Consumer Access Devices (CADs) & GB Smart Metering

Foreword

Context

Consumer Access Device (CAD) is the term used in this document to describe a Device which:

- is chosen by the Consumer and not provided under Energy Suppliers' SMETS rollout obligation;
- via the Data Communication Company (DCC), can:
  - be allowed to communication on a GB Smart Metering home area network (SMHAN). This allows the CAD to access data about other Devices on the SMHAN, but does not give access to information about the supply of Gas or Electricity to the Premises;
  - when permitted to do so, be allowed access to Gas information, as laid out in CHTS 4.5.3 (via the GPF);
  - and / or be then allowed access to Electricity information from each of the ESME / SAPC on the SMHAN. Specifically, these are the data items that are annotated '[INFO]' in SMETS sections 5.7.1, 5.7.4 and 5.7.5 (for ESME) and SMETS sections 9.6.1, 9.6.2 and 9.6.3 (for SAPC). Note that additional information could be available, but that is dependent on the make and model of the ESME / SAPC; and
  - have that access to GPF / ESME / SAPC / the SMHAN withdrawn.

Note that CADs cannot access any other SMETS defined information from any other Device types, so cannot access SMETS information from GSME, HCALCS, PPMIDs or IHDs.

Purpose

This document is intended to assist providers of CADs to the GB market, with ensuring the Devices can function effectively and without adverse effects on other Devices. Specifically, the document covers the requirements in the Technical Specifications, that such providers might need to be aware of, and the implications of those requirements from a CAD perspective.

Note that this paper focuses mainly on home area networks containing SMETS2+ Devices for which all operation is via the DCC. SMETS1 Devices vary significantly by Device Model, in terms of technical implementation, and so the technical functioning of CADs with such Devices varies correspondingly.

SEC Requirements

In GB, there are no regulatory requirements for (or indeed definitions of) CADs and so the term is rarely used in the SEC[1]. However, there are, in effect, SEC requirements that come from the need for a CAD to be able to:

[1] The SEC uses the term 'Type 2 Device' which means 'A Device that is not required to have a Device Log.'. There are no SEC requirements for a CAD, so CADs are Type 2 Devices, as are IHDs. CADs can include an

- be admitted to a Smart Metering HAN (SMHAN) and leave a SMHAN; and
- operate effectively on that SMHAN, including through Device replacement; and
- access information related to Gas and Electricity over that HAN (from ESME, SAPC and GPF).

References

This document refers to:

- the Smart Energy Code (SEC) of which the Technical Specifications form a part. All parts of the SEC can be found at https://smartenergycodecompany.co.uk/the-smart-energy-code-2/;
- the ZigBee specifications, details of which can be accessed through the link in the GB Companion Specification (part of the SEC);
- GB supply licences (which GB Energy Suppliers must comply with) which can be found at https://www.ofgem.gov.uk/licences-industry-codes-and-standards/licences/licence-conditions.

In this document, the key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**" and "**MAY**" are intended to be interpreted as described in IETF RFC 2119.

interface to the SMHAN and have additional interfaces such as to the internet (so acting as a 'gateway'), but additional interfaces are not required.

Contents

CAD requirements

Gaining admission to a GB SMHAN (and not being ejected from it)

Suppliers are required to admit CADs to an SMHAN, and give CADs access to Gas / Electricity information, if the Consumer asks[2]. Alternatively, a third party (e.g. the CAD provider) can do that for the Consumer using the DCC[3], either directly (as a SEC Other User) or via a provider of such 'CAD joining' services.

There are, however, provisions for the Supplier to remove a CAD if the CADs' behaviour interferes with the operation of other devices on the SMHAN[4]. This may happen, for example, if the CAD causes significant numbers of 'Unauthorised Communication Access attempted' Alerts from other Devices (code 0x8F3E – see GBCS 16.2). Therefore, CADs should be designed to minimise the impact on other SMHAN Devices.

