Smart Grid Privacy via Anonymization of Smart Metering Data

Wei Niu

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Paper information

- Title: “Smart Grid Privacy via Anonymization of Smart Metering Data”
- This paper appears in 2010 1st International Conference on Smart Grid Communications
- Author: Costas Efthymiou and Georgios Kalogridis

Organization

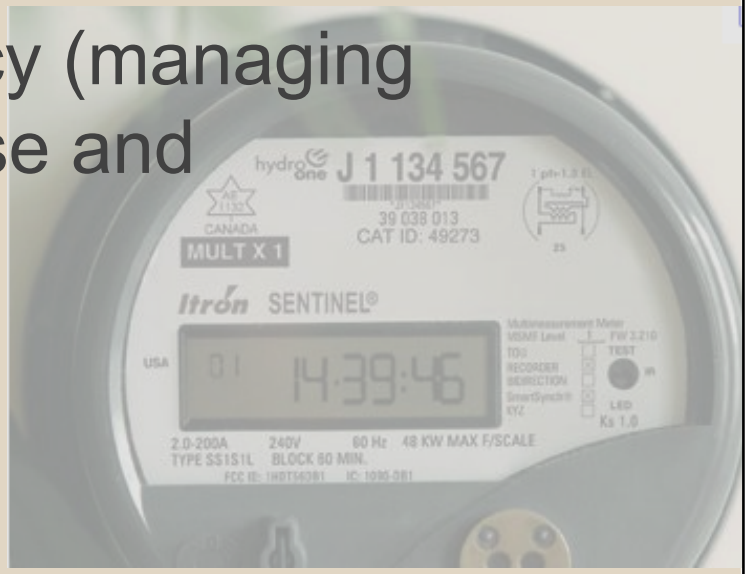
- Introduction
- Background
- Problem Statement
- Proposed Solution
- Security Analysis
- Conclusion

Introduction

- Trends of developing smart grid
- Cyber security and privacy are prime issues
- Focus on privacy of smart metering data

