



# Solution Design Advisory Group (SDAG)

BIS Conference Centre

24 July 2013

# Agenda: SDAG #9

## BIS Conference Centre

### 10:00 Wednesday 24 July 2013



Department  
of Energy &  
Climate Change

No	Time	Subject	Lead
1	10.00 – 10.15	Actions from previous meeting	Colin Sawyer
2	10.15 – 10.45	Consolidated Issues Log	Colin Sawyer
3	10.45 – 11.30	Feedback from Workshops - HHT & GUID	Mark Robins/Ed Williams
4	11.30 – 12.00	Transition Approach	Colin Sawyer
5	12.00 - 12.30	SMETS2 Updates	Charlotte Middleton
6	13.00 – 13.30	SMKI Process Impacts	Mike Bennett
7	13.30 – 14.00	AOB - Contractor's Switch in Electricity meters	Alastair Manson



# 1. ACTIONS FROM PREVIOUS MEETING

Colin Sawyer

SDAG_2.15	<p><b>Outage reporting:</b> DECC to talk to Alan Creighton of the ENA to discuss Outage Management requirements and confirm requirements from the ENA and ensure alignment within the CSP schedule 2.1</p> <p><b>Update:</b> Alan Creighton agreed to write to the Chairman on service levels by 28.03.13.</p> <p><b>Update:</b> clarification on device states following power outage is documented in the ALC ELPM</p> <p><b>Update:</b> AC and CS agreed to discuss this matter separately and AC would be sent a copy of the HCALC model. Meeting on the 11<sup>th</sup> July</p>	28.03.13	Alan C	Ongoing
SDAG_3.01	<p>DECC agreed to issue product descriptions to SDAG Members when they had been completed</p> <p><b>Update:</b> Following agreement of PDs submitted by bidders, DECC would issue to SDAG members</p>		CS	Ongoing
1.1. SDAG_5.01	<p><b>Design Phase Milestones.</b> It was agreed that the design phase of the DSP and CSP would be discussed at a future SDAG meeting.</p>	24.07.13	CS	Ongoing
SDAG_6.02	<p>SDAG members were invited to provide evidence that the gas enable function was a safe process at the earliest opportunity.</p> <p><b>Update:</b> SDAG members advised that the evidence was being collated and report would be issued in the near future</p>	02.07.13	ALL	Ongoing

SDAG_6.03	<p>A final version of the PPMID DDS was complete it would be issued to SDAG members for information.</p> <p><b>Update:</b> The DDS was undergoing legal review at DECC and would be issued to SDAG members in early June 2013.</p> <p>Update: The legal review took longer than estimated and DECC are in the process of a consistency review. Once completed will be sent out to members.</p>	02.07.13	PM	Ongoing
2.6	<p>Process to Support MOP working - As no conclusions were made bar to all agreeing that an 'option' should be made available, the Chair requested that the Group consider the options presented and email DECC with any particular opinions to assist further discussions at the next SDAG meeting.</p>	23.07.13	All	Open
4.4	<p><b>Service Management – workshop feedback:</b> It was agreed that the slides would be updated to reflect members' views. <b>ACTION DECC</b></p>	24.07.13	Tim Hall	Open
4.6.3	<p><b>Prepayment – workshop feedback:</b> Confirm requirement to re-set the 'floor value' of the UTRN sequence number at CoS – No update at present. <b>ACTION DECC</b></p>	24.07.13	DECC	Open

1.1.

4.6.4	<b>Prepayment – workshop feedback:</b> Arrange further briefing for small suppliers – Delayed due to procurement. <b>ACTION DECC (CERB's James Biott)</b>	TBC	DECC – James Biott	Open
4.6.5	<b>Prepayment – workshop feedback:</b> Circulate updated PPM Issues Log – <b>ACTION DECC (CERB's James Biott)</b>	24.07.13	DECC James Biott	Open
8.4	<b>Privacy PIN:</b> There was some concern from the Group in allowing activation of the PIN locally, however did not want to withdraw that option from the consumer. The Group agreed options for the consumer needed further discussion. <b>ACTION DECC TIM BAILEY</b> to discuss within discussions with consumer groups.	24.07.13	DECC – Tim Bailey	Open
8.6	<b>Privacy PIN - options for setting protected data/functions</b> - The Group agreed that an option between the third and 5 <sup>th</sup> Option would be preferable. Following Tim's meeting with consumer groups, feedback to members of the discussion to assist members with further consideration of the options and provide DECC with a firmer view. <b>ACTION DECC AND MEMBERS</b>	24.07.13	ALL	Open

9.1	<b>SMETS2 export consumption</b> – Some members have seen the AMO document covering situations where a twin element meter also has export, and the rates appear inconsistent. AMO suggested that modifications to SMETS might be required. <b>ACTION DECC – Peter Morgan to write to AMO.</b>	24.07.13	Peter Morgan	Open
-----	---	----------	--------------	------

1.1.