A CAD **MUST** meet a number of technical requirements, if it is to successfully be admitted to any GB SMHAN:

1. it **MUST** be 'capable of joining a ZigBee SEP (ZSE) Smart Metering Home Area Network which operates within the 2400 – 2483.5 MHz harmonised frequency band or Sub GHz Bands'[5]. The CAD, therefore, would need corresponding ZigBee certification;
2. it **MUST** support the ZSE Key Establishment Cluster as both a client and a server, as specified in Annex C of ZSE and 'Crypto Suite 2' (GBCS 13.7.2). Therefore, the associated ZigBee implicit certificates need to be installed on the CAD before deployment;
3. it **MUST**, as per ZSE 6.1 support the Basic cluster as a server, and any ZigBee Smart Energy mandated Clusters for its ZigBee device type. Note that, if the CAD's ZigBee device type is 'In-Home Display', there are no further mandated clusters;
4. it **MUST** support all mandated attributes and commands within the Basic, Key Establishment and other mandated clusters; and
5. it **MUST** have an Install Code generated at manufacture which is 128 bits in length (excluding the CRC)[6], the MMO hash of which **MUST** be installed on the CAD at manufacture.

Note that the IEEE address of the CAD's ZigBee radio interface and its Install Code **MUST** both be supplied to the organisation joining the CAD, if a Device is to be admitted to a GB SMHAN[7].

[2] e.g. electricity supply licence condition 49.4(d)
[3] DCC is obliged to offer these services – SEC Appendix E, Join Service (8.7.2) and Update HAN Device Log (8.11)
[4] e.g. electricity supply licence condition 49.4(d) / SEC section I 1.3
[5] See SMETS 6.2. Note, that CADs only supporting Sub GHz Bands would only be able to operate on SMHANs where a Dual Band Communications Hub is installed – that will be a minority of SMHANs (currently expected to be ~25% of GB premises). CADs supporting 2400 – 2483.5 MHz can operate on any SMHAN.
[6] As per GBCS CCS01 Use Case, Devices must use 128 bit install codes (excluding CRC). Specifically, CCS01 states for this field in the Command: 'The octet-string containing an Install Code. As per Table 5-10 of the ZSE specification, this is a 16 octet string (so is a 128 bit install code). Note that it does not include the 16 bit CRC'.
[7] See DUIS 'Device Pre-notification' Service Request (SRV 12.2).

Staying connected to the SMHAN

SMETS Devices (so ESME, SAPC, HCALCS, GSME, PPMIDs & IHDs) are mandated in Great Britain and have to support ZigBee 'Trust Center Swapout'. This means SMETS Device will automatically re-connect to the SMHAN, if the Communications Hub (CH) is replaced.

A CAD **MAY** also support this automatic re-connection, and so **MAY** also support the ZigBee 'Trust Center Swapout' requirements.

A CAD **MAY** also support a reset mechanism, which switches it back to using the MMO hash of the Install Code as its link key (where those terms have their ZigBee meaning). This allows the CAD to be used on multiple SMHAN over its lifetime. It may also help where there are any initial communications difficulties, on installation of Devices.

For reliable SMHAN communications at the network layer, the CAD:

1. **SHOULD** also follow the requirements at GBCS 10.7, which are applicable to CAD (see 'Annex A GBCS 10.7 SMHAN requirements applicable to CADs'). Note, that a CAD **MAY** be a ZigBee Router or a ZigBee End Device, and so requirements for both are included in the Annex;
2. **SHOULD** use ZigBee's Trust Center Rejoin rather than ZigBee's Secure Rejoin, when re-joining the SMHAN, as explained at 'Annex B – TS1298 explanation: preference for Trust Center Rejoin';
3. **SHOULD NOT** initiate ZigBee CBKE unless it is to establish communications with a CH with which it does not have an existing Trust Center Link Key (so a newly installed CH), as explained at 'Annex C - TS1256 explanation: when should a device initiate CBKE?'; and
4. either **SHOULD NOT** support the ZSE Price Cluster CommodityType or the Metering Cluster MeteringDeviceType attributes, or **SHOULD** use values for those attributes that are different than those specified in GBCS 10.4.2.11 for GB Smart Metering mandated Devices. Specifically, the CAD **SHOULD NOT** use any Energy Services Interface value (since it is not a device interfacing with the Energy Supplier) and it **SHOULD NOT** use either Gas Metering or Mirrored Gas Metering (since it is not a GSME or GPF).

Accessing Electricity information

SMETS specifies the Electricity related information which an ESME / SAPC must provide to authorised Devices on the same SMHAN (and requires that this is not provided to Devices without authorisation). A CAD has to be added to an ESME's / SAPC's Device Log if it is to be authorised. This can only be undertaken through the DCC. To be successful, the CAD, therefore, **MUST** support mechanisms that are optional in ZigBee, as laid out in this section.