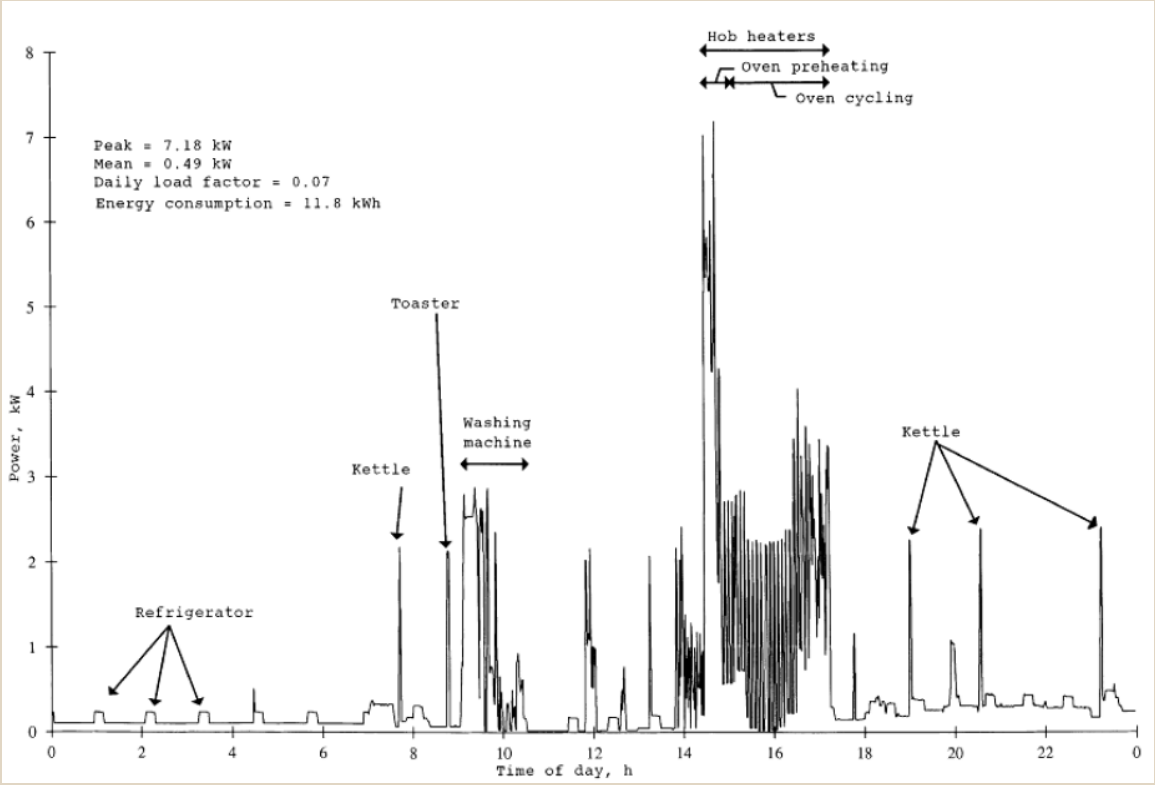
Background-Smart meter

- Measure energy consumption in much more detail
- Communicate to local utility for monitoring and billing
- High meter reading frequency (managing load, Demand Side Response and Management)



Background-potential problem

- Detailed energy usage information may expose the user's privacy !



From E.L.Quinn, "Privacy and the New energy Infrastructure"

Problem Statement

- How can high-frequency data be anonymized?
- Proposed Solution: 3rd party Escrow-based Anonymization

Assumptions

- 1.Metering data needed for billing or account management purposes needs to be attributable
- 2.Attributable metering data will typically be collected at low frequency
- 3.Metering data needed for power generation and distribution network control doesn't need to be attributable

Assumptions Cont'd

- 4.Anonymous data will be collected at high-frequency
- 5.The smallest 'unit', which consumer is known to network, is a distribution sub-station or equivalent
- 6.An adequate trust relationship is present between 3rd party escrow service providers, utility companies and their customers.

Escrow-Based Anoymization-Defination

- High-frequency metering data
- The meter readings which a smart meter transmits to the utility often enough to suggest information related with the electrical data user's private life
- Low-frequency metering data
- The meter readings which a smart meter transmits to the utility scarcely enough to offer adequate privacy

Meter architecture

- Two separate IDs
  - HIFD (anonymous)
  - LFID (attributable)
- Best strategy to keep anonymous is for it never known to the utility or installer
- Problem of authentication arise
- 3rd party escrow will come to the rescue
  - manufacture or some other trusted 3rd party

Cont'd

- Required to comply with a strong data privacy policy

  -do not access or store smart metering data and only know the relationship between a valid HFID and LFID

PISM & ANSM

- Personal Identifiable SM Profile (PISM)

