

# Solution Design Advisory Group (SDAG)

Inaugural Meeting  
BIS Conference Centre

4 December 2012

**Agenda: SDAG**  
**BIS Conference Centre**  
**10:00 Tuesday 4<sup>th</sup> December 2012**



1. Introduction.
2. Review of Terms of reference and scope, and objectives of SDAG
3. Update on Actions from extended STEG Workshops
4. Plans for Strategic review of technical requirements sections of the ISDS (CSP & DSP)
5. Update on installation and maintenance processes (including the use of handheld terminals)
6. Date of next meeting.
7. AOB.

## **2. REVIEW OF TERMS OF REFERENCE AND SCOPE, AND OBJECTIVES OF SDAG**

*Colin Sawyer*

## **3. UPDATE ON ACTIONS FROM EXTENDED STEG WORKSHOPS**

*Gordon Hextall*

# Security architecture update - 1

- The security architecture is defined within the overall technical architecture:
- Work is in progress on;
  - new change of supplier processes;
  - utilising the ZigBee protocol;
  - completing SMETS 2;
  - PKI and key management detail & processes;
  - UTRN definition;
- Responses to a request for a costing update are being analysed.

Objective is to provide an optimal solution that is proportionate and:

- *minimises risks to critical national infrastructure;*
- *minimises reputational damage to smart metering;*
- *places trust with responsible parties;*
- *provides a cost-effective, workable, low risk solution;*
- *provides an acceptable customer experience e.g. data privacy /change of supplier;*
- *minimises risks of fraud;*
- *minimises barriers to entry for new entrants/ small suppliers;*
- *can cope with future changes to business & operational processes;*
- *provides headroom for additional controls as new threats emerge*

# Security architecture update - 2

- A further (expanded STEG) security architecture workshop is being arranged;
- The purpose is to:
  - review the work in progress;
  - consider options for implementation;

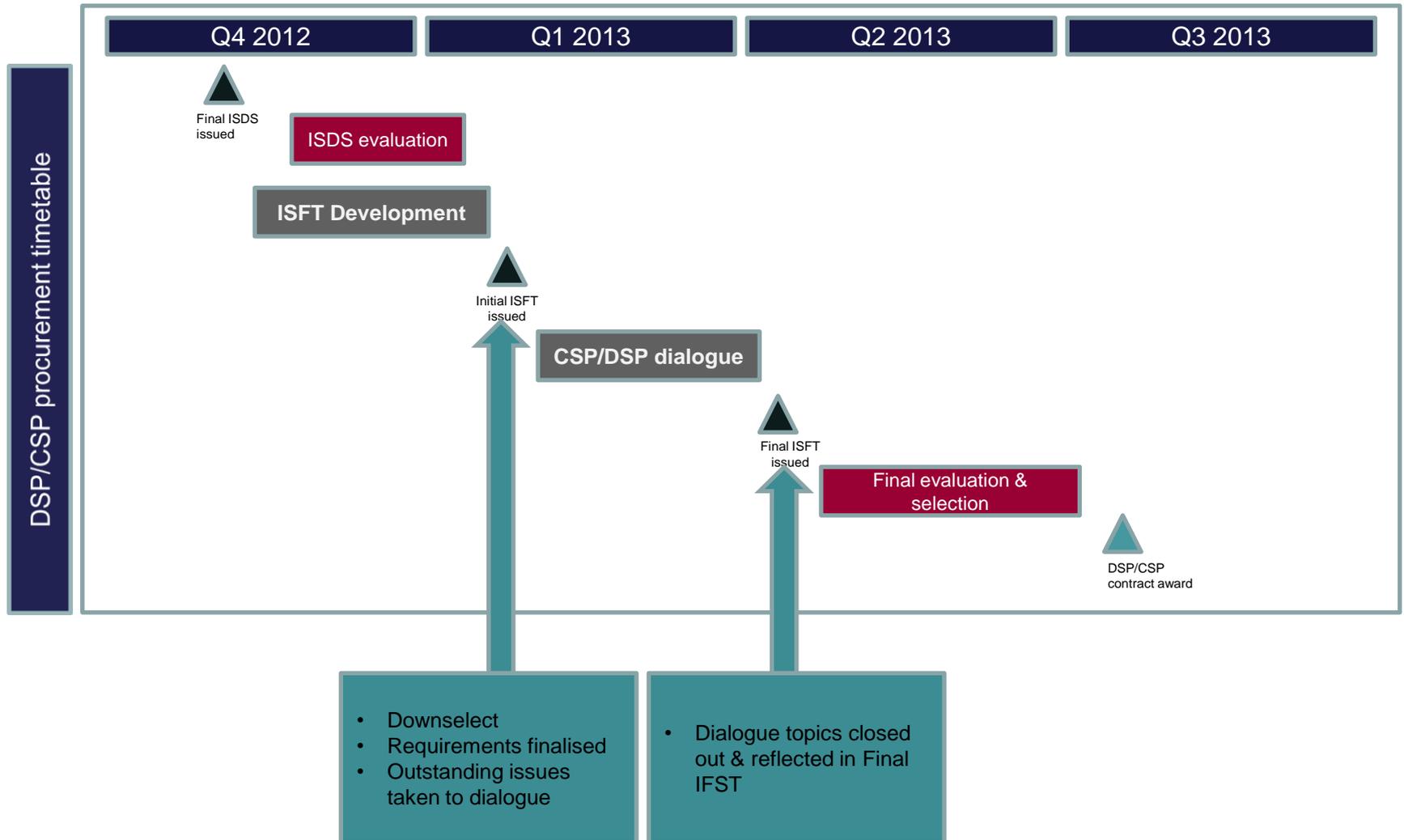
## Other security work underway:

- Update the Risk Assessment (initiation workshop 29 November);
- Update the Security requirements (to produce V0.6);
- Initiate action to identify the security characteristics for a CPA scheme;
- Address new and changed CNI risks (workshop to be arranged January 2013);
- Complete the security input to SMETS 2 and continue the Companion Spec;
- Continue to shape the roles & responsibilities under SEC;
- Progress proposals for accreditation, certification & assurance regimes for:
  - DCC; and
  - DCC Users.

## 4. PLANS FOR STRATEGIC REVIEW OF TECHNICAL REQUIREMENTS SECTIONS OF THE ISDS (CSP & DSP)

*Lesley Keable*

# DSP/CSP procurement timeline



# Review of ISDS technical requirements



- Walkthrough major themes/issues at SDAG 18<sup>th</sup> December
- Only material technical/strategic comments to be provided
  - Focus on high priority material issues for procurement
  - “Top 10”
- Cut off for any review comments **mid-day 14<sup>th</sup> December** for consideration at next SDAG
- Templates for review comments to be provided
- Due to timescales, unable to provide responses to individual comments

## In scope

- Strategic issues relating to technical requirements (i.e. gaps/areas which materially impact Service Users)
- Changes to FRs since last BPDG review
- Changes arising from security architecture revisions
- Comms hub (CSP Schedule 2.1, Schedule 11)
- DCC interfaces – DCC Service User focus
  - DCC User Gateway
  - DCC Self service interface
  - Registration Systems interface
- DCC User Gateway Catalogue

# Scope of feedback

## Out of scope

Comms Hub Technical Spec

Service levels & volumetrics

Security requirements

Service management

Foundation Support

Testing & trialling

SSAG/SDAG

Commercial Working Group

STEG

Commercial Working Group

FTTS ( Foundation, Testing and Trailing),

Foundation Steering Group

FTTS & Foundation Steering Group

# Functional requirements

## Changes since last BPDG

### Changes as a result of security architecture

#### Addition of requirements for,

- Transitional CoS Service
- Transform Service
  - still listed under access control section but greater emphasis on this functionality
- Anomaly Detection requirements

#### Update of requirements for,

- Revised definition of DSP scheduling requirements
  - distinction between schedules controlled by the SMS and the DSP
- Security Credentials requirements to add detail and align with the revised security model
- DCC Self Service Interface
  - further definition provided
- WAN Service Coverage Map
  - coverage at postcode level. No requirement to provide GIS tool

#### Update of requirements for (Cont..)

- Data Storage
  - Audit Data retention
- Firmware compatibility testing
  - restricted to environment provision only as a service

#### Removal of requirements for,

- UTRN requirements
  - transferred to Energy Suppliers or form part of the Supplier X service

## Key issues “in progress”

- CIN requirements
- CAD/ HHT Pairing
- Supplier X
  - awaiting costs from bidders
  - subject to cost benefit analysis