Specifically, if the CAD is to access information about Electricity (so from ESME / SAPC), it **MUST** support the 'Partner Link Key' mechanisms specified in ZSE 5.4.7.4 / GBCS 13.7.2 including the establishment of CBKE based Link Keys, with that CBKE being initiated by ESME / SAPC the CAD has been authorised to communicate with.

A CAD **MAY** access the MeteringDeviceType attribute in the Metering cluster to establish which SMHAN Devices are ESME / SAPC, and so which Devices it **SHOULD** request 'Partner Link Keys' for, when it first accesses an SMHAN (so that it is prepared for any subsequent authorisation). Access to this attribute is not constrained by access controls (DBAC) in GBCS13.7.2 to support this process. GBCS 10.4.2.11 specifies the values GB mandated Devices must use and so those that will be used

by any ESME / SAPC. For each ESME / SAPC, the CAD **SHOULD** request a Partner Link Key from the CHF (which acts as the ZigBee Trust Center).

A CAD **SHOULD NOT** attempt to read any 'SMETS data' from any ESME / SAPC until that ESME / SAPC has requested CBKE with the CAD and that CBKE process has completed. If the CAD were to make such attempts, the ESME / SAPC will report unauthorised access attempts (in the form of 0x8F3E Alerts), so potentially degrading HAN performance, which could lead to the CAD being removed from the HAN.

Accessing Gas information

CHTS specifies the Gas related information which a GPF must provide to authorised Devices on the same SMHAN (and requires that this is not provided to Devices without authorisation). A CAD has to be added to a GPF's Device Log if it is to be authorised. This can only be undertaken through the DCC and does not require that the CAD supports additional ZigBee mechanisms.

However, the CAD **SHOULD** have mechanisms to detect when it is not authorised to access Gas data and to 'back off' in such cases. The lack of authorisation **MAY** be detected by a CAD by:

1. attempting to read the GPF's *MeteringDeviceType* attribute (which does not require authorisation) and receiving a successful response. This check is to confirm that the CAD can communicate with the GPF; and
2. attempting to read a GPF attribute from the GPF Gas ESI that does require authorisation (e.g. *CalorificValue*) and not receiving a successful response. This confirms that, whilst the CAD can communicate with the GPF, the GPF will not allow it access to information requiring authorisation. Therefore, the CAD does not have authorisation.

In such cases, the second read will cause an Alert to be sent to the Gas Supplier. The CAD **SHOULD** therefore incrementally back off, in terms of the timing of any retries for reading attributes requiring authorisation. This is so as not to generate excessive volumes of 0x8F3E Alerts to the Gas Supplier (which could lead to the CAD being removed from the SMHAN by that Supplier).

Further details can be found at 'Annex D – TS0793 explanation: Minimising unauthorised access attempt alert Alerts'.

Change of Tenancy

For GPF (CHTS 4.5.4.10) and ESME (SMETS 5.6.3.31) there are requirements not to share historic data relating to the prior tenancy with SMHAN Devices. This means that the CAD can be authorised to access Gas and / or Electricity information but would not gain access to some historic data. Where the CAD accesses such historic data, it **SHOULD** factor in this 'Change of Tenancy' related limitation on access. Note though, that the date of the Change of Tenancy is not available to the CAD in current SMETS2 versions and as such alternative mechanisms need to be utilised. Further details can be found at 'Annex G – TS0830 explanation: Change of Tenancy'.

Accessing information from other HAN Devices

Information that is available over the SMHAN is detailed in GBCS Table 7.4. For a CAD, that information falls in to three categories:

1. Electricity information available from the ESME / SAPC which is required by SMETS, and so will only be available if the CAD has been added to the ESME / SAPC Device Log. Note that SAPC may additionally support other ESME functionality, and so may share additional data listed under the ESME entries;
2. Gas information available from the GPF which is required by CHTS, and so will only be available if the CAD has been added to the GPF Device Log; and
3. Information available to all SMHAN Devices. This includes the CHF date / time, keepalive mechanisms and Sub GHz mechanisms.

These categories are detailed in the following embedded documents:


ESME%20and%20SAPC%20data%20for%2


GPF%20data%20for%20CADs%20(1).xlsx


CHF%20data%20for%20CADs.xlsx

Pulling information & getting it pushed

CADs **MAY** request information, from Devices they are authorised to access, by:

3. For ZigBee attributes, sending a ReadAttributes command; and
4. For ZigBee 'publish' commands, sending the corresponding 'get' command.