  - PISM CERT: LFID, Public Key and PISM Certifying Authority Information

  - PISM Private Key

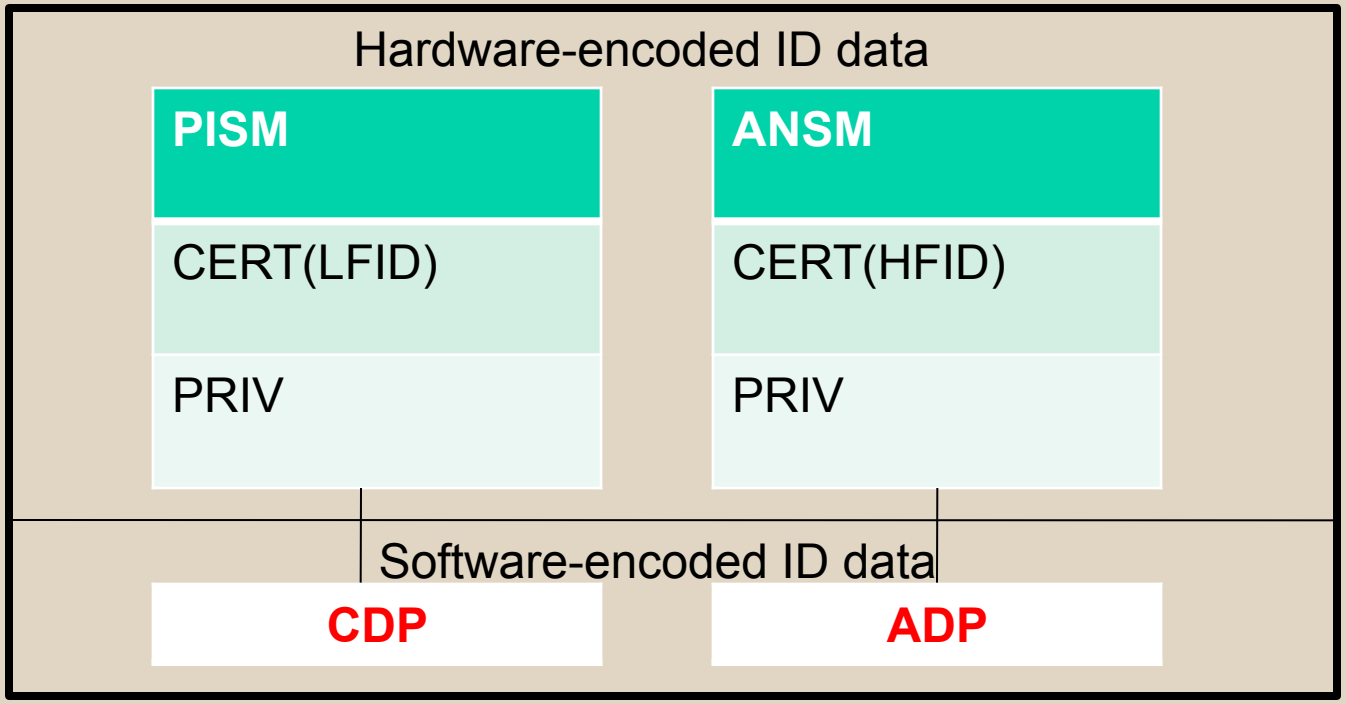
- Anonymous SM Profile (ANSM)

