Making Everything Easier!™

Special Edition

Smart Metering Implementation Programme For Dummies®

A Wiley Brand

With the compliments of

CGI

Chris Beard

About CGI

CGI is a global business with 68,000 professionals in 40 countries across the Americas, Asia–Pacific and Europe who provide end-to-end IT and business process services that facilitate the on-going evolution of our clients' businesses.

Across the UK, we have around 6,000 members with specific industry knowledge and a broad range of client experience, making CGI a true local partner.

CGI is a pioneer of innovative technology in the utilities sector, with 3,000 consultants worldwide delivering innovative solutions to our clients' most complex business challenges.

CGI has been at the heart of every major change in the UK energy market since privatisation, helping clients to thrive in changing times. We enable network operators to implement smart grids, creating a reliable, economic, sustainable low-carbon energy infrastructure; we support the Data Communications Company (DCC) by delivering the systems at the heart of Britain's Smart Metering Implementation Programme and we help DCC Users to connect to these systems and realise the benefits of smart metering.

CGI

Experience the commitment®

www.cgi-group.co.uk/utilities
enquiry.uk@cgi.com

facebook.com/CGI.UK
twitter.com/CGI_UKNEWS
linkedin.com/company/cgi
youtube.com/user/CGIGroup

Smart Metering Implementation Programme

FOR DUMMIES®

A Wiley Brand

By Chris Beard

FOR DUMMIES®

A Wiley Brand

Smart Metering Implementation Programme For Dummies®

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

For details on how to create a custom *For Dummies* book for your business or organisation, contact `CorporateDevelopment@wiley.com`. For information about licensing the *For Dummies* brand for products or services, contact `BrandedRights&Licenses@Wiley.com`.

Visit our Home Page on `www.customdummies.com`

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER, THE AUTHOR, AND ANYONE ELSE INVOLVED IN PREPARING THIS WORK MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN: 978-1-119-12229-6 (pbk); 978-1-119-12228-9 (ebk)

Printed and bound in Great Britain by Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Table of Contents

Chapter 9: Life as a DCC User 125

Chapter 10: The Future 141

Introduction

Welcome to *Smart Metering Implementation Programme For Dummies*, your essential pocket guide to the Smart Metering Implementation Programme. This book has it all – action, suspense, romance and a broad introduction to one of the most challenging industry programmes ever attempted in Great Britain. (Well, one out of four isn't too shabby!)

About This Book

If you've bothered to pick up this book, you're probably already aware that the UK government has mandated energy suppliers to roll out smart meters to all their domestic and small business customers in Great Britain by 2020. To achieve this, the Department of Energy and Climate Change (DECC) has created the *Smart Metering Implementation Programme (SMIP)*, a customer-focused, supplier-led approach to rolling out an estimated 53 million smart electricity and gas meters to more than 30 million homes and small businesses across Great Britain.

The SMIP is a behemoth of a programme, arguably bigger than any other retail utility industry change programme to date. Its 51 industry working groups represent just the tip of an iceberg of individuals, all slaving away to make the largest single rollout of smart meters ever attempted in the world a reality.

This book makes an ambitious attempt to summarise the key features of the programme, its main stakeholders and the smart metering infrastructure it aims to deliver.

Foolish Assumptions

I've made a few assumptions while writing this book.

- You're not entirely unfamiliar with the GB energy industry but are looking for a relatively painless introduction to this major industry change programme that everyone else is talking about or that you've happened to end up in.
- Having read the highly entertaining chapter on the SMIP in *GB Electricity Industry For Dummies*, you'd like to know a bit more.
- You're reasonably familiar with the concept of smart meters, what they are, what they do and why everyone should want one. If you're not, I recommend a perusal of *Smart Metering For Dummies*.

How This Book Is Organised

SMIP For Dummies comes in eleven informative and easy-to-digest morsels.

- *Chapter 1: Setting the Scene:* A quick résumé of how the SMIP came about.
- *Chapter 2: Stakeholders:* A summary of the key participants in the SMIP, and their roles and motivations.
- *Chapter 3: Devices:* A brief description of the bits of kit that will hopefully end up in your home by 2020.
- *Chapter 4: Messaging:* The nuts and bolts of sending/ receiving messages via the Data Communication Company's (DCC's) infrastructure.
- *Chapter 5: Messages:* A précis of the different types of messages available to send and receive.
- *Chapter 6: End-to-End Security:* The unique security model that underpins the SMIP.
- *Chapter 7: The Smart Energy Code (SEC):* An essential digest of what's worth reading in the SEC and its vast array of SEC Subsidiary Documents.
- *Chapter 8: The SMIP:* A quick tour of the programme itself, including its working groups and phases.

- *Chapter 9: Life as a DCC User:* A crash course in becoming, and surviving as, a DCC User.
- *Chapter 10: The Future:* Some crystal-ball gazing at the role of the DCC beyond Go Live.
- *Chapter 11: Top Ten SMIP Tips:* Some pearls of wisdom for you to take away.

As those of you who've had any exposure to the utility industry well know, jargon is an insidious feature and acronyms abound. However, similar to working abroad, learning the local lingo is essential, so this guide makes unapologetic use of industry terminology throughout. I do, however, introduce each term I use, remind you of the meaning of acronyms at first use within each subsequent chapter and provide a mammoth jargon-busting glossary at the end of the guide.

Icons Used in This Book

To make navigating to particular information even easier, these icons highlight key text.

REMEMBER

Important points to keep in mind.

TECHNICAL STUFF

A warning for casual readers not wanting to get drawn into too much technical detail to turn the page.

WARNING!

This icon highlights potential pitfalls.

TIP

Here, you can benefit from the author's suggestions.

Where to Go from Here

This book aims at breadth rather than depth. It's highly likely that you have a far more detailed knowledge than the author of some areas covered, but hopefully the guide provides you with an insight into areas of the programme with which you're perhaps not so well acquainted. As with all *For Dummies* guides, you can dip in and out of this book as you like, or read it from cover to cover.

Use the headings to guide you to the information you need. If you require any more information, visit `www.cgi-group.co.uk/utilities` and feel free to contact us at enquiry.uk@cgi.com.

WARNING!

All *For Dummies* guides have a shelf life, but this is particularly true for one about a transitional programme. Inevitably, by the time you read this book some of the contents will be out-of-date so I recommend keeping your ears to the ground.

Chapter 1

Setting the Scene

In This Chapter

- Explaining how the SMIP came about
- Understanding why Britain is different to the rest of the world
- Examining how all the bits hang together, from DCC Users to devices

So, you may ask, why are we rolling out smart meters and how did we end up with the programme that we have today? This chapter attempts to answer these questions and give a very high-level overview of what we should end up with once the SMIP has successfully delivered. For those with only a passing interest in the SMIP, this chapter may be all you need to read.

Why Roll Out Smart Meters?

The national rollout of electricity and gas smart meters to domestic and small business customers is a key plank in the UK government's strategy for achieving its carbon reduction commitments. The theory goes that making us more aware of how much energy we're actually using will make us use less of it.

Currently, unless you're a prepayment customer, a massive disconnect exists between using energy and paying for it. By the time your bill arrives, the energy's long gone, and chances are that the bill's estimated and bears little relation to your actual usage. For us to start using less energy (thus, saving the world and our bank balances at the same time), we need to become more aware of the link between energy usage and its cost, not just *how much* we're using but also *when* we use it. Smart meters are the government's solution to making us more energy savvy.

Aside from the government's carbon reduction commitments, a series of government impact assessments have shown a favourable business case for a national rollout. The latest, published in January 2014, estimated the programme as costing just under £10.5 billion but returning benefits of almost £15 billion over a 19-year period. The majority of the cost (a little over £6 billion) is incurred by suppliers in providing and installing meters in homes. However, suppliers also receive the majority of the estimated benefits (£8 billion) through avoided site visits, fewer customer complaints and so on.

And if all of that wasn't incentive enough, you also have the European Directives 2009/72/EC (Electricity) and 2009/73/EC (Gas) which require member states to provide at least 80 per cent of consumers with smart meters by 2020.

Delving into the History of the SMIP

The industry has been discussing a national rollout of smart meters for an embarrassingly long time. It considered various models, from *Regional Franchise* (a centrally managed, street-by-street rollout) to *Supplier Hub* (a continuation of the status quo where suppliers are responsible for not only providing and installing meters, but also the infrastructure required to communicate with them). What we've ended up with is a hybrid *Central Communications Model* in which suppliers retain responsibility for procuring, installing and maintaining meters, but are required to use a common, franchised central communication infrastructure.