CADs **MAY** also use ZigBee's 'binding' mechanisms to have information pushed to them from the GPF / ESME / SAPC whenever it changes. Specifically, ESME / SAPC & GPF needs to push the following ZigBee commands to authorised Devices registered with them (so where the Device has sent a corresponding ZigBee Bind Request to the ESME / SAPC / GPF for the relevant Cluster(s)):

- Calendar cluster:
  - Publish Calendar command (for ESME / SAPC whenever any part of a calendar except special days changes; for GPF, when the GSME confirms, as part of the TOM mechanism, any part of a calendar except special days changes) ; and
  - PublishSpecialDays (for ESME / SAPC whenever any special days change; for GPF, when the GSME confirms, as part of the TOM mechanism, any special days change).
- Price cluster:
  - Publish Price command (for ESME / SAPC, whenever a new tariff is accepted and whenever it changes the current price; for GPF, after the GSME confirms as part of the TOM mechanism that a new tariff is accepted, and whenever the GPF calculates that the GSME should have changed the current price[8]); and
  - PublishTariffInformation (for ESME, whenever a new tariff is applied; for GPF, when the GSME confirms, as part of the TOM mechanism, the price / tariff has changed).
- Events Cluster:
  - Publish Event command (for ESME / SAPC, whenever it is required to send a HAN Alert; for GPF, when a corresponding command, requiring a HAN Alert, is pushed by the GSME).
- Message Cluster:
  - Display Message command (for ESME / SAPC, whenever it has accepted a new supplier message; for GPF, when the GSME confirms, as part of the TOM mechanism, it has accepted a new supplier message).

[8] There may be cases where the GPF is somewhat out of line with the GSME e.g. where the GSME clock and the GPF clock have different times but in normal circumstances this will be no more than 10 seconds.

For further information, see *'*Annex F – TS0932 explanation: ESME & GPF requirements to push information*'*.

Sub GHz CAD requirements

CADs **MAY** be built to operate on Sub GHz frequencies. This functionality can be used in SMHANs where the Communications Hub is a Dual Band Communications Hub (DBCH). To ensure that such Sub GHz CAD operation stays within bandwidth usage requirements, and so avoid the risk of being removed from the SMHAN, the CAD **SHOULD** comply with GBCS requirements for Sub GHz Devices (but excluding those for Sub GHz GSME or CH). Specifically, a CAD:

- **SHOULD NOT** act as a ZigBee router when operating on a Sub GHz Channel;
- **SHOULD**, where the CAD can also support 2.4 GHz operation:
  - on first connecting to a ZigBee network, attempt to establish network communication in the 2.4GHz band. Only where communications are not of sufficient quality, **SHOULD** the CAD attempt to establish network communications in the Sub GHz band; and
  - having connected to a ZigBee network at either 2.4 GHz or at Sub GHz, not attempt to change to the other of 2.4 GHz or Sub GHz except when undertaking a Trust Centre re-join, with its ZSE meaning; and
- **SHOULD NOT** use the Mgmt_NWK_Unsolicited_Enhanced_Update_notify command to notify the CH of problems with its communications link more frequently than once in any 30-minute period.

Annex A GBCS 10.7 SMHAN requirements applicable to CADs

In this Section, all terms in italics have their ZSE or ZigBee Specification meanings and ZS means the ZigBee Specification.

Where a CAD is not a ZigBee *end device*, the *nwkLeaveRequestAllowed* attribute of the *NIB (Network layer information base)* **SHOULD** be set to *FALSE*. This means that, in line with the ZigBee specification, *Leave* commands received by such CADs **SHOULD** be immediately and silently discarded and such CADs **SHOULD NOT** leave the SMHAN on receipt of such *Leave* commands.

When a CAD, which is a ZigBee *end device*, has received and executed a ZigBee *Leave* command with a value in the *Rejoin Sub-Field* of 0, the CAD **SHOULD** attempt to re-establish SMHAN communications using the ZSE 5.4.2 mechanisms.

In line with the 'ZigBee PRO/2007 Layer PICS and Stack Profiles' requirement, CADs **MUST** be capable of maintaining a minimum of two *Network Keys*.

Should any CAD not receive new *Network Keys* from the CHF and the instruction to switch to it, that CAD will discover a communication failure. In such circumstances, the CAD **MUST** use the ZSE 5.4.2 ('Re-joining a Secured Network') mechanisms to re-establish communications.