## 2. CONSOLIDATED ISSUES LOG

Colin Sawyer





## **3. FEEDBACK FROM WORKSHOPS - HHT & GUID**

Mark Robins and Ed Williams



- Security requirements and responsibilities
- General HHT use case
- Usage scenarios: installation and maintenance
- How ZigBee inter-PAN joining works
- Install and leave considerations
- Sending commands via both CSP and HHT
  - Mixed approach to HHTs amongst Suppliers:
    - some may use HHTs even when there is WAN as installation may be faster
  - DECC confirmed that there is **no intent to draft a DDS for an HHT**



- **What happens if WAN and HHT installation are undertaken?**
  - In-bound commands: 1<sup>st</sup> instance received executed, 2<sup>nd</sup> rejected
  - Responses: could come back via the WAN *and* via the HHT
- **Does installer need equipment matched to property?**

**Options:**

  - Collect commands to configure SME *on demand* through HHT
  - Load HHT with every combination of device IDs and commands for a given number of installs that day / week / month etc

*Discussion highlighted: no benefit associated with local entry of MPXN*
- **What is HHT security compared with Type 1/2 devices?**
  - HHT doesn't join the PAN
  - HHT connection is effectively firewalled at the comms Hub
  - Type 1 + 2 devices require critical commands to enable functionality
  - HHT is essentially a “carrier pigeon” for supplier commands

- **How can HHT connect on ZigBee inter-PAN?**  
**What is the function of Comms Hub beaconing?**
  - CH beacons to allow devices to join the network
  - CH can set a flag to allow inter-PAN communication
    - Set ON when the Comms Hub powered up
    - Could be set OFF by installer or time out
    - Leaving the flag ON all the time adds DOS vulnerability + installer confusion (which HAN to communicate with?)
    - Method required to turn flag ON during maintenance visit
      - » “Installer-PIN” protected menu on a trusted device (ESME and GSME).
      - » AMO suggested to set ON when WAN is lost

**ACTION: DECC to consider options for turning the beaconing flag on and off.**



- **Will an 868 HHT be required?**
  - Will be driven by future SEC panel decisions re: single / dual band CH
    - If single band 868 CH became available, 868 HHT required
- **What will HHT be able to read + display?**
  - Suppliers free to implement [Parse](#) functionality on HHT
    - Allow installer to look at the contents of all message types except those with sensitive data
- **How will HHT sequence service requests + commands?**
  - Commands are sequenced within service requests:
    - Same whether delivered over the WAN or for HHT
    - Suppliers are free to sequence service requests in any order.
    - What if HHT connection lost during transfer of a service request?
      - » Meters log which commands have executed: should be possible for a process to restart where it broke off



- **What happens on CoS if HHT not ‘unloaded’ by previous supplier?**
  - Details for registered supplier on DCC may not be current supplier
  - Incoming supplier would have to contact registered supplier to effect any change
- **How will HHT be tested?**
  - It is expected that HHT can be tested as part of *Testing and Trialling*
  - HHT interface could be certified as part of ZigBee testing



- EDF indicated that it would be useful for a central register of aborted installs due to no WAN
  - Subsequent supplier visits are forewarned
- DECC clarified that time could be set using an HHT
  - Accuracy requirement would take “under normal operating conditions” into account



- **Option 1:** Comms Hub enables Inter-PAN for (60) minutes from a power-up, and keeps Inter-PAN alive whilst in use
  - During maintenance visit, installer can power-cycle Comms Hub, and then re-seal
  - *No changes to SMETS required; detail captured in GBCS*
- **Option 2:** Inter-PAN enabled on Comms Hub over ZigBee by trusted device
  - ESME and GSME trusted to send this command
  - PIN-protected menu required on ESME + GSME user interface to support this
  - *Changes to SMETS required; detail captured in GBCS*
- **Option 3:** Inter-PAN enabled without timeout if WAN is not present
  - Assuming good WAN coverage, this will only apply to a small % of Comms Hubs
  - Allows comms without entering the property in these cases
  - *Changes to CHTS required; detail captured in GBCS*