REMEMBER

In most other countries, metering is the responsibility of regulated distribution companies and any attempt at rolling out smart meters follows the Regional Franchise model. In Britain, we're a bit different. We've spent the past 20 years stripping away anything vaguely competitive from the natural monopoly businesses (that is, the network operators and their distribution assets) and this includes metering. Since 1996, the supplier has been responsible for providing settlement metering. Hence, we've ended up with a supplier-led rollout mandated through a supplier licence obligation to replace all domestic and small business energy meters with smart equivalents by 2020. I talk more about the SMIP itself in Chapter 8.

So we've ended up with a programme driven by government policy, delivered by suppliers (exhibiting varying levels of enthusiasm), partially paid for by distribution network operators (most of whom are unconvinced of the benefits), underpinned by commercial organisations (focused on delivering to their contracts) and heavily dependent on device manufacturers (who recognise the prize of 53 million sales but are struggling with ever changing requirements and a chequered track record of delivery). Not a promising start. . . .

Smart metering hasn't experienced a complete hiatus whilst the SMIP has been established. Some suppliers have elected to forge ahead in the interim, procuring their own communication services to service the smart meters they deploy in the so-called *Foundation* phase (that's the period before the DCC goes live – I talk about what's likely to happen to these Foundation smart meters in Chapter 10.)

Taking a Quick Guided Tour

For those that find even For Dummies guides hard going, these next few paragraphs may be all you need. Here's a whistle-stop tour of the key parts of the SMIP in terms of technology and stakeholders (which I pull apart in more detail in rest of the guide).

Figure 1-1 depicts the high level end-to-end architecture for the GB smart-metering rollout. At the heart of this is the *Data Communications Company (DCC)*, the body responsible for enabling communication between smart devices within the home and those who want to talk to them *(DCC Users)*. I look at the different flavours of DCC User and smart devices in Chapters 2 and 3, respectively.

In some ways, the smart metering infrastructure is the tale of three networks:

- **Home Area Network (HAN):** Smart devices communicate with each other via the HAN, a ZigBee-based network established by the *Communications Hub* (*CH*), one of the smart devices installed within the home. In addition to establishing the HAN, the CH also provides connectivity to the *SM WAN* that connects the smart devices to the DCC.

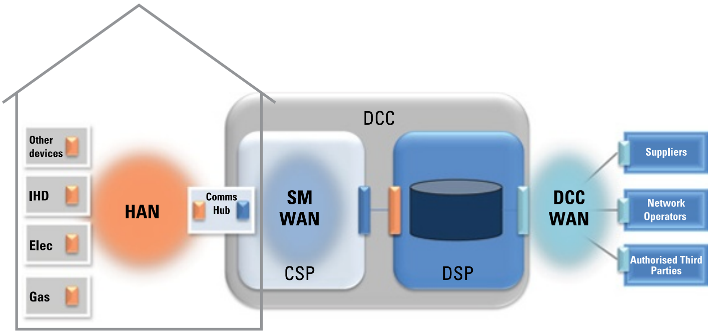


Figure 1-1: End-to-end GB smart metering infrastructure.

- **Smart Metering Wide Area Network (SM WAN):** The responsibility of the *Communication Service Provider* (*CSP*), a sub-contractor to the DCC who's also responsible for providing the CHs. National CSP WAN coverage is split into three regional contracts, held by two CSPs (Arqiva and Telefónica). The SM WANs connect the HANs to a central system, the *DCC Data Systems* provided by the *Data Service Provider* (*DSP*), another sub-contractor to the DCC (in this case, CGI).
- **DCC User Gateway Network:** In addition to providing the DCC Data Systems that manage smart communications, the DSP also provides DCC Users with a 'to-the-door' connection service comprising another wide area network (the *DCC User Gateway Network*) and a piece of kit (the *DCC User Gateway Equipment*) with which to connect to it. I take a closer look at the roles of the DCC and its service providers in Chapter 2.

The reason for this chain of networks (the HAN, SM WAN and DCC User Gateway Network) is to enable messages to be sent from DCC Users to smart devices and vice versa. Here's the lowdown on the types of message that fly around the networks:

- **Service Requests:** Messages sent from DCC Users to devices (or the DCC).
- **Service Responses:** Replies from the devices (or the DCC) to DCC Users.

- **Device Alerts:** Unsolicited messages sent by devices to DCC Users.
- **DCC Alerts:** Unsolicited messages sent by the DCC to DCC Users.

Chapter 4 looks at the mechanics of sending/receiving messages and Chapter 5 summarises the different types of messages you can send/receive and what they're for. Chapter 6 attempts the hopeless task of explaining the security model for keeping these messages safe from malevolent interference.

Chapter 2

Stakeholders

In This Chapter

- Examining the key players in the SMIP
- Understanding stakeholders' roles and what motivates them

Success of the SMIP rests on a disparate set of stakeholders, ranging from the government to consumers and taking in a myriad of organisations, roles and working groups in between. Figure 2-1 attempts to highlight the key stakeholders involved in the SMIP.

Not surprisingly perhaps, it's a population that's stuffed full of acronyms, some of which change depending on which industry document you look at. So here's a brief tour of some of the key participants in the programme. In attempting to impose a little order, I've divided them up into the DCC and its service providers, DCC Users and 'others'.

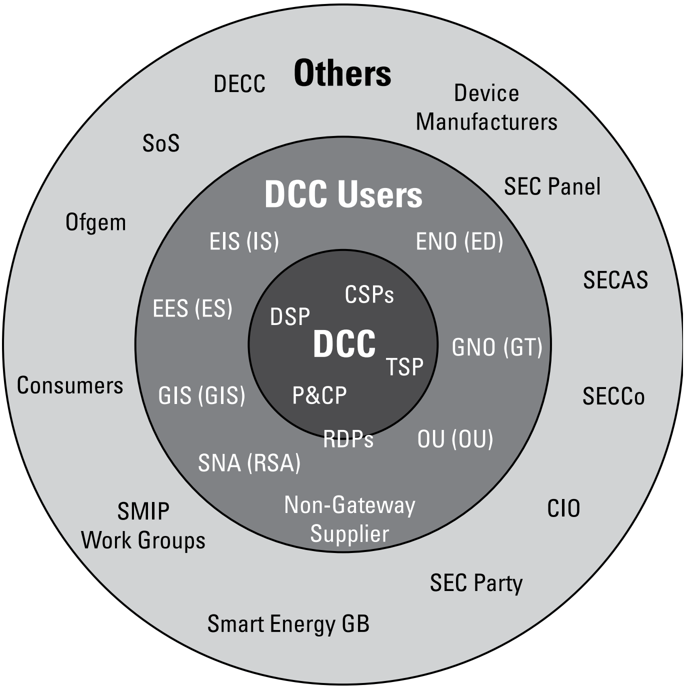


Figure 2-1: Stakeholder map.

The DCC and its Service Providers

At the heart of the programme sits the Data Communications Company (DCC), ably assisted by an array of service providers. In the sections that follow, I take a closer look at who they are.

Data Communications Company

The *Data Communications Company (DCC)* is the party responsible for providing energy suppliers, network operators and energy service companies with access to smart meters installed in homes and small businesses. The Department of Energy and Climate Change (DECC) awarded a brand new DCC licence to Smart DCC Ltd, a subsidiary of Capita plc, on 23 September 2013 following a competitive tendering process. Smart DCC Ltd has the DCC licence for 12 years and has inherited a number of

DCC Service Provider contracts, procured by DECC in parallel to the DCC Licensee; namely, the *Data Service Provider (DSP)* and *Communication Service Provider (CSP)* contracts (which I describe in the following sections). When it's time to re-procure these service providers, the DCC will get to choose but, for now, they're stuck with the choices made by DECC.

Data Service Provider

The *Data Service Provider (DSP)* is responsible for delivering and operating the central *DCC Data Systems* to which DCC Users interface when communicating with smart devices. This includes the *DCC User Gateway Network* to which DCC Users connect. The DSP also acts as the DCC's Systems Integrator, managing the integration of the various components of the central solution, including the *Interface Testing* phase of the SMIP in which the DCC gets to formally test with would-be DCC Users for the first time (see Chapter 8 for more detail). Following a two-year procurement run by DECC, CGI was awarded the DSP contract on 23 September 2013, a contract that the DCC has since inherited. It's an eight-year contract with three optional one-year extensions.