When a CAD receives a new *Network Key*, the CAD **SHOULD** only store that *Network Key* where either:

1. the CAD does not currently hold any *Network Key* (so meaning it is being installed); or

2. the CAD receives the new *Network Key* encrypted with a hash of its *Trust Center Link Key* (so meaning that a *Trust Center Swapout* is in progress); or

3. the CAD receives the new *Network Key* encrypted with its *Trust Center Link Key* (and potentially with an existing *Network Key*) and either:

    a) the value of *KeySeqNumber* for the new *Network Key* is greater than the value of the CAD's *nwkActiveKeySeqNumber*; or

    b) the CAD's *nwkActiveKeySeqNumber* is greater than 127 and the value of *KeySeqNumber* for the new *Network Key* is not greater than (*nwkActiveKeySeqNumber* + 128) modulo 256.

Where a CAD stores a new *Network Key*, it **SHOULD** switch to using that new *Network Key* for outgoing messages where either:

- it does not hold any other *Network Key*;
- it received the new *Network Key* encrypted only with a hash of its *Trust Center Link Key*; or
- it receives a message validly encrypted with the new *Network Key*.

Where a CAD stores a new *Network Key* and that storage leads to the CAD needing to remove details related to an old *Network Key*, the CAD **SHOULD** remove the *Network Key* that it received furthest back in time, and remove the *nwkSecurityMaterialSet* details associated with that key.

Where a CAD receives a *switch-key* command requesting that it switches to using a new *Network Key*, the CAD **SHOULD** only act in response to that command where either:

1. the value of the '*sequence number*' parameter in the *switch-key* command is greater than the value of the CAD's *nwkActiveKeySeqNumber*; or

2. the CAD's *nwkActiveKeySeqNumber* is greater than 127 and the value of the '*sequence number*' parameter in the *switch-key* command is not greater than (*nwkActiveKeySeqNumber* + 128) modulo 256.

Where a CAD switches to using a new *Network Key*, the CAD **SHOULD**:

- in line with ZS 4.3.4 (and contrary to ZS 4.6.3.4.2), only set the associated *OutgoingFrameCounter* to zero if *OutgoingFrameCounter* is currently greater than 0x80000000; and
- ensure that, in the *IncomingFrameCounterSet* within the *nwkSecurityMaterialSet* for this new *Network Key*:
    - For a CAD which is not an End Device, any SenderAddress is an identifier for a Device that is in the CAD's nwkNeighborTable;
    - For a CAD which is an End Device, the only SenderAddress is the identifier for the CAD's current parent Device; and
    - In line with ZS 4.6.3.4.2, all IncomingFrameCounters are set to zero.

A CAD **SHOULD**:

- only increment the value of the *IncomingFrameCounter* for the sending Device as a result of processing incoming messages from the sending Device which are secured with the *Network Key* the receiving Device is currently using for outgoing messages; and
- whenever it removes a Device from its *nwkNeighborTable*, also remove that Device's details from the *IncomingFrameCounterSet* within the *nwkSecurityMaterialSet* for the *Network Key* it is currently using to secure outgoing messages.

For the purposes of aging out entries from the *nwkNeighborTable*, a CAD **SHOULD**, where it is a *Router*:

- only use the ZS table 3-58 specified default values for *nwkRouterAgeLimit* and *nwkLinkStatusPeriod*, so 3 and 15 seconds respectively;
- set bit 0 of *nwkParentInformation* to 0b0, and so bit 1 to 0b1, meaning that *End Devices* need to send *End Device Timeout Request* commands as a unicast to refresh the *keepalive timer*;
- Only refresh the *keepalive timer* when the *Network Key* used to secure such *End Device Timeout Request* commands is that currently in use by the Device for its outgoing messages; and
- have the *nwkEndDeviceTimeoutDefault* set to the default 8 (so meaning 256 minutes) in line with ZS table 3-58 and not change the value of a Device's *keepalive* timeout where it receives an *End Device Timeout Request* command with a *Requested Timeout Enumeration Value* greater than 10 (so meaning greater than 1,024 minutes).

When a CAD has chosen a network to join, it **SHOULD** remove *Neighbor table entries* corresponding to Devices that are not members of the chosen network.

Where a CAD is an *End Device*, the CAD **SHOULD NOT** send an *End Device Timeout Request* command with a *Requested Timeout Enumeration Value* greater than 10 (so meaning greater than 1,024 minutes).