  - ANSM CERT: HFID, Public Key and ANSM Certifying Authority Information

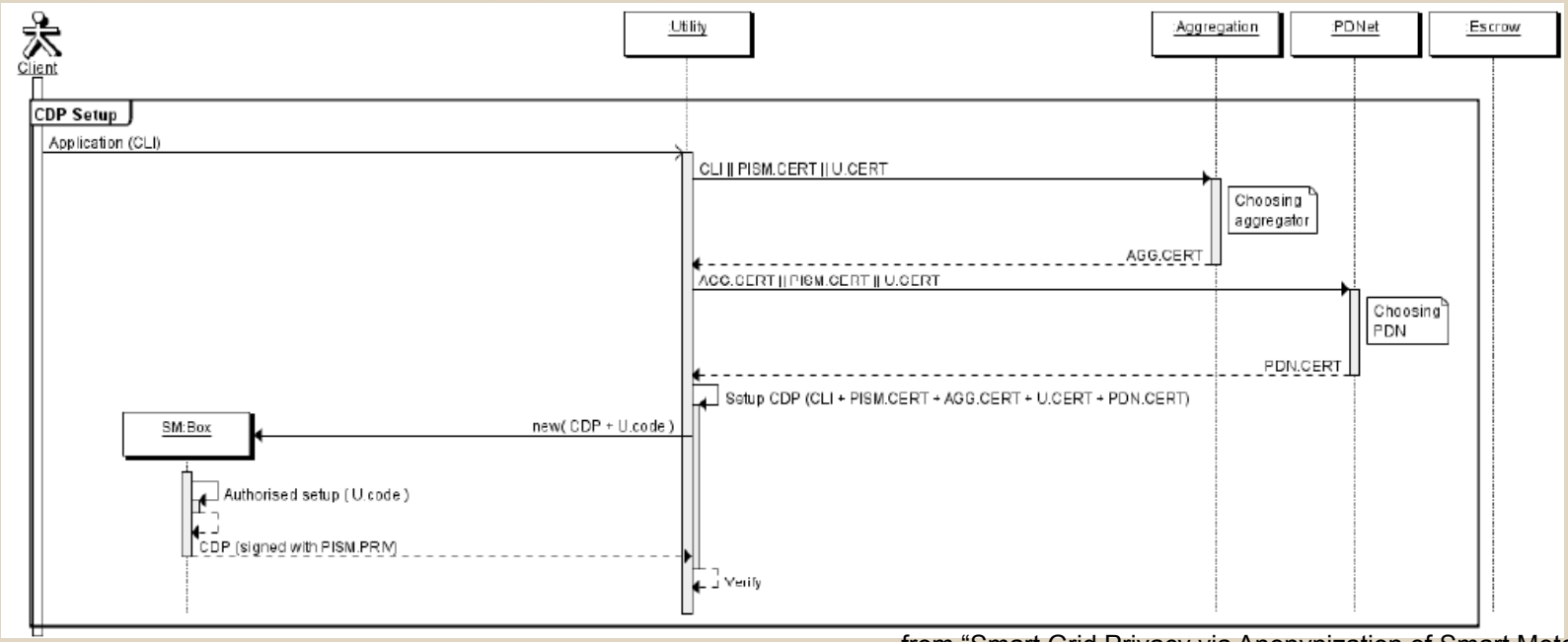
  - ANSM Private Key

Cont'd

Structure of smart meter



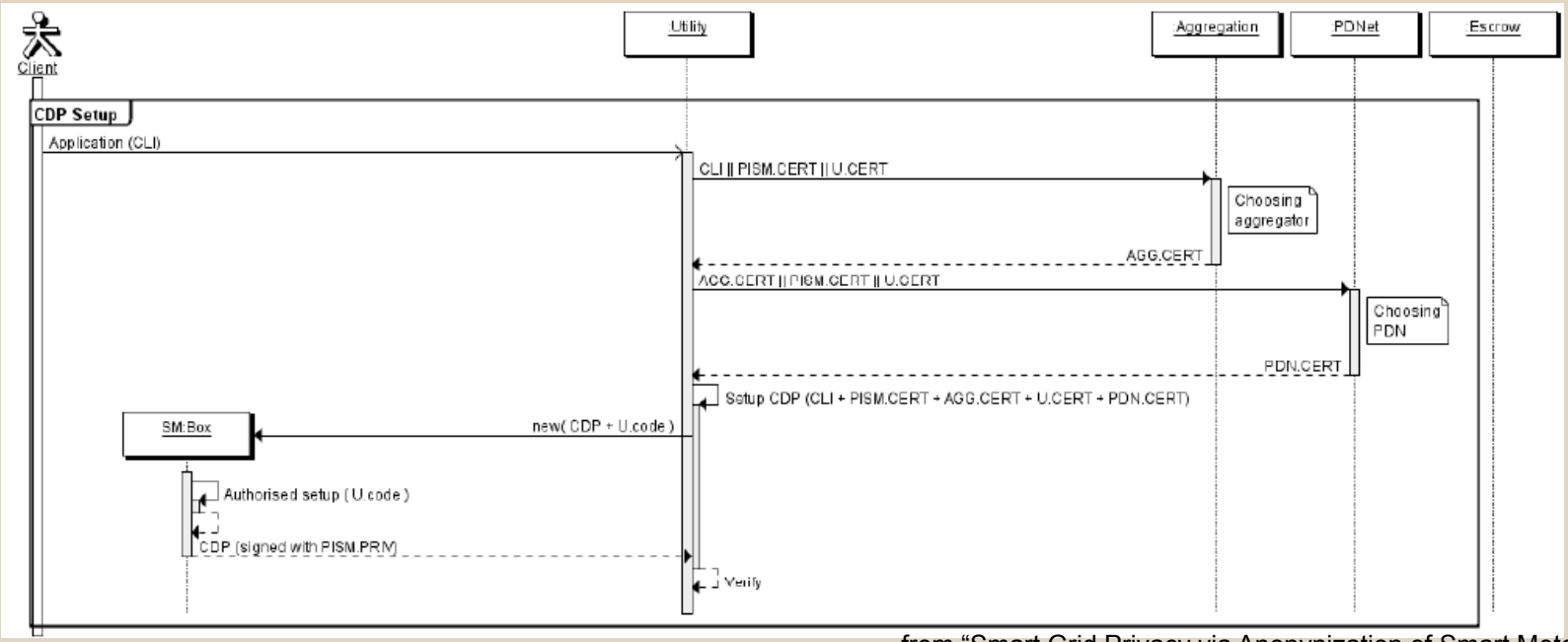
CDP Setup Process



from "Smart Grid Privacy via Anonynization of Smart Metering Data"