Communication Service Providers

The *Communication Service Providers (CSPs)* are responsible for providing the *Smart Metering Wide Area Network (SM WAN)* and *Communication Hubs (CHs)* through which the DCC Data Systems communicate with smart devices. The CSP and DSP procurements ran in parallel with three CSP regions up for grabs. Arqiva was successful in winning the Scotland/North of England contract, and Telefónica won the Wales/Central England and Southern England contracts. The CSP contracts are fifteen years in duration with the option of five one-year extensions.

Trusted Service Provider

The *Trusted Service Provider (TSP)* is responsible for providing the *Smart Metering Key Infrastructure (SMKI)* and *Infrastructure Key Infrastructure (IKI)* solutions that underpin the end-to-end security model used in the SMIP (described in more detail than you'd like in Chapter 6). The TSP is BT, however, unlike the DSP and CSP contracts, the TSP contract has yet to be made public, even in redacted form, so details are unknown.

WARNING!

Just because the DCC has a ‘trusted’ service provider, doesn’t necessarily mean that its other service providers are shifty and unreliable. It may just appear that way.

Parse and Correlate Provider

The *Parse and Correlate (P&C) Provider* is responsible for developing the software application used by DCC Users to convert *GBCS* (the protocol used by the DCC to talk to smart devices) into *DUIS* (the protocol used by DCC Users to talk to the DCC). P&C also checks that the DSP has done its job correctly when translating *critical commands* (*really* important ones) into GBCS (the *correlate* bit of Parse and Correlate). This will all make much more sense when you’ve read Chapter 4 (trust me). Critical Software was appointed P&C Provider on 29 April 2014 under a three-year contract with the option of two one-year extensions.

Registration Data Providers

Registration Data Providers (RDPs) aren’t DCC service providers in that they’re not appointed by, or contracted to, the DCC. Neither do RDPs qualify as DCC Users (see the next section). They do, however, provide an essential service to the DCC by providing daily updates of registration data that the DCC uses to determine the level of access to a smart device to which a DCC User is entitled. For example, it’s the RDP that tells the DCC who the legitimate supplier is for a smart meter at any given time. Electricity registration data is held within *Meter Point Registration Systems (MPRSs)* maintained by the *Distribution Network Operators (DNOs)* and independent DNOs *(iDNOs)*, and the gas equivalent is held by Xoserve. Xoserve and the DNOs have a licence obligation to fulfill the RDP role.

DCC Users

DCC Users are *SEC Parties* (that is, signatories to the *Smart Energy Code* – see Chapter 7) that have successfully completed *User Entry Process Testing* (*UEPT* – see Chapter 8) and, as such, are allowed to use DCC Services. They come in different flavours, termed *DCC User Roles*, and each role has access to a different set of services. A SEC Party has to go through UEPT for each DCC User Role that it wants to operate as.

When turning the *DCC User Gateway Interface Design Specification (DUGIDS)* into its SEC Subsidiary alter ego, the *DCC User Interface Specification* (*DUIS* – see Chapter 7), someone thought it would be a good idea to rename most of the DCC User Roles. So, when you turn up at the SEC Party convention and are asked what DCC User Role you are, the correct etiquette for answering this question is, ‘DUGIDS or DUIS?’ To avoid confusion, I include both terms (leading with the DUIS version).

Import Supplier

The *Import Supplier (IS)* is the supplier from whom a consumer buys his or her electricity and is the party that installs electricity smart meters. An IS has access to nearly all the functionality within an electricity smart meter (there’s just a few export and network-related functions that it can’t use). It’s also the party that pays the largest fixed monthly charge for every electricity smart meter serviced by the DCC (almost half of the total, in fact). IS translates into *Electricity Import Supplier (EIS)* in DUGIDS dialect.

Gas Supplier

The *Gas Supplier (GS)* is the supplier from whom the customer buys his or her gas. As per the IS, the GS is responsible for gas smart meter installations and has access to the majority of its functionality. It also picks up the entire fixed monthly DCC charge per gas meter. A GS is a *Gas Import Supplier* (*GIS*) when conversing in DUGIDS.

Export Supplier

The *Export Supplier (ES)* is the supplier to whom the customer sells surplus electricity from his or her *Feed In Tariff Scheme (FITS)* installation (typically solar panels). As such, an ES can only access messages relating to export registers on the electricity smart meter and makes only a modest contribution to the monthly DCC charge for an electricity meter. ES translates into *Electricity Export Supplier* (*EES*) in DUGIDS.

Measuring spill

In addition to measuring consumption, smart electricity meters are capable of recording electricity exported to the distribution grid. Under the government's FITS, consumers who install their own generation (usually in the form of solar panels) get paid for every kWh they generate and a much smaller amount for every kWh they don't use and, therefore, 'spill' onto the grid. Because traditional meters don't record export, export suppliers currently assume spill to be 50 per cent of generation.

Smart meters now mean that suppliers can measure spill. However, given that an average 4kW array will generate between 10 and 15kWh per day (300 to 450kWh per month), a 50 per cent spill at £0.04/kWh equates to an average monthly payment of around £7.50 for spilt generation. If metering were to show that the customer is only spilling 40 per cent rather than the estimated 50 per cent, the export supplier would save £1.50 per month, which would more than offset the fixed monthly ES charge per meter of 3p. However, on a sunny day, an empty household (with the occupants out at work or school) could easily spill three quarters of its generation, costing the ES an additional £3.75 per month for the privilege of metering, rather than estimating, the export. Given this dubious business case, it's unlikely we'll end up with many ESs unless the government chooses to mandate the use of smart meters for measuring export.

Electricity Distributor

The *Electricity Distributor (ED)* is responsible for the cables and wires that deliver electricity to a consumer's house. EDs are more commonly referred to in the industry as *Distribution Network Operators (DNOs)* and, just to confuse matters, are referred to as *Electricity Network Operators (ENOs)* in DUGIDS.

Other than changing their own security certificates (see Chapter 6) and setting some alert thresholds and maximum demand registers, EDs are restricted to reading information from smart meters and receiving alerts. EDs incur a fixed monthly charge for every smart meter installed on their network, regardless of whether they make any use of it, so there's some incentive (and, indeed, expectation from Ofgem, the energy regulator) for them to make use of DCC services. That said, I can best describe the smart metering benefits identified by most DNOs in their recent price control submissions as ‘modest’. Even the government’s impact assessment only identifies £877 million of network benefits over 19 years (which is about a tenth of those identified for suppliers).

Gas Transporter

The *Gas Transporter (GT)* is responsible for the pipes that take gas to a consumer’s house. GTs, like EDs, are restricted primarily to reading information from smart meters and receiving alerts. Unlike EDs, GTs don’t (currently) incur any fixed charges for having smart meters installed on their networks and have, not surprisingly, shown little interest to date in becoming DCC Users. A recent DECC consultation may change all this by placing an obligation on GTs to become DCC Users within a defined period after the DCC goes live. GT translates into *Gas Network Operator* (or *GNO*) in DUGIDS.

TECHNICAL STUFF

Starting the clock on Customer Minutes Lost

Spend any time chatting to a DNO about smart metering and it won’t be long before you hear the words ‘last gasp’. This is the alert issued by a dying Communications Hub following a power cut and is probably at the top of most DNOs’ smart metering agendas. DNOs monitor their high- and medium-voltage networks, but the low-voltage network that feeds most domestic customers is largely invisible. So the first that DNOs currently hear about power cuts on the low-voltage network is when customers pick up the phone to complain. At that point, the clock starts on *Customer Minutes Lost* (or *CML*, for short), a very important measure of a DNO’s performance. On the plus side, a customer with a smart meter will no longer need to pick up the phone to start the CML clock. However, from a DNO’s perspective, the threat exists of higher CMLs and associated penalties.

Registered Supplier Agent

The *Registered Supplier Agent (RSA)* is the *Meter Operator (MOP)* appointed by the IS or the *Meter Asset Manager (MAM)* appointed by the GS to physically install and maintain the smart meters. It could also be the *Meter Asset Provider (MAP)* in both cases (that's the party that owns the meter and rents it to the import supplier).