- *Use case*: During maintenance visit, the HHT operative can perform SME configuration without entering the property (no-WAN only)
- Proposal: CH enables Inter-PAN when WAN is not available
- Risks identified:
  - An attacker can repeatedly attempt to connect to the CH, as a Denial Of Service (DOS), or brute-force attack
  - If connecting to CH successful the attacker can attempt to send commands to the SME
  - If connecting to CH successful the attacker can continuously send commands to keep the equipment occupied, and prevent other ZigBee HAN comms
  - If connecting to CH successful the attacker can continuously send commands to run down GSME battery
- Risks and mitigations under review by DECC



- Questions for SDAG
  - Suppliers: What is the preferred option and why?
    - All options: Should the keep-alive timeout be mandated? If so what should it be set to?
    - Option 2: Should the provision of a PIN-protected installer menu to enable Inter-PAN be mandated on both ESME and GSME?
  - Manufacturers: What are the cost and development timescale impacts for implementing each option?
  - All: Should DECC also mandate inclusion of a ZigBee Inter-PAN command to turn Inter-PAN off?
- **Action: DECC to send formal questions to SDAG members**



- Each Device within GB Smart Metering requires an Id that uniquely identifies it
- This supports messaging through the DCC and underpins the end-to-end Security Model
- It applies to any Device that can be sent GBCS messages from the DCC, and has implications for Organisations that send and receive GBCS messages
- There are six requirements from a Programme perspective:
  - Universal Uniqueness across GB Smart Metering;
  - No greater than 64 bits in length;
  - Part of the Device Binding;
  - Electronically stored and non-modifiable;
  - Physically displayed; and
  - Inventory mapping of GUID to MPxN.
- DECC does not consider its place is to mandate the format of this ID, however there are a set of requirements that have to be met

1. Use of existing Electricity Meter Serial Number (MSN) scheme
2. An additional identifier, such as EUI-64
3. New MSN scheme
  - Combining aspects of (1) and (2), to mitigate any impact of a new numbering scheme by replacing the current MSN
4. Use of existing Electricity MSN scheme AND emerging Gas MSN scheme

1. Use of existing Electricity Meter Serial Number (MSN) scheme
2. An additional identifier, such as EUI-64
3. New MSN scheme
  - Combining aspects of (1) and (2), to mitigate any impact of a new numbering scheme by replacing the current MSN
4. Use of existing Electricity MSN scheme AND emerging Gas MSN scheme

## EUI-64

- 64 bits in length (24 bits for the Organisation Unit Identifier (OUI), 40 for the organisation generated segment)
- OUI Administered by IEEE Registration Authority
- Cross-industry standard, but not used for GB metering currently
- Example:
  - 00-23-7E-00-00-12-D6-87<sub>hex</sub>, or rendered in a human readable decimal format
  - 00-23-7E-0000001234567
  - In this example, the manufacturer would be Elster, as identified by the “00-23-7E”



- EUI-64 will be adopted for GUIDs for both Devices and Organisations;
- All organisations sending and receiving GBCS messages through the DCC, and all Device manufacturers, will be required to use an OUI issued by the IEEE Registration Authority;
- The Device manufacturer will be responsible for generating the GUID for each Device;
- The manufacturer controlled part of the GUID will be an incrementing sequence number; and
- The GUID will exist in conjunction with the current Meter Serial Number (MSN) schemes for Gas and Electric Smart Meters, although it was recognised that an opportunity exists to use the GUID instead of the MSN, and this will be investigated further by the industry.



## 4. TRANSITION APPROACH

Colin Sawyer



## 5. SMETS2 UPDATES

Charlotte Middleton



# SMETS 2 Update



Department  
of Energy &  
Climate Change

- 16 potential changes
  - For details, see separate excel table sent to you on 22/07/13, hard copies will be available at the meeting



## 6. SMKI - Process and service impacts of Emerging requirements

Mike Bennett

E2E Security Requirements defines credential management requirements:

- Requirement to obtain Bindings for a meter's public key material
- Requirement to regenerate device private keying material after commissioning
- Requirement to store device Binding on the device
- Requirement to remotely read public certificates held on a device
- Requirement to validate root and recovery keys