## **5. UPDATE ON INSTALLATION AND MAINTENANCE PROCESSES (INCLUDING THE USE OF HANDHELD TERMINALS)**

*Mark Robins*

- Objectives of SDAG discussion
  - Presentation of proposed approaches to supporting installation and maintenance when **no WAN is available**
  - *Options may be applied when WAN is available to improve operational efficiency*
- In scope
  - Valid and reasonable approaches to installing and maintaining smart metering equipment where no WAN is available during the site visit
- *Not* in scope
  - Full list of installation and maintenance business processes

- HHT Requirement Sources
  - Consultation Responses
  - Consolidated Supplier Requirements from the HHT Working Group
- Broad Summary of Requirements:
  - Capability required to support installation processes with the HHT where the WAN is not present
  - Capability required to support maintenance processes with the HHT where the WAN is not present
  - Interoperable installation/maintenance interface required to all equipment
  - Any solution must not compromise system security
  - All actions performed on the SME are authorised by the supplier

# Installation and Maintenance Approaches



No HHT, no pre-configured Smart Metering Equipment (SME)

- Leave existing meters in place / replace with new 'dumb' / smart-ready meters

No HHT, pre-configured SME

- All metering equipment replaced with pre-configured SME, with configured HAN

GPRS PicoCell to establish WAN temporarily

- Perform installation and maintenance functions through the WAN
- Self-authentication through the metering equipment user interface

Engineering menu

- Engineering menu on SME to perform installation / maintenance functions

HHT Connected Through Dedicated Configuration Interface

- Industry-standard optical part
- Perform installation functions only

Configuration Code Programming

- "switch to credit mode"; "enable supply" emergency configuration codes

Pass-through HHT

- An installer can use a HHT to apply signed commands pre-loaded on the device to the metering equipment

Restricted HHT

- The HHT operator may perform a limited set of actions through the HHT menus to perform maintenance functions on the SMS  
*This is the way maintenance field tools work today*

# 1. No HHT, no pre-configured SME

- In the event of WAN being unavailable:
  -  Leave existing meters in place / replace with
    - new 'dumb' / smart-ready meters
  -  The consumer would not be provided with an IHD (no possibility to configure the HAN)
- An unresolvable configuration problem will require the relevant equipment to be replaced
  -  Any dumb meters installed will not provide consumers with benefits of smart metering
    - E.g. will have limited tariff capability, not compliant with SMETS 2
  -  Any smart-ready meter would have to be replaced with a meter pre-configured with the correct tariff to effect a tariff change for a consumer

NO IMPACT ON SMETS / CHTS

## 2. No HHT, pre-configured SME

- Pre-configured SME installed comprising communications hub, smart meters + IHD + optional PPMID
  - Smart ready, able to connect through the WAN in the future should this option become available
  - In the event of any component failure, the entire SME would need to be replaced, as this equipment can only be installed as a pre-configured set
  - **No support for tariff upgrade** except by replacing entire SME

NO IMPACT ON SMETS / CHTS

### 3. GPRS PicoCell to establish WAN temporarily

- Installer has equipment to create a temporary GPRS cell
  - Time-consuming to set up, may not always be possible
  - Can perform all installation and maintenance functions through the WAN

NO IMPACT ON SMETS / CHTS

# 4. Engineering Menu

- SME provides menu access through local user interface (push-buttons and display)
  - Authentication through PIN code
  - Once authenticated, operations can be performed using an engineering menu
  -  **Not practical or reliable for configuring tariffs**
    - Could be used to configure load switching times, **but with risk of human error**
  -  Any critical functions available from the menu left enabled would present a significant security risk