The RSA has been granted access to a relatively paltry set of Service Requests and can only extract information from meters to see how they're being used (for example, read the configurations that have been placed on the meter by other DCC Users). Just to confuse matters, RSAs are called *Supplier Nominated Agents (SNAs)* in DUGIDS.

WARNING!

If you're a MOP or MAM and you aspire to become an RSA in the hope of being able to install meters on your own, think again. The commands required to commission a device are only available to the installing supplier (the IS in the case of an electricity smart meter, and the GS in the case of a gas smart meter). If you're an independent MOP or MAM looking to secure lucrative smart meter installation contracts, you'll need to ensure that you can communicate with your employers to instigate the necessary DCC Service Requests to install meters, either via the SM WAN or locally via your *Hand Held Terminal* (*HHT* – see Chapter 3).

Other User

As its name suggests, the *Other User (OU)* DCC User Role covers a hotchpotch of parties and is likely to include energy service companies, price comparison websites and Customer Access Device (CAD) providers (see Chapter 3). OUs have a meagre set of messages available to them, but they can read consumption data (with appropriate customer consent, of course) and provide services for installing CADs. Remarkably, *Other User* is OU in both DUIS and DUGIDS.

REMEMBER

OUs need to have a privacy assessment from the *Independent Privacy Auditor* (one of the roles of the *Competent Independent Organisation* appointed by the *SEC Panel*). See Chapter 9 for more details.

Non-Gateway Supplier

Technically not a DCC User, a *Non-Gateway Supplier* (*NGS*) is a supplier that's still going through User Entry Process Testing (UEPT) and has yet to become a bona fide DCC User.

When a supplier who's a DCC User gains a DCC-serviced meter through the change of supplier process, they instruct the DCC to put their Organisation Certificate on the meter to claim ownership (see Chapter 6). The supplier does this by sending a Service Request via the DCC User Gateway. If a Non-Gateway Supplier gains a DCC-serviced smart meter, they're still required to instruct the DCC to put their own Organisation Certificate on the meter. They can't, however, do this by sending a Service Request via the DCC User Gateway, so they require some other mechanism. This mechanism is the Non-Gateway Interface (which is, essentially, email). NGSs do, however, need to go through the *Smart Metering Key Infrastructure Registration Agency Policies and Procedures (SMKI RAPP)* in order to be able to request Organisation Certificates. (Don't worry, all is revealed in Chapter 6.)

WARNING!

Whilst small suppliers (that is, those with fewer than 250,000 customers) and non-domestic suppliers aren't obliged to use DCC Services from day one, a recent DECC consultation is likely to require small suppliers to become DCC Users within 12 months of DCC Go Live and may deny non-domestic suppliers the right to opt out of using DCC Services to communicate with their smart meters. Small suppliers and non-domestic suppliers who thought they could happily ignore the SMIP should think again.

Multi-talented

A DCC User may have multiple DCC User Roles. For example, a dual fuel supplier needs accreditation as an IS and GS. If they're an export supplier and want to use smart meters to measure export, they also need to be an ES. And if they want to be able to provide quotations to potential new customers based on their historic consumption, they also need to be an OU.

REMEMBER

A DCC User needs to go through *User Entry Process Testing* (*UEPT* – see Chapter 8) for each individual DCC User Role that they want to operate as.

Other Stakeholders

Okay, I've covered the DCC, its service providers and the DCC Users who use it. Now it's time to move on to some other key stakeholders in the SMIP.

Consumers

The government would probably argue that consumers should be in the centre of the stakeholder map in Figure 2-1. According to their website, 'smart meters put consumers in control of their energy use, allowing them to adopt energy efficiency measures that can help save money on their energy bills and offset price increases'. Many of the forecasted benefits of the SMIP depend on consumers changing their energy consumption behaviour as a response to becoming more energy savvy through use of their smart meter. They're also the ones who'll ultimately pay for the programme through their energy bills.

Department of Energy and Climate Change

The *Department of Energy and Climate Change (DECC)* is the government department responsible for instigating the SMIP. DECC left Ofgem (another stakeholder who we introduce in the Office of Gas and Electricity Markets section) to manage the early stages of the programme, but it took back the reigns for the two-year central procurement that appointed the DCC, DSP and CSPs, and DECC has been active in shaping much of the programme ever since. When the rollout is underway, responsibility for the SMIP will pass back to the industry under the adjudication of Ofgem, but for the time being it's DECC that makes the key decisions driving the programme.

Secretary of State

Powers conferred by the Energy Act 2008 and extended by the Energy Act 2011 allow the *Secretary of State (SoS)* to make changes to legislation, licences and codes for the purposes of supporting the rollout of smart meters. These same powers allowed the SoS to introduce the new DCC licence and the *Smart Energy Code* (*SEC* – see Chapter 7). The SEC and its Subsidiary Documents are being developed by a number of parties including DECC, numerous working groups and the DCC. Following industry consultation, they must all go to the SoS for designation before coming into force. Given the number of documents involved (45 and counting), the SoS is going to be very busy.

Office of Gas and Electricity Markets

The *Office of Gas and Electricity Markets (Ofgem)* is the energy regulator charged with protecting the interests of existing and future electricity and gas consumers. Ofgem managed the first phase of the SMIP before DECC wrested control. However, Ofgem is destined to become the final adjudicator for any changes to the SEC or its Subsidiary Documents once transition is complete and we reach steady state.

SEC Panel

The *SEC Panel* is charged with managing the *Smart Energy Code (SEC)* and its Subsidiary Documents (which I examine in more detail in Chapter 7). It comprises an independent chair and elected representatives from the industry, plus representatives from the DCC and consumer groups.

The SEC Panel is also responsible for appointing a number of *SEC Sub-Committees*; namely:

- **SEC Change Board:** The body charged with assessing modifications to the SEC and making recommendations to Ofgem as to whether or not they should be implemented.
- **Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA):** A panel of security experts responsible for governance of the *SMKI Document Set* and assurance of the DCC-operated SMKI services (I describe the SMKI in Chapter 6).
- **Technical Sub-Committee (TSC):** Another bunch of experts responsible for providing support and advice on technical specifications and the end-to-end technical architecture.

- **Security Sub-Committee (SSC):** Responsible for developing and maintaining security documents under the end-to-end security architecture that escape the grasp of the SMKI PMA.

Like the SEC Panel, membership of the Change Board, SMKI PMA and SSC have prescribed compositions to ensure that the views of all stakeholders are represented. Membership of the TSC, on the other hand, is wholly determined by the SEC Panel. Cross-fertilisation also exists between sub-committees (for example, the SSC and TSC both provide a member to the SMKI PMA).

Smart Energy Code Company

The *SEC Company (SECCo)* is the commercial alter ego of the SEC Panel and is the corporate vehicle set up to support SEC Panel business. Its board of directors comprises the SEC Panel members and it's used for contracting services with third parties such as SECAS (see the next section).

SEC Administrator and Secretariat

The *SEC Administrator and Secretariat (SECAS)* is contracted by SECCo to provide the day-to-day management of the Smart Energy Code and SEC Subsidiary Documents. It will take on this role fully only when DECC relinquishes control of the SEC at the end of transition after the DCC goes live. Gemserv was awarded a four-year contract to provide the SECAS role in September 2013.

Competent Independent Organisation

Not to be confused with the Inept Prejudiced Organisation *(IPO)*, the *Competent Independent Organisation (CIO)* is responsible for conducting security and privacy assessments for DCC Users and SEC Parties wanting to become DCC Users. In doing so, the CIO wears two hats:

- **User Independent Security Assurance Service Provider (UISASP):** Does the security assessments (against DCC User obligations set out in sections G3 to G6 of the SEC) for anyone using or wanting to use the DCC. (No, I don't know how you're supposed to pronounce 'UISASP' either.)

- **Independent Privacy Auditor (IPA):** Conducts privacy assessments (against SEC, section I2) for DCC Users with a DCC User Role of Other User (OU).

The CIO is appointed by SECCo and, at time of writing, we're all waiting with bated breath to find out who'll get the job.