# Regeneration of Meter Private Keys



Department  
of Energy &  
Climate Change

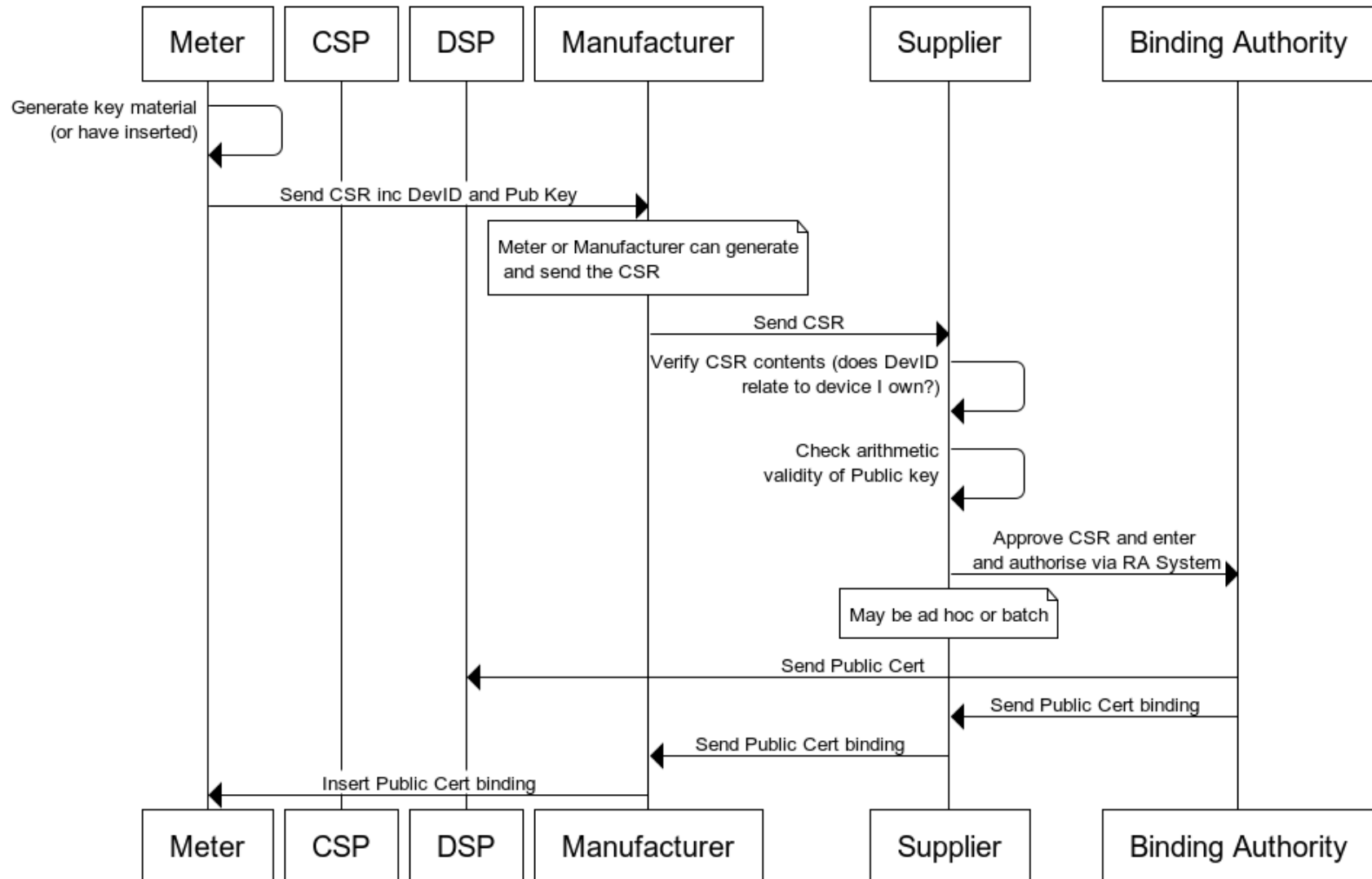
Paraphrased from STEG (18/07/13):

- SMKI places limited reliance on meter supply chain (could be offshore).
- Therefore there is a risk that the meter's private key, whether generated on-board or injected could be compromised.
- The risks this present are:
  - Supply affecting (with 2 party collusion)
  - Fraud (device impersonation)
  - Confidentiality (other parties reading meter data)
- So limited reliance can be placed on the meter's private keying material as provided at manufacture
- It will however require a device Binding at the outset, as it is used in the update process
- Therefore meter private keying material should be regenerated at or close after, the commissioning process