# 5. HHT Connected Through Dedicated Configuration Interface



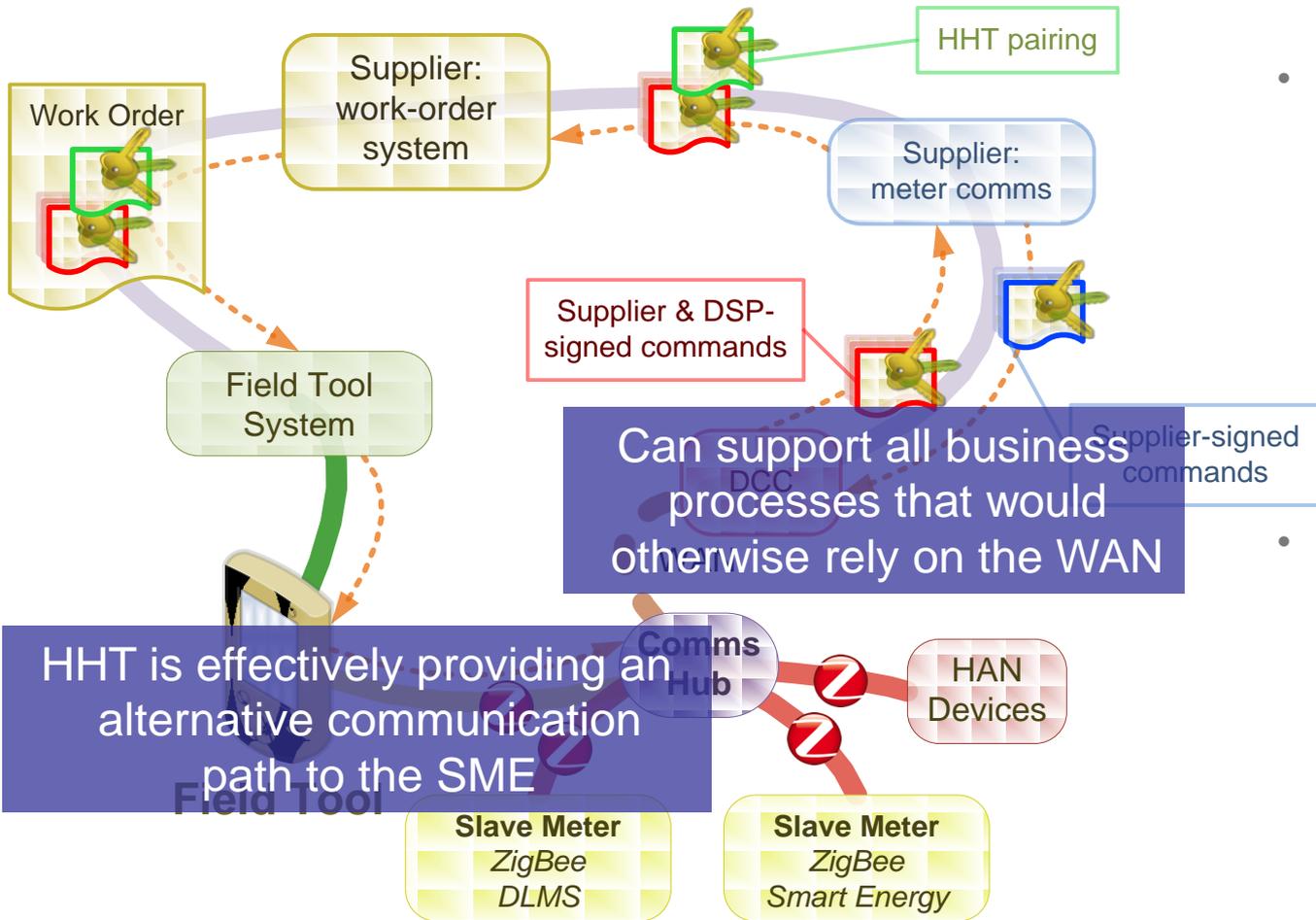
- Industry-standard optical interface on meter
    - Once authenticated, operations can be performed using a field tool
      - Can be used to perform complex configuration including tariff programming and load switching times
-  If left enabled, would present a significant security risk