SEC Parties

Some industry participants (for example, suppliers and network operators) have licence obligations that require them to sign up to the SEC. In doing so, they must register for the DCC User Role(s) under which they intend to operate. However, anyone with £450 to spare and a passing interest in smart metering can become a SEC Party. If you're such a person and you're toying with the idea of offering smart metering-related goods or services, it's a small price to pay to gain access to a wealth of information. As of 15 May 2015, there were 139 SEC Parties from 91 different organisations, as shown in Table 2-1.

SMIP working groups

Too numerous to mention, a host of working groups, change boards, design authorities, expert groups, sub-committees and advisory groups contribute to the SMIP. Most will cease to be at the end of transition, but some will endure by morphing into their enduring counterparts. I revisit the most notable groups in Chapter 8.

Table 2-1 SEC Parties as of 15 May 2015

Category	*SEC Parties*	*Organisations*
Large suppliers	23	9
Small suppliers	41	32
Electricity Network Operators	20	10
Gas Network Operators	16	9
Others	39	33
Totals	**139**	**91**

Device manufacturers

Central to the whole SMIP are the manufacturers responsible for producing the smart devices that will be rolled out. Because the build standards for these devices are regulated, the government is obliged to notify the standards to the European Commission under the Technical Standards and Regulations Directive 98/34. This requirement, combined with problems agreeing on the specifications in the first place, has placed the availability of certified devices well and truly on the SMIP's critical path.

Based on experience in the *Foundation* market (the smart meters that have been, and are being, installed prior to DCC Go Live – see Chapter 10), probably no more than a dozen meter manufacturers will vie to provide devices for rollout and not all will succeed in producing working devices in the required timescales.

Smart Energy GB

Formerly known as the *Central Delivery Board (CDB)*, Smart Energy GB is a not-for-profit organisation set up in 2013 with the unenviable task of getting Joe Public excited at the prospect of getting a smart meter. Analogous to Digital UK's role in promoting the switchover from analogue to digital TV, Smart Energy GB is funded by the energy suppliers.

WARNING!

Smart Energy GB has settled on two cartoon characters ('Gaz' and 'Leccy') to convey to the public the benefits of smart metering. Digital UK had a cute silver robot with an unfeasibly large head, but Gaz and Leccy have the potential of being infinitely more annoying. Smart Energy GB's self-proclaimed role is to be the 'voice for the consumer at the heart of the national smart meter programme'. So if you haven't heard of them by the time you read this, either the programme's been delayed again or they're not doing a great job.

Chapter 3
Devices

In This Chapter

- Getting to grips with smart devices
- Understanding the differences between Type 1 and Type 2 Devices
- Ensuring that smart devices work

A smart meter rollout is a tad difficult to achieve without an adequate supply of tested, reliable devices to install. And the rollout doesn't only require smart meters. The engineer turning up to replace your meter will need an array of smart devices in his or her kit bag. Several types of smart device exist (for example, GSMEs, ESMEs, CHs, IHDs, PPMIDs and HCALCSs), many of which come in different variants (like single element, twin element and polyphase ESMEs). The devices themselves will come from competing manufacturers but will need to work with each other, and all need to be tested and certified. Sounds a bit confusing? Well, it is. And it's probably fair to say that availability of smart devices is currently the greatest threat to the SMIP.

In this chapter, I have a look at the devices that sit behind the acronyms and explain what they're for. I try to get a handle on why delivery of smart devices is on the SMIP's critical path, and I finish up by looking at who's responsible for ensuring that they work and how they're going about achieving this.

SMETS and CHTS

Discussing smart devices without mentioning SMETS or CHTS is virtually impossible, so here's a brief explanation of both.

SMETS

The *Smart Metering Equipment Technical Specification* (*SMETS*) is an industry document that defines the minimum physical, functional, interface, data, testing and certification requirements for smart devices wishing to connect to the DCC. In the case of electricity and gas smart meters, SMETS is also the yardstick that determines whether a meter needs replacing by 2020. (If it's SMETS-compliant, it can stay. Otherwise, it goes.)

SMETS comes in two flavours: *SMETS1* and *SMETS2*. *SMETS1* is the minimum standard a *Foundation* smart meter must meet to be eligible for adoption by the DCC (that's meters installed and operated outside of the DCC and then brought into the DCC fold some time later). Official figures from DECC put the number of Foundation meters installed in GB domestic homes at just over a million, as of 31 March 2015. I touch on adoption of Foundation meters again in Chapter 10 but, clearly, adoption can't happen until the DCC is live. *SMETS2* applies to smart devices that are installed and enrolled in the DCC from the get-go.

Truth be told, there's not much between SMETS1 and SMETS2 meters in terms of functionality. The major differences are the security model they use (see Chapter 6) and their SM WAN communications. Whereas SMETS2 devices communicate with the DCC via Communications Hubs and SM WANs provided by the Communication Service Providers (CSPs), SMETS1 devices initially use Communications Hubs and SM WAN providers chosen by the installing supplier. If the DCC deigns to take on a SMETS1 meter, it will adopt the meter's SM WAN communications contract and enroll the meter within its meter estate, thus allowing DCC Users to communicate with it via the DCC User Gateway Network as they would any other SMETS2 device.

SMETS is an important document for device manufacturers and suppliers alike as it's one of the key measures that determines whether a device gets to talk to the DCC.

CHTS

The *Communications Hub Technical Specification* (*CHTS*) is essentially the SMETS equivalent for Communications Hubs. It sets out the minimum physical, functional, interface, data, testing and certification requirements for Communications Hubs to be procured by the DCC.

SMETS1, SMETS2 and CHTS figure prominently in the myriad of industry documents (discussed in Chapter 7) that underpins the SMIP. CHTS first emerged in July 2012 and has been through 29 iterations to get to version 1.46, the latest version at time of writing. SMETS2 has taken less than two years and a mere 15 iterations to get to its current version 1.58. In contrast, SMETS1 has proved a veritable rock, first appearing in December 2012 and only being re-issued once (version 1.1, published on 31 March 2014).

Smart Devices

Here are the smart devices that you may see appearing in your home, hopefully sometime before 2020.

Communications Hubs

The *Communications Hub* (*CH*) has three key functions:

- Establishing the *Home Area Network (HAN)* over which smart devices within the home communicate with each other.
- Connecting to the Communication Service Provider's (CSP's) Smart Metering Wide Area Network (SM WAN) over which the DCC communicates with the smart devices.
- Relaying messages to and from the gas meter (something I explain in the later section, 'GSMEs and GPFs').

The first two of these tasks are performed by the *Communications Hub Function (CHF)* component of the CH whilst the latter falls to the *Gas Proxy Function (GPF)* component.

CHs are provided by the CSP, and each CSP provides its own version incorporating its own preferred SM WAN technology. So which CH you have installed in your home depends on where you live:

- If you live in **Scotland or the north of England**, you'll be getting an Arqiva CH.
- If you live **anywhere else**, you'll be getting a Telefónica CH.

Arqiva's CHs come in a single, one-size-fits-all variant, manufactured by EDMI. They communicate via an SM WAN that uses long-range radio technology.

Telefónica has gone for a combination of cellular and mesh technology to achieve their obligated SM WAN coverage. This complicates things a little in that their CHs come in three flavours: cellular, mesh and cellular/mesh. Cellular and cellular/mesh CHs communicate directly with the CSP over the 2G/3G mobile network. However, in areas with no mobile coverage (estimated by Telefónica as less than 10 per cent), Telefónica's mesh CHs use Radio Frequency (RF) mesh technology to pass messages to neighbouring mesh CHs until they reach a cellular/mesh CH that's got access to the mobile network. The RF mesh network is referred to as a *Neighbourhood Area Network*, or *NAN* for short.

It's up to an installing supplier to determine which type of Telefónica CH to use depending on information provided by Telefónica via the DCC's *Self-Service Interface* (see Chapter 9). Toshiba and WNC are manufacturing Telefónica's CHs, with Toshiba providing cellular, cellular/mesh and mesh variants and WNC only providing a cellular variant.

Communications Hubs get their power via an Intimate Physical Interface (ooh err, Missus!) so you'll find them snuggling up to the electricity meter.

CHs are owned by the DCC; therefore, suppliers don't need to pay for them. They will, however, have to pay a fixed monthly CH charge for each meter they access via a CH and also charges for CHs held in stock or returned unused.

Electricity and Gas Smart Meters

Any self-respecting For Dummies guide aims to give its reader the jargon essential to get by in the chosen topic. So forget all thoughts of electricity and gas smart meters. From now on, they're *ESMEs* and *GSMEs*. *ESME* stands for *Electricity Smart Metering Equipment* (I'll leave you to work out *GSME* as a homework exercise).