# Public binding at manufacture

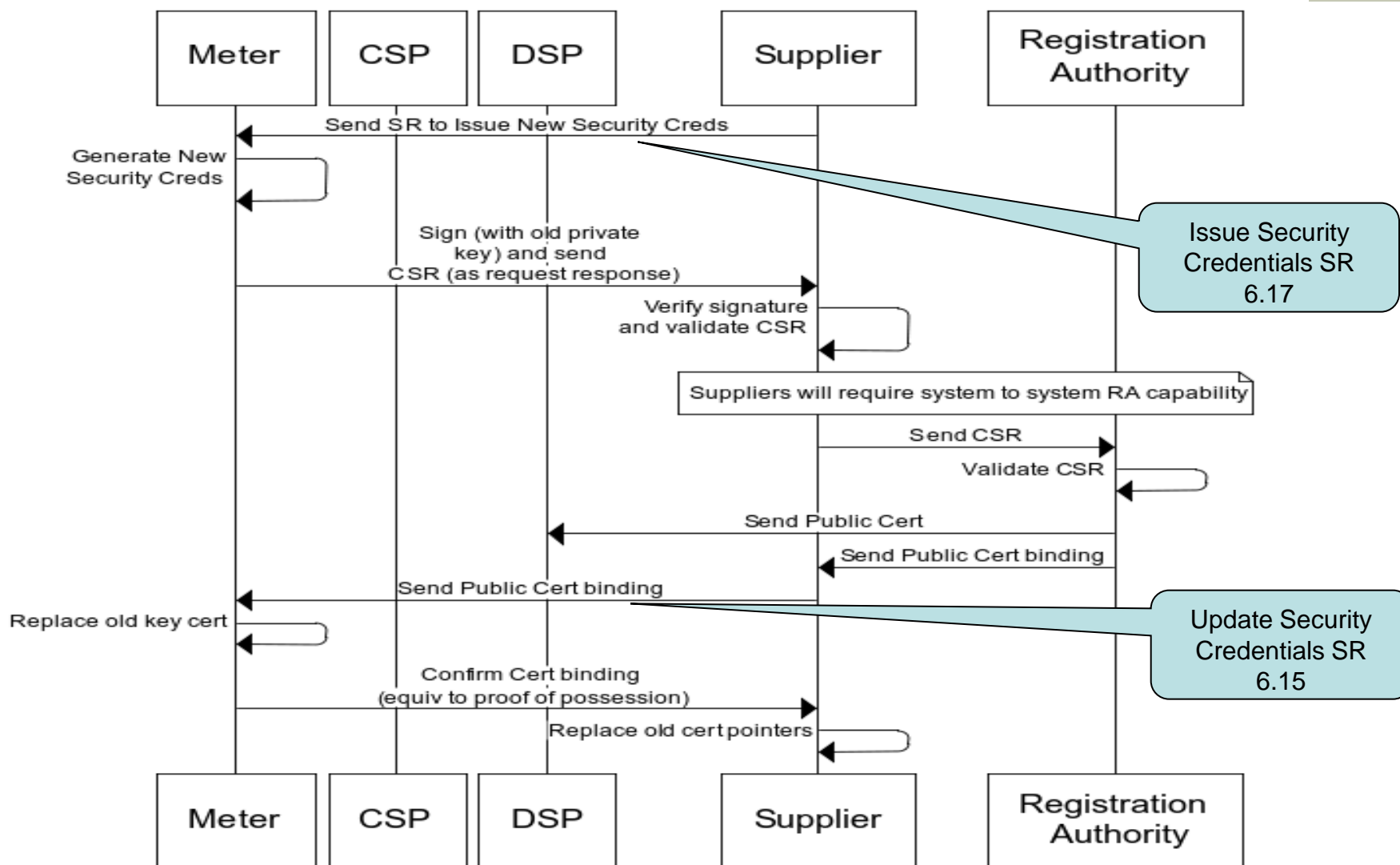


Department  
of Energy &  
Climate Change





# Regeneration interaction diagram



# Remote reading of public security credentials



Department  
of Energy &  
Climate Change

- DCC Service Users need to validate their own certificates on a meter.
- Likewise, there is also a need to validate Root and Recovery certificates.
- How to achieve this:
  - Supplier public certificate validated by Commission SR (critical command)
  - Root certificate validated by Updating Network operators public certificate
  - Recovery certificate needs validation by Recovery party
- Mechanism (SR) required to retrieve Meter's public certificate (held on meter)



## 7. AOB

Contractor's Switch in Electricity meters – Alastair Manson



# DATE FOR NEXT MEETING



Department  
of Energy &  
Climate Change

## Next Meeting

- 28<sup>th</sup> August 10 – 3pm