Annex B – TS1298 explanation: preference for Trust Center Rejoin

In summary:

- All GB mandated Devices must support Trust Center rejoin, due to the GBCS 10.4.2.11 requirement to support Trust Center Swap Out;
- The benefit to always using Trust Center rejoin is that its successful completion relies on successfully communicating with the CH, so meaning a successfully rejoining Device is on the current radio channel, and gets the current Network Key (see the ZigBee Specification Table 4-24). Note that the CH as the Trust Center controls both changes to radio channels and changes to Network Keys; and
- ZigBee's Secure Rejoin only necessarily involves the rejoining Device's parent, which may not be the CH and so does not ensure that the rejoining Device is either on the current radio channel, or gets the current Network Key (see the ZigBee Specification Table 4-23).

Annex C - TS1256 explanation: when should a device initiate CBKE?

Issue

When should ZigBee End Devices initiate CBKE with the Communications Hub (so with the Trust Center, in ZigBee terminology)?

Explanation:

In summary:

- an End Device must initiate CBKE when (1) it first joins a HAN and (2) when the CH on the HAN is physically swapped out;
- End Devices are not required to initiate CBKE under other conditions, although are not banned explicitly from doing so; and
- however, given the consequences of CBKE, including in shortening Device's lives and the load on wider systems, End Devices should initiate CBKE under other conditions only if they bring sufficient benefit.

By way of context, CBKE between an End Device and CH is the mechanism ZigBee uses to establish a shared, symmetric key (called the Trust Center Link Key). It is known only to those two Devices. Once established, it is used to secure most (but not all) of the communications between the CH and End Device (see ZSE Table 5-12). An End Device can check it has a valid Trust Center Link Key by using is to read some CH information, for example the CHF's Time attribute (this is not subject to additional GBCS DBAC, and so is available to any End Device that is allowed on the HAN, so is in the CHF Device Log). This attribute is in the Time cluster which ZSE Table 5-12 requires is accessed using the Trust Center Link Key, so can be used to tell that a Link Key is properly operating.

An End Device must initiate key establishment:

- when it first joins the HAN (so after it has first been whitelisted on the CHF, by being added to the CHF Device Log, and communications established using the End Device's Install Code), as per ZSE Figure 5.5 /5.4.7. This establishes the Trust Center Link Key between the CHF and End Device – this key is a shared symmetric key that is known only to the CH and End Device; and
- when the CH has been swapped out and communications have been established using the hash of the Trust Center Link Key, as per ZSE 5.4.2.2.3.5.

A ZigBee End Device would not initiate key establishment:

- If it is added to the same CHF Device Log a second or further time (e.g. where it has been removed in error). The End Device would be unaware that this had happened. The End Device may attempt the fall backs for Trust Center swap out, in the period where it is not in the CHF Device Log, but these would fail until the Device is re-added. At that point, the original TC Link Key would still work, so there is no trigger for CBKE; and
- As a result of 're-registration'. This is a ZSE concept that is not used in GB; and
- A ZigBee End Device may, as per ZSE 5.4.5, additionally change Link Keys (so by initiating CBKE) with Devices that are NOT the Trust Center (so are not the CH, so for Link Keys other than the Trust Center Link Key), as per ZSE 5.4.5. However, there is no requirement to do this and no clear circumstances where it would be beneficial.

Whilst there is no explicit prohibition on End Device's initiating CBKE in other circumstances, there are negative consequences of so doing:

- The symmetric keys produced have to be stored by Devices in storage that survives power loss. Such storage can typically only be written a finite number of times in its life, before it becomes unreliable. Device lifetimes are likely to have assumed very small numbers of CBKE occurrences, so a low number of writes. Significantly larger number of occurrences would likely reduce Device's usable lives. This is true of both the End Device and CH; and

- To support Trust Center swap out, a backup of the CHF Device Log (which contains hashes of all Trust Center Link Keys) is sent by the CHF to the DSP every time the log changes, so including every time CBKE occurs. Scaling for the corresponding parts of DSP Systems are based on CBKE with the CH being undertaken only when needed. Use in other circumstances increases the load on, and so potential costs of, DCC Systems.

Annex D – TS0793 explanation: Minimising unauthorised access attempt alert Alerts

TS0793%20Minimisin
g%20unauthorised%2

Annex E – TS0893 explanation: Historic Personal Data on the HAN

TS0893%20-%20Hist
oric%20data%20on%

Annex F – TS0932 explanation: ESME & GPF requirements to push information

TS0932%20-%20ESM
E%20&%20GPF%20re

Annex G – TS0830 explanation: Change of Tenancy

TS0830%20-%20GPF
%20and%20Change%