- CL->U:CL.CLI
- U->AGG: CL.CLI||PISM.CERT||U.CERT
- AGG->U:AGG.CERT
- U->PDNet: AGG.CERT||PISM.CERT||U.CERT

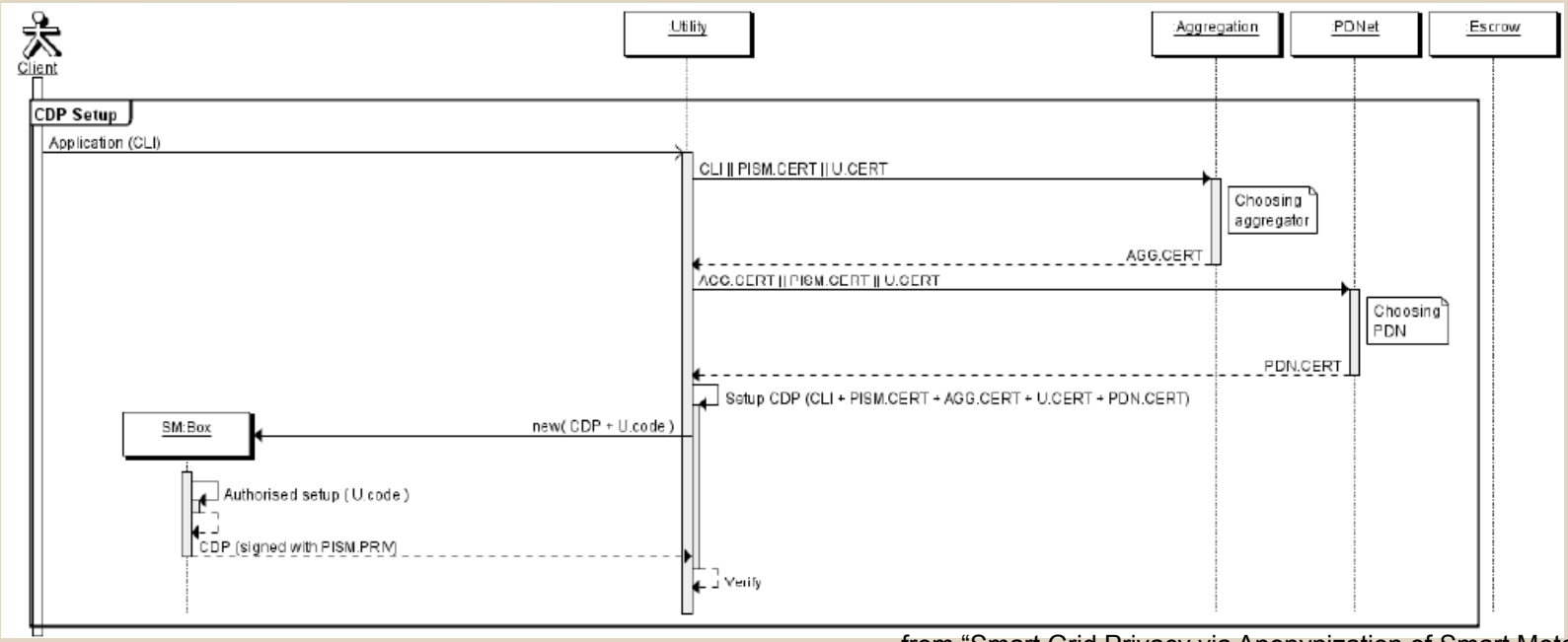
Cont'd



from "Smart Grid Privacy via Anonynization of Smart Metering Data"