ESMEs and ALCSs

ESMEs come in three flavours: *single element*, *twin element* and *polyphase*.

Most of us will be getting a single element ESME, but those of us with electricity storage heating are likely to need a twin element ESME. Twin element ESMEs have two measuring elements, which means that they can record the electricity used for an auxiliary load separately from electricity used in the rest of the home, allowing the supplier to apply different tariffs for each. The most common example of auxiliary load is electric storage heating where the electricity used for heating is charged at a cheaper rate than that used to boil the kettle or watch TV. In the future, auxiliary load may also include heat pumps and electric vehicle charging.

Twin element ESMEs are also likely to incorporate up to five Auxiliary Load Control Switches (ALCSs). As its name suggests, an ALCS switches the auxiliary load on and off according to a calendar held within the ESME that a supplier can update remotely via the DCC. When switching auxiliary loads, the ESME applies a randomised offset to prevent all the houses in a particular area switching their heating on at exactly the same time, thus blowing up the network. Suppliers can also override the calendar remotely, switching the heating circuit on or off on as required.

Twin-element ESMEs can also include a Boost function that allows the customer to override the switching calendar and activate the ALCS by pressing a button (for example, to turn the heating on during the day during a cold snap).

The functionality of all ESME variants, the ALCS and the boost function are defined in SMETS.

ALCSs don't have to be built into an ESME. HAN Connected ALCSs (or *HCALCSs*) are standalone devices that perform the same function as an ALCS but can be installed on the HAN anytime. Think of them as ALCSs that have grown up and left the ESME to make their own way on the HAN. Just bought an electric car and want to start home charging? No problem. ESMEs are being future-proofed to support up to five HCALCSs.

Finally, polyphase ESMEs contain three measuring elements and are used for larger customers (almost certainly non-domestic) on a three-phase supply.

ESMEs can respond to the greatest proportion of Service Request types of any device type, handling just over three quarters of the 115 Service Request types.

GSMEs and GPFs

Compared to ESMEs, GSMEs are a bit simpler because it's a case of 'one-size-fits-all', but GSMEs have their own complexities.

Given the potentially disastrous consequences of mixing gas and electricity and the often remote location of the gas meter from any power supply, GSMEs must rely on power from a battery for their entire life. This means that they spend most of their time asleep, waking only every half hour to take measurements and respond to any commands that may have been sent to them while they were snoozing. Because they spend so much time asleep, GSMEs need a proxy to field any enquiries and hold on to requests that arrive while they're sleeping. The *Gas Proxy Function (GPF* – aka the *gas mirror)* is the GSME's permanent representative on the HAN and it lives within the CH (the third function of the CH that I touched on earlier).

Like ESMEs, the functionality of GSMEs is defined in SMETS. GSMEs can receive just over half of all Service Request types (see Chapter 5), with GPFs handling about a third.

Type 1 and Type 2 Devices

Getting up to speed with ESMEs, GSMEs, ALCs, HCALCs, CHs, CHFs and GPFs is only part of the picture (see the preceding sections). Unfortunately, that's not quite the end of it. You need to know about some more smart devices that fall into two categories, namely Type 1 and Type 2 Devices.

To understand what they are and how they differ, you need to know about the security model that underpins GB smart metering (which I discuss at some length in Chapter 6).

In brief, some smart devices only talk to other devices that they've been introduced to whereas others are less discerning and will talk to anyone. Your discerning device is a *Type 1 Device* whereas its less discriminating cousin is a *Type 2 Device*.

Unlike Type 2 Devices, a Type 1 Device has a Device Log in which it stores details of other devices with whom it's allowed to communicate. These details (which actually take the form of Public Certificates, something that I discuss in detail in Chapter 6) allow the Type 1 Device to check that another device is who it says it is. Only a suitably authorised DCC User can update a Type 1 Device's Device Log and they do this by sending a Service Request via the DCC. Type 1 Devices could, therefore, be considered a bit snooty as they won't talk to any other device without this formal introduction. Some devices, on the other hand, are far more trusting and are happy to talk to anyone. These more gregarious devices that don't have Device Logs are called *Type 2 Devices*.

Clearly, Type 1 Devices are a bit more reliable than their less discerning Type 2 brethren and, as a result, get to do more. A capability that both Type 1 Devices and Type 2 Devices share is the ability to access information stored in ESMEs, GSMEs and GPFs. But what separates the men from the boys is that Type 1 Devices also get to issue and execute HAN commands, whereas Type 2 Devices don't. What this means is that Type 1 Devices get to *do* things whereas Type 2 Devices only get to *commentate* on what's happening.

Although we don't refer to GSMEs, ESMEs, GPFs and CHFs as Type 1 Devices, they look a lot like them, in that they get to execute and issue HAN commands and have their own Device Logs for storing the details of devices with which they communicate.

Type 1 Devices

Given the absence of GSMEs, ESMEs, GPFs and CHFs, the category of Type 1 Devices is currently limited to HCALCSs and Prepayment Interface Devices (PPMIDs). I've talked a bit about HCALCSs already (see the section 'ESMEs and ALCSs'), but it's probably worth saying something about PPMIDs.

As you're no doubt aware, a *prepayment meter* is one that requires customers to pay for energy in advance. Both ESMEs and GSMEs can operate in prepayment mode. Suppliers are likely to offer a whole range of different means of paying for top-ups (for example, over the web, by phone and at the corner shop) and, once paid, will apply the credit remotely via the DCC.

However, top-ups can also be applied locally if, for some reason, the remote top-up fails. To do this, the customer has to enter the *Unique Transaction Reference Number (UTRN)* that they're given at time of purchase directly into the ESME or GSME. This isn't always that easy if the meter's in the far corner of the garage or buried under the stairs.

A *PPMID* is a device that allows customers to enter UTRNs into ESMEs and GSMEs and, because it's HAN-connected and probably battery-powered, it can be located anywhere. In addition to supporting local top-ups, a customer can also use a PPMID to display pre-payment related info, activate emergency credit and (in the case of ESMEs) re-enable supply if he or she goes off supply having used up all their credit. PPMID functionality is defined in SMETS, including the ability to process their meagre allocation of four Service Request types.

HCALCSs qualify as Type 1 Devices because they get to switch auxiliary load on and off, whereas PPMIDs earn their Type 1 status by being able to add credit, activate emergency credit and re-enable supply. Like PPMIDs, only a handful of Service Request types (eight, to be precise) are directed towards HCALCSs and their functionality is defined in SMETS.

Type 2 Devices

Type 2 Devices, if you remember, can't do very much other than access data in ESMEs, GSMEs and GPFs. So what are they for? Well, they can provide a wealth of near real-time information to customers, as the following sections show.

In Home Displays (IHDs)

In addition to installing smart meters, suppliers are obliged to provide customers with an *In Home Display (IHD)*, assuming they want one. The minimum functionality that an IHD must provide is defined in the SMETS and includes:

- Cumulative daily, weekly and monthly consumption and its cost
- Historic consumption
- Tariff, balance and prepayment values

According to the government, it's the IHD that will tell us how much it costs to boil a kettle or microwave a chicken jalfrezi and, thus, make us more energy savvy.

Customer Access Devices (CADs)

The other Type 2 Device in discussion is the *Customer Access Device* (or *CAD* for short). This is (or, rather, will be) a commercially available device that a customer can install on the HAN to access the same data set available to an IHD. A CAD provides the link between the regulated smart metering HAN (or *SM HAN*) and a non-regulated customer HAN (or *C HAN*). A minimum set of CAD functionality is expected to be added to the SMETS, but has yet to materialise.

REMEMBER

The C HAN is where you can expect to see exciting, innovative energy-related products and services developing; from energy management systems and energy brokerage solutions through to smart washing machines and dishwashers.

TIP

Imagine that instead of a cute cuddly toy, your switching site of choice offered you a branded CAD that linked your SM HAN to a cloud-based, real-time brokerage service via your home ADSL router. No more filling in house type, number of bedrooms, the value of last month's bills and the name of your current supplier and tariff. The switching site now has continual access to your current and historic consumption and your active tariff, and can proactively tell you when it's time to switch and to whom. With the prospective of a shorter, more efficient switching process through centralised registration (see Chapter 10), the CAD could also conceivably switch supplier for you! Okay, probably not as good as a cuddly toy, but nothing stops you providing your CAD embedded in, say, a cute, cuddly meerkat (a meerCAD, perhaps?).

