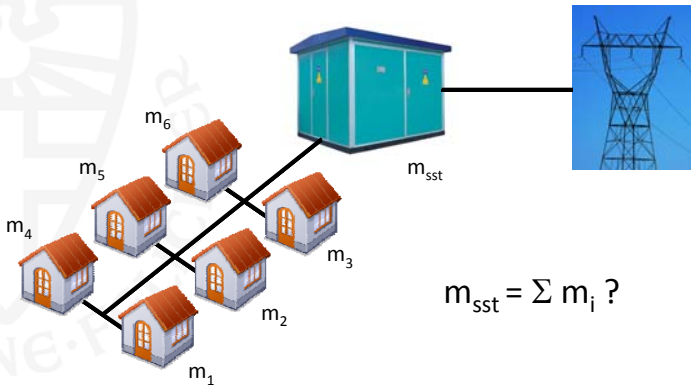
- Current smart-meters are not 'smart' (limited to symmetric key crypto)
- Grid operators can upgrade firmware at will
- Remote disconnect is very sensitive
- What kind of warranties does the user get?
  - Trust should be mutual

How can we improve this situation?



- Incorporate a trusted element
- Provide certain autonomy to the meters
  - This requires PKI
  - On card key generation
- Limit updates
- Data minimization

Fraud/leakage detection



$m_{sst} = \Sigma\, m_i$?

Homomorphic encryption

- An encryption scheme $\{\text{-}\}_{pk}$ is additively homomorphic if:

$$\{m\}_{pk} \otimes \{m'\}_{pk} = \{m + m'\}_{pk}$$

- Makes it possible to design a protocol that
  - checks for leakage in a subnetwork
  - without revealing any individual measurement

Smart Electricity Metering Conclusions

- Provide e-meters with autonomy
  - i.e., secure element + PKI capabilities
- Separations of goals and data minimization
- Same protocol works for grid optimization
- Security proof in the standard model

Cell-Based road pricing (CBR)

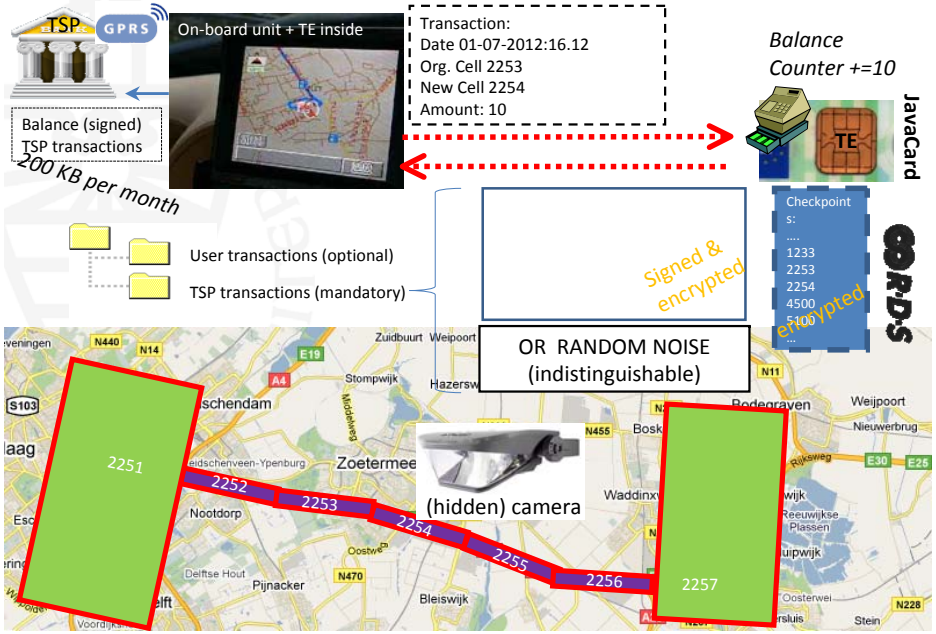
Open Universiteit www.ou.nl
Radboud University Nijmegen

Cell-Based Road pricing 'pay yourself shop' metaphor

- Take items yourself and put them on your tab yourself
- Taking of 'some' items is covertly photographed in shop
- During payment, presence of these items on the tab is checked by the shop
- Parameter 'Some' provides balance between fraud resistance and privacy

Radboud University Nijmegen

Cell-Based Road pricing highlights



Cell-Based Road pricing add-ons

Model and its implicit payment infrastructure supports many side applications, e.g.:

- parking payment
- conventional toll roads,
- Congestion Based Rewarding (spitsmijden in Dutch),i.e. the positive way of implementing road pricing

Model introduces new business models for e.g., governments, toll chargers, city parking authorities and SATNAV manufacturers.


Amsterdam.nl

Homepage ▸ Parkeren & verkeer: Veelgestelde vragen over par

Veelgestelde vragen over parkeren op kenteken

13 oktober 2010 - Jacqueline Schermer

Bij parkeren op kenteken voert u het kenteken van uw auto in op e parkeerautomaat. In de parkeerrechtendatabase (PRDB) wordt vastgelegd dat u betaald hebt. U ontvangt een betalingsbewijs voo eigen administratie. Dit bewijs hoeft u niet in de auto te leggen.

Het vervangen van het parkeerkaartje door kentekeninvoer past in het digitaliseren van parkeerbewijzen. Vergunningen en betalingen via belserviceproviders worden in Amsterdam al uitgegeven op kenteken en daarmee als digitaal recht centraal geregistreerd in een beveiligde

The Future of Green ICT

Smart systems

- Green systems with more Intelligent Control
- Secure setup
- Based on well protected, selected information

Smart systems research needed in many application areas

SIEnergyLAB
SUSTAINABLE ICT & ENERGY RESEARCH