- PDNet->U:PDN.CERT
- CDP = CLI || PISM.CERT || AGG.CERT || U.CERT ||PDN.CERT
- U->SM: CDP||U.code
- SM->U:CDP||$S_{PISM.PRIV}$(CDP)

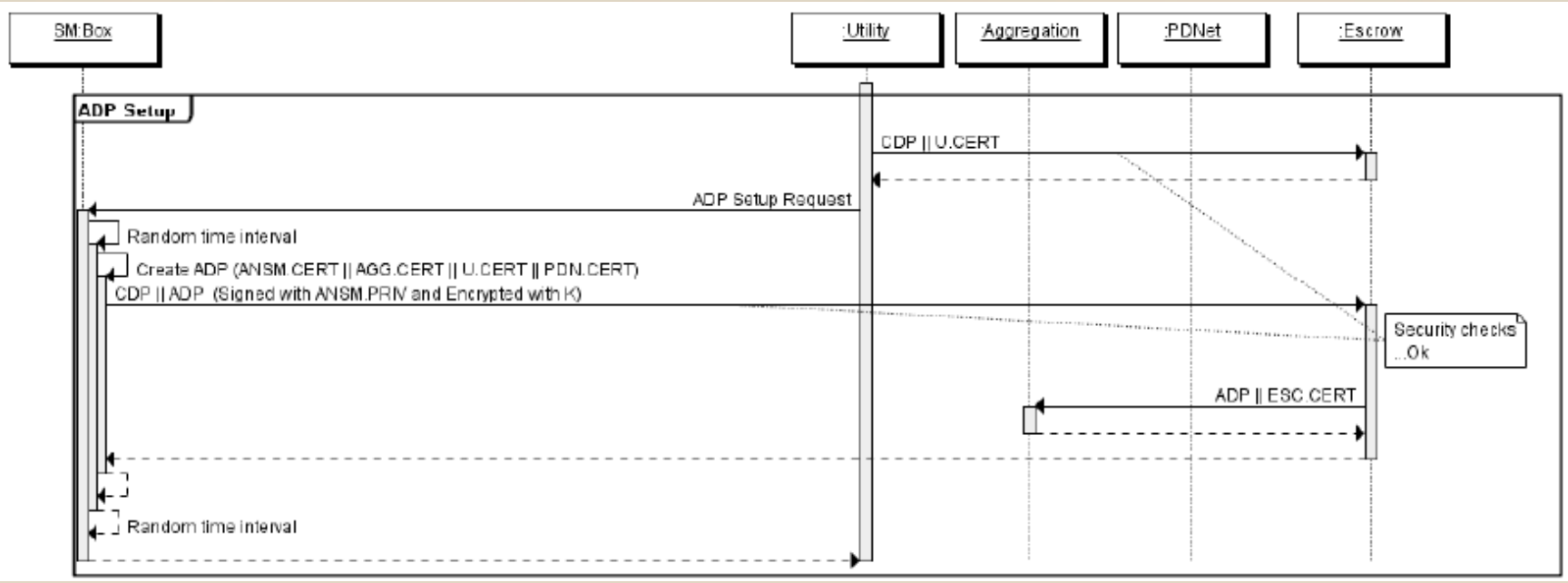
Cont'd



from "Smart Grid Privacy via Anonynization of Smart Metering Data"

- SM begins sending CDP data(infrequently)
- SM->U:CDP||Data.LF|| $S_{PISM.PRIV}$(CDP|| Data.LF)