Hand Held Terminals (HHTs)

For completeness, I should also mention *Hand Held Terminals (HHTs)*, which may be used by suppliers to support meter installations or configuration of meters in the absence of the SM WAN. When submitting Service Requests over the DCC User Gateway, suppliers can ask the DCC to return HAN-ready commands for local delivery via an HHT as opposed (or in addition) to being sent over the SM WAN. Like CADs, the SMETS is set to include a minimum set of HHT functionality, but it's yet to make an appearance.

REMEMBER

Whereas most existing meters have some means of connecting an HHT (optical ports, for example), SMETS2 meters have none (a facet of the end-to-end security model). The intention is for HHTs to be able to communicate with the CH for a period of one hour from the time the CH is first switched on over a *Personal Area Network (PAN)* – essentially, a proximity network. However, this 'Inter-PAN' interface has yet to be defined.

Testing Devices

The government's impact assessment for the national rollout estimates the cost of smart devices to be a little under £5 billion, with installation costing another £1.6 billion. Based on these figures, a 1 per cent failure of installed devices would cost in the region of £66 million. It's essential, therefore, that devices are subjected to adequate testing before being installed in customers' homes.

Types of testing

At least eight different types of testing can be applied to devices – five of which are mandated. Figure 3-1 summarises these, including the drivers for undertaking the various types of testing and the practitioners capable of providing them.

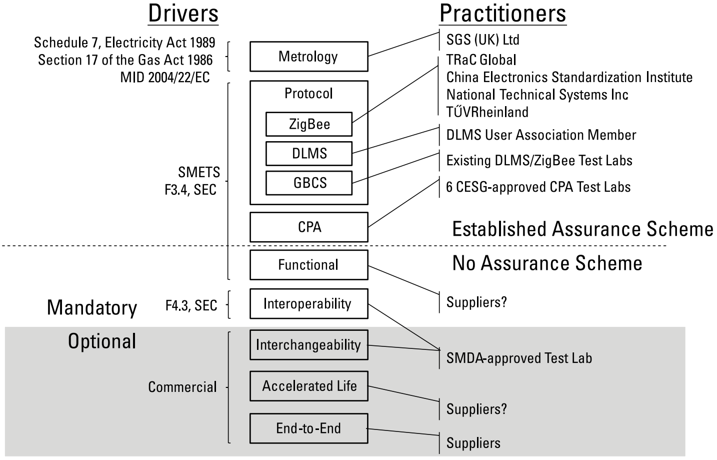


Figure 3-1: Types of Device Testing.

Metrology testing

This is mandatory testing to ensure that ESMEs and GSMEs are certified safe and fit for purpose. 'Safe and fit for purpose' translates into compliance with Schedule 7 of the Electricity Act 1989 and its associated Statutory Instruments (for an ESME), Section 17 of the Gas Act 1986 (for a GSME) and the European Measuring Instruments Directive (MID 2004/22/EC) (for both).

Testing is conducted by an Ofgem-appointed meter examiner (currently SGS (UK) Ltd) and, if successful, results in the meter being listed in a statutory register of meter types approved for use in the UK. After a model is approved, individual meters of that type can be tested and, once certified, are sealed to secure the measuring elements of the meter from tamper. This form of meter approval and verification has been around for some time and applies to all meters (smart or traditional), so it's business-as-usual for meter manufacturers.

Protocol testing

Protocol testing is also mandatory and ensures that a smart device conforms to the communications protocols that it uses over the HAN and/or SM WAN. SMETS2 devices use a new hybrid of ZigBee and *Device Language Message Specification Companion Specification for Energy Metering* (*DLMS/COSEM*) protocols as defined in the *GB Companion Specification* (*GBCS* – see Chapter 7), so protocol testing means compliance with the GBCS.

Four Authorised Test Service Providers exist for certifying ZigBee products:

- TRaC Global
- China Electronics Standardisation Institute
- National Technical Systems Inc.
- TŰVRheinland

In contrast, any member of the DLMS User Association who has purchased the DLMS Conformance Test Tool (CTT) can do DLMS/COSEM testing. As such, most device manufacturers do their own DLMS/COSEM protocol testing.

ZigBee and DLMS/COSEM testing is well established, but GBCS compliance is new. It's likely, however, that GBCS testing will emerge as an extension to the existing ZigBee testing services.

In an attempt to accelerate development of devices in the absence of a DCC environment, the DCC has commissioned Critical Software to modify a tool previously developed to validate GBCS (the unfortunately named *GBCS Interface Testing*, or *GIT* for short). The modified tool, *GIT for Industry (GFI)* will allow device manufacturers to generate 'gold standard' GBCS commands on a ZigBee HAN to which they can connect and test their devices. By the time you read this, the first version of this tool should have been released and we should be well into a series of seven GBCS Test Events organised by the DCC for budding device manufacturers to come along and test out their devices against GIT.

Security testing

ESMEs, GSMEs, CHs and most Type 1 Devices (devices that actually get to do things) need to be security certified under CESG's Commercial Product Assurance (CPA) scheme. Type 2 Devices, which are essentially 'read only', don't need to be CPA assured. Specific CPA Security Characteristics exist for each device type (ESME, GSME, CH and HCALCS) that set out the features, testing and deployment requirements necessary to meet CPA certification. These cover features such as:

- Physical protection (detecting, logging and notifying tampering, for example)
- Message protection (authentication, integrity checking, protection against replay and so on)
- Protection of sensitive data (encryption and provision of Privacy PINs)

PPMIDs, although designated as Type 1 Devices, are not subject to CPA testing by virtue of the fact that, although they get to control supply, they can only enable it, not disable it.

CESG's website cites six CESG-approved CPA Test Labs (CGI being one of them). Although the CPA Security Characteristics for these devices are new, the CPA testing process is well established.

CESG is a branch of the more famous Government Communications Headquarters (GCHQ). It used to stand for Communications Electronics Security Group but it now stands for the National Technical Authority for Information Assurance (no doubt they retained the CESG acronym to confuse the enemy).

Functional testing

ESMEs, GSMEs, PPMIDs, HCALCS and IHDs must be tested to ensure that they meet the functional requirements set out in SMETS. Similarly, the CSPs must demonstrate that their CHs comply with CHTS functionality. SMETS functional testing is new but is probably something that existing test houses will want to offer. Whether there'll be any accepted certification scheme for this testing is another matter.

Interoperability testing

In this context, *interoperability* means the ability for a ESME, GSME, CH or Type 1 Device to respond to commands received from the DCC in accordance with GBCS (if you remember, Type 2 Devices don't get to receive HAN commands, so this type of testing doesn't apply to them). As with functional testing, interoperability testing is new. Unlike functional testing, it requires a DCC test environment and the ability to interface with it. Would-be interoperability testers are, therefore, likely to need to become DCC Users, or at least pass whatever entry criteria the DCC chooses to mandate in order to gain access to a DCC test environment.

Interchangeability testing

In this context, *interchangeability* means the ability for a given device to work with any other device on the same HAN, regardless of type, manufacturer, make, model or firmware version.

REMEMBER

Most devices are installed by suppliers, so when a customer switches supplier, the new supplier may inherit devices that are unfamiliar. If one of those devices fails, it's the new supplier's responsibility to replace it, and this may well be with a different make and model. The replacement device must be compatible with the rest of the installed devices to avoid the expense of replacing the lot.

As with interoperability testing, interchangeability testing is new and likely to require a DCC test environment. Given the need to test devices with every other type of device, it's also likely to require a very large and ever-growing permanent collection of devices (a 'device zoo').

Accelerated life testing

Most smart devices have a life expectancy of at least 10 to 15 years. Given the cost of a device (not to mention the expense of a site visit to install it), a device must achieve a ripe old age, preferably shuffling off its mortal coil via a statutory meter change (replacement when its certification expires). Because many of the devices that will be rolled out are still on the drawing board, little evidence exists that they'll achieve their dotage. As its name suggests, *accelerated life testing* aims to exercise a device far in excess of normal operating conditions, thus simulating the passage of time.