## 6. Configuration Code Programming



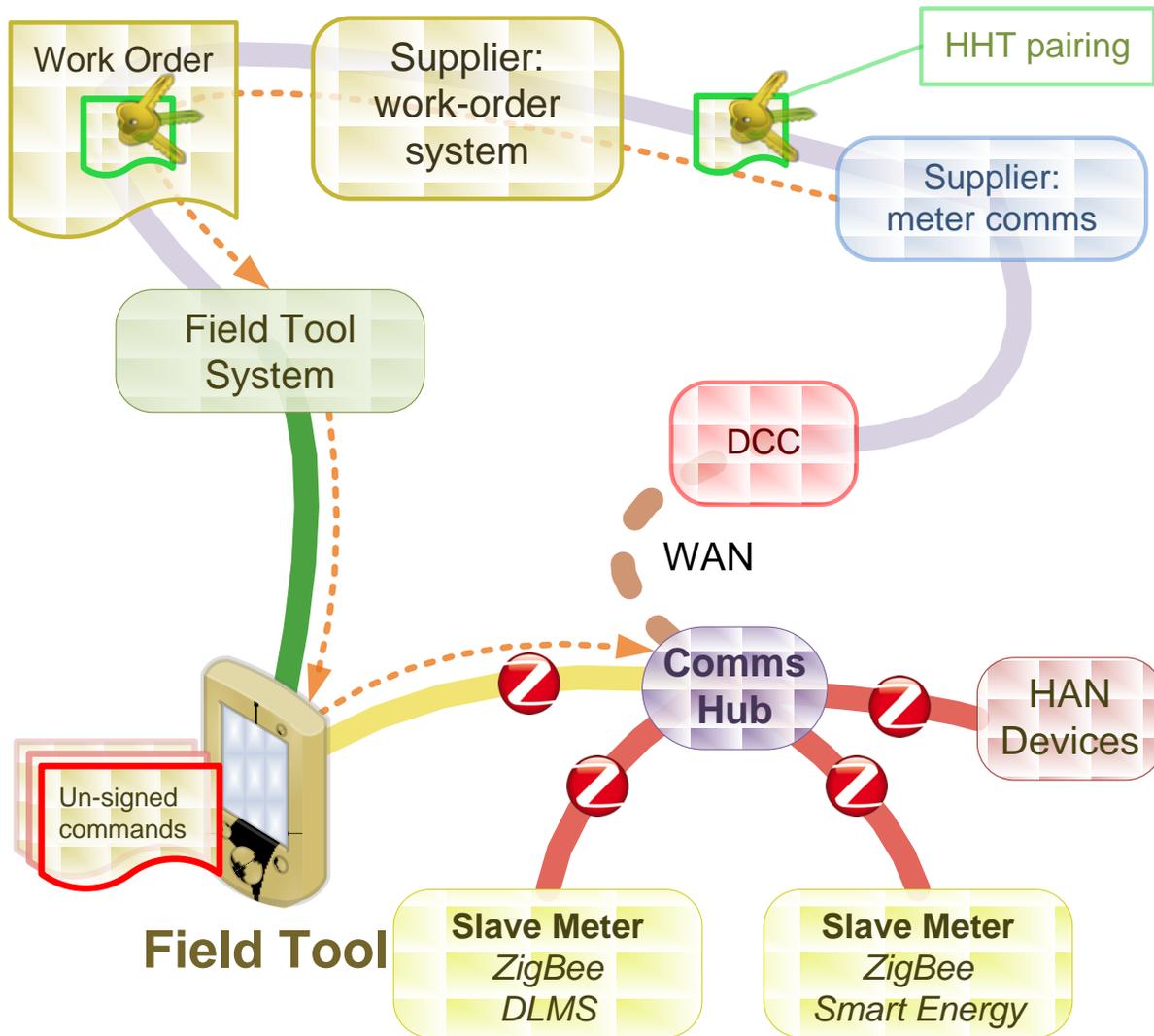
- Configuration codes, similar to UTRN, which could be used to perform emergency maintenance functions
  - Switch to Credit Mode: For use where a prepayment consumer has an unreliable WAN/HAN, and the supplier requires them to be switched to credit mode immediately
  - Enable Supply: For use where a consumer must be put on supply immediately, and the consumer is unable to perform this action remotely
  - Codes would only work on the target meter, and would only be accepted once by the meter

# 7. Pass-through HHT



- Signed commands and signed device pairing pre-loaded on device together with the work-order
  - Includes supplier and DSP signing according to current security model
- HHT operator may be allowed to select which signed messages to apply, e.g.
  - Open/close contactor/valve

# 8. Restricted HHT



- HHT can be used like current field tools
    - HHT operator able to perform a limited set of actions from menus
  - The SME must recognise a HHT device and limit the commands accepted
    - Scope of allowed interface defined in a HHT interface specification
    - Commands from HHT will not be signed
- Vulnerable to attack through misuse of HHT / through the HHT interface

## 6. DATE OF NEXT MEETING

# Date for Next Meeting



## Next Meeting(s)

- Confirm Meeting 2: 18 December 2012  
BIS Conference Centre, 10am – 3pm,  
Formal invite to follow.

## 7. AOB