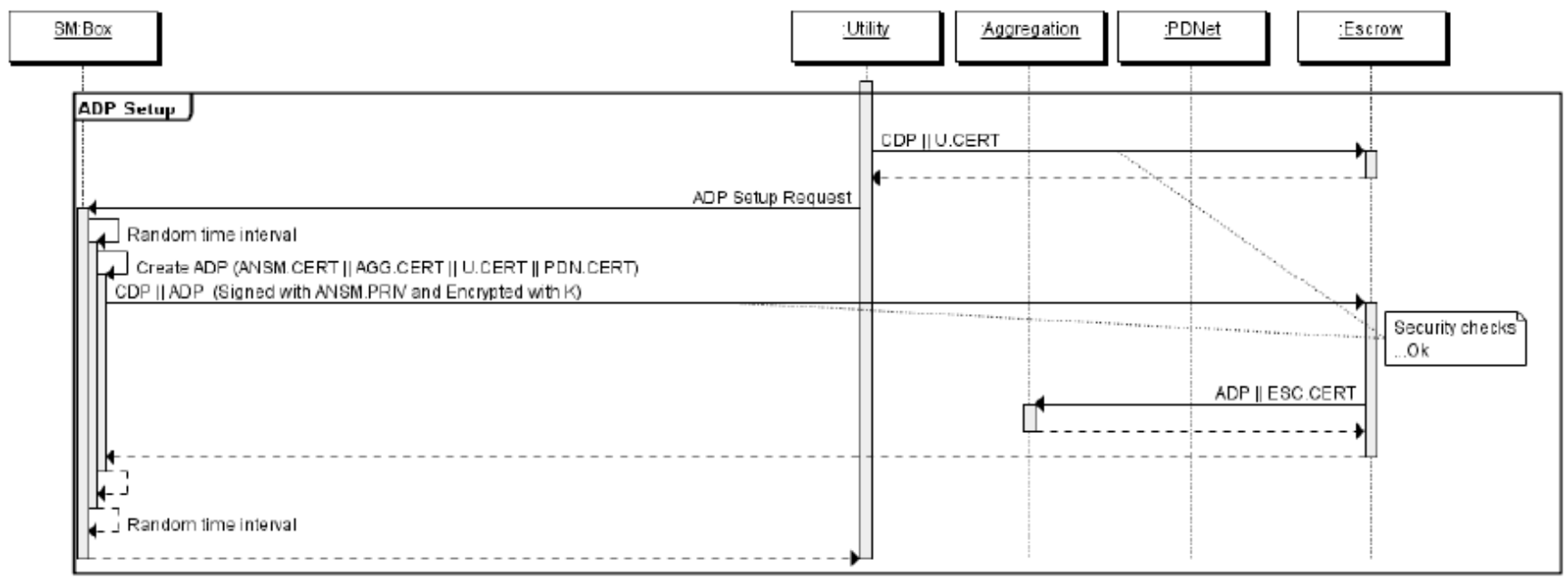
ADP Setup Process



from "Smart Grid Privacy via Anonynization of Smart Metering Data"

- U->ESC: CDP || U.CERT
- ESC->U: OK
- U ->SM: ADP setup request
- ADP = ANSM.CERT || AGG.CERT || U.CERT||PDN.CERT

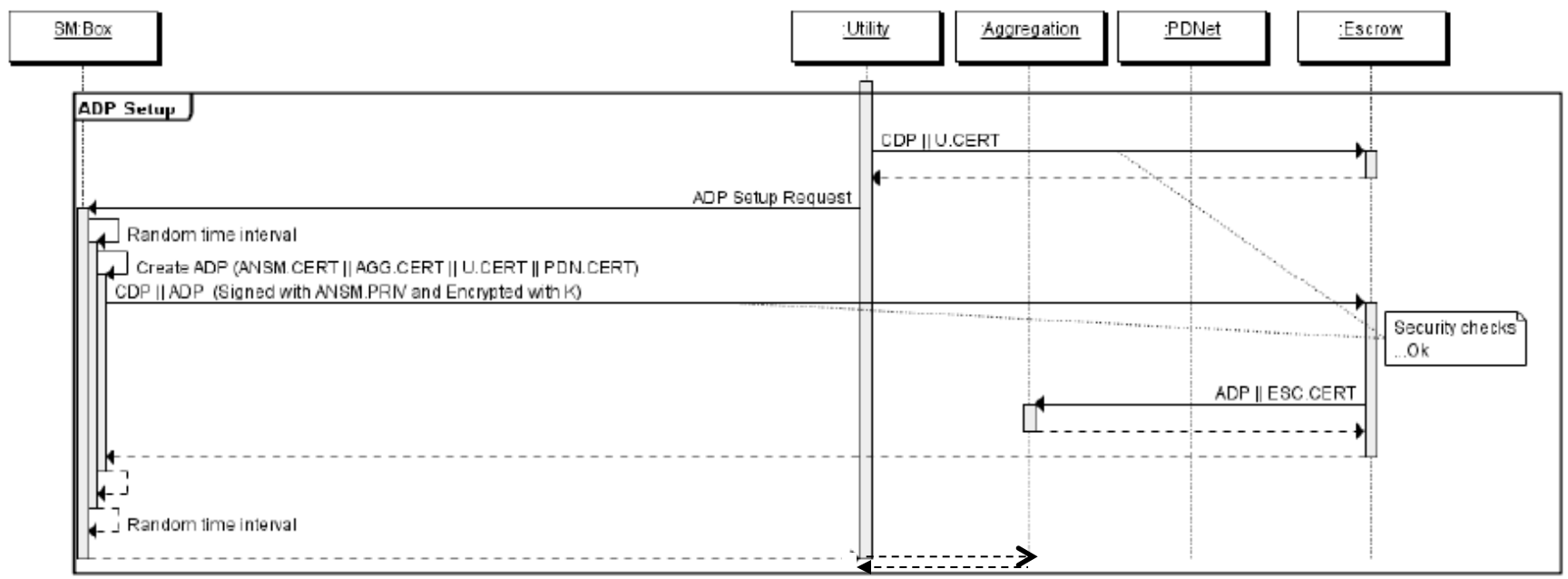
Cont'd



from "Smart Grid Privacy via Anonynization of Smart Metering Data"

- SM->ESC: $E_K(CDP||ADP) || S_{ANSM.PRIV}(E_K(CDP||ADP))$
- ESC->AGG: ADP || ESC.CERT
- AGG->ESC: OK

Cont'd



from "Smart Grid Privacy via Anonynization of Smart Metering Data"

- ESC->SM: OK
- SM begins sending ADP data (frequently)
- SM-> AGG: ADP||Data.HF||$S_{ANSM.PRIV}$(ADP|| Data.HF)

Normal Operation

- CDP setup
- ADP setup and appropriate random time interval passed
- SM chooses a random number as initial meter reading to remove LF and HF correlation
- then proceeds to send frequent updates
- For ‘micro-management’, utility send control message to relevant aggregator, then forward onto the anonymous ID

Operation in Abnormal Situations

- There may be situations where temporary lifting of the anonymity provided by this solution is required and may be sanctioned.
- Power theft, meter fail, new homes
- Anonymity may be reinstated by triggering a ‘refresh cycle’, effectively forcing each of the smart meters connected to a certain aggregator to re-setup their ADPs

Security Analysis

- Data communication should provide CIA
- In our proposed protocols, we assume all logical or physical communication entities are equipped with digital certificates
- The Security of CDP setup
- Authentication of both SM and client cannot be guaranteed at beginning.
- Client be verified by utility engineer during installation
- SM authenticity be varified after administering the secure code U.code.

Cont'd

- The anonymity of ADP

- The harder to link ADP with CDP, the better anonymity is achieved
- Degree of anonymity depends on the random time interval

  the anonymity set comprises all the ADP finalization responses the utility receives dring the period between one SM sends CDP finalization response and any ADP finalization response

  Its average value needs to be large enough to allow a large enough anonymity set to be created

Example

- Suppose there is a rate of x CDP installations per unit of time for a certain aggregator
- We want to acquire an anonymity set of size y
- The time interval should be on average larger than y/x

Potential Problem and Solution

- Utility may deliberately spread delay in some CDP setup procedures in order to reduce the anonymity set.
- The escrow service control the random time interval

Conclusion

- The author attempted to address the smart metering privacy issue by anonymizing the identity of high-frequency metering data through escrow service
- The key is trust level of such escrow service and the random time intervals between the setup of ADP and CDP
- Future work: defining how the anonymization process can be extended to address a number of practical scenarios

Pros & Cons

- Pros
  - Provide more privacy to user
  - More control and guarantee of metering system
- Cons
  - Complex system
    two ID, two setup process
  - Need joint effort of escrow

Thank You