End-to-end testing

Though not specifically aimed at testing devices, devices will play an essential part in a DCC User's end-to-end testing (in which the DCC User tests full operation of all their processes from their back office systems right through to the customer).

Mandatory or optional?

Table 3-1 summarises the eight types of device testing and the device types to which they apply ('M' means 'Mandatory'; 'O' means 'Optional').

Table 3-1 SMETS2 Device Testing

Type of Testing	*ESME*	*GSME*	*CH*	*PPMID*	*HCALCS*	*IHD/CAD*
Metrology	M	M				
Protocol (ZigBee)	M	M	M	M	M	M
Protocol (DLMS/COSEM)	M					
Protocol (GBCS)	M	M	M	M	M	M
Security (CPA)	M	M	M		M	
Functional	M	M	M	M	M	M
Interoperability	M	M	M	M	M	
Interchangeability	0	0	0	0	0	0
Accelerated life	0	0	0	0	0	0
End-to-end	0	0	0	0	0	0

WARNING!

Just because a device has been certified doesn't mean that it won't need to be re-tested. Smart devices these days comprise both hardware and firmware, the latter being upgradeable remotely. Depending on the extent of the change, a new version of firmware may require a new set of testing. And don't forget that the life span of some certificates is less than the anticipated life of the device (for example, CPA certificates for a given product must be renewed every six years).

REMEMBER

You can update the firmware in an ESME or GSME remotely via the DCC. The process is as follows:

1. **Distribute the new firmware in bulk.** (To multiple devices in a single command – the only bulk Service Request that the DCC supports.)
2. **Activate the firmware in each device individually using a different Service Request.**

Who's responsible?

With the exception of the CH (which is the responsibility of the CSP), the responsibility for just about all other device testing falls to the registered supplier. If the registered supplier changes (that is, if the customer switches supplier), the responsibility passes to the new supplier.

Why test?

The requirements for metrology testing are set out in the Electricity and Gas Acts. SMETS defines the requirements for protocol, security and functional testing. The Smart Energy Code (SEC) not only requires a supplier to use SMETS-compliant equipment (section F3.4), but also requires them to install interoperable devices (section F4.3). No regulatory obligation exists to do any interchangeability, accelerated life or end-to-end testing, but most suppliers recognise the commercial imperative for these.

Providing evidence of testing

Suppliers are ultimately responsible for ensuring that a device has been adequately tested and for providing evidence that this has been done, if requested to do so by the DCC. However, this doesn't mean that they have to do the actual physical testing. It's likely that the device manufacturers will be required to provide evidence that their products have been adequately tested before even making it onto a supplier's shortlist.

Providing evidence is easy enough for testing where established testing regimes and certification processes exist (for example, CPA Certificates for Security testing). But it's a bit more challenging where no such regimes and processes exist (as is currently the case for functional, interoperability and interchangeability testing).

WARNING!

In an ideal world, a supplier would insist on seeing a full set of test certificates as a prerequisite to procuring a device. In practice, these won't be available within the timescales currently set out in the Joint Industry Plan and suppliers are likely to make procurement decisions contingent on manufacturers achieving certification post contract signature.

Smart Metering Device Assurance

To address the absence of certification schemes for interoperability and interchangeability testing, the following bodies came together and appointed Gemserv as the *Smart Metering Device Assurance (SMDA)* scheme operator:

- Energy UK, representing the suppliers responsible for testing the devices
- British Electrotechnical and Allied Manufacturers' Association (BEAMA), representing the device manufacturers
- Community of Meter Asset Providers (CMAP), representing the device owners
- Energy and Utilities Alliance, representing just about everybody

The SMDA scheme operator is tasked with establishing an independent assurance scheme covering interoperability and interchangeability testing. This is likely to entail:

- Developing a set of test specifications
- Approving one or more test houses to conduct the tests
- Awarding certification based on test output

Therefore, device manufacturers will likely need to add an SMDA certificate to their bundle of certifications in order to get on a supplier's shortlist.

That just leaves functional and accelerated life testing, neither of which currently has an assurance scheme. It's conceivable that functional testing may find its way into the SMDA's remit, but accelerated life testing probably won't, so it will doubtless fall to testing houses to come up with compelling accelerated life testing propositions.

TIP

It would make a lot of sense for SMDA to add functional testing to its remit. Whilst much of a device's functionality will undoubtedly be tested during end-to-end testing, suppliers will not be testing non-supplier functionality such as that exclusive to network operators. Just because a supplier doesn't have access to maximum demand registers doesn't free them from their obligation to demonstrate that they work. Far easier to give this to the SMDA scheme operator to sort out.

Chapter 4

Messaging

In This Chapter

- Distinguishing between different types of message
- Mastering the mechanics of sending/receiving messages
- Dealing with issues

Many definitions of what constitutes a smart meter exist, but perhaps the key feature that makes a smart meter smarter than a traditional or Automated Meter Reading (AMR) meter is its ability to support *two-way* communication. The primary role of the Data Communications Company (DCC) is to put in place the infrastructure to support this communication between the smart devices described in Chapter 3 and the DCC Users described in Chapter 2. This chapter is devoted to the mechanics of sending messages over the DCC infrastructure.

I'll start with an apology. There's no easy or entertaining way to describe the workings of the DCC, so this chapter's going to be tough going. It's divided into two sections: the first introduces the basics of DCC messaging using a dubious analogy and the second section is devoted to the mechanics of sending messages. You may find the first section mildly entertaining but the second is unavoidably complicated and inescapably dry. I suggest you get a strong coffee before proceeding any further.

Grasping the Basics of DCC Messaging

Let's start with the basics. The messages that fly around the DCC infrastructure divide into *Service Requests*, *Service Responses*, *Device Alert*s and *DCC Alerts*. Commands sent by a DCC User are called *Service Requests* and the replies that come back are called *Service Responses*. Most Service Requests are sent to devices but some can be satisfied by the DCC itself (the latter referred to as *non-Device Service Requests* or *DCC-Only Service Requests* depending on which document you read). Unsolicited messages from devices are called *Device Alerts* and, not surprisingly, those from the DCC are called *DCC Alerts*.

The DCC is a bit like the Royal Mail in that their job is to deliver messages (Service Requests) from senders (DCC Users) to recipients (devices) and vice versa (Service Responses/Alerts from devices to DCC Users). They offer first class (on-demand) and second class (scheduled, future-dated) services and even a form of recorded delivery service (for Critical Service Requests, which I'll come to in a minute).

However, the DCC and Royal Mail differ in that, in addition to just delivering mail, the DCC also offers a one-way translation service. DCC Users send Service Requests to the DCC in something called *DCC User Interface Specification (DUIS)* format. Devices, however, speak in a difficult *Home Area Network (HAN)-ready* dialect defined in a document called the *Great Britain Companion Specification (GBCS)*.

GBCS defines the language that devices need to speak if they want to be supported by the DCC (more detail in the later section 'Protocols'). You may also hear the term *HAN-ready messages*. To all intents and purposes, these two terms are synonymous.

A dubious analogy

Here's a tenuous analogy for how messages are sent and received via the DCC, broken down into bite size pieces.

1. Imagine your daughter (a DCC User) has a pen pal in Bratislava (a device in someone's home) but her Slovak leaves a bit to be desired. She writes a letter (a Service Request) in English (DUIS) and posts it in the nearest letterbox (her DCC User Gateway Equipment).
2. The new, improved Royal Mail (the DCC) collects the letter from the post box (the DCC User Gateway Equipment) and takes it to the sorting office (the Data Service Provider – DSP).

3. The DSP translates the letter from English (DUIS) into Slovak (GBCS) and gives it to a third-party courier service (the Communication Service Provider – CSP).
4. The CSP puts the letter on the plane, train or automobile (Smart Metering Wide Area Network – SM WAN) for delivery to your child's pen pal (the device).
5. On delivery to the pen pal's house (the premise), the pen pal's mother (the Communications Hub) hands out the post for the different members of the family (devices on the HAN).
6. The pen pal (device) reads the letter and writes a reply (a Service Response). He does this in Slovak (GBCS – his English is pretty ropey).
7. The pen pal passes the letter to his mum (the Communications Hub), who sends it back via the courier (over the SM WAN) to the sorting office (the DSP).
8. Unfortunately, the sorting office doesn't offer a Slovak-to-English translation service, so they just send on the reply (via the DCC User Gateway Network) in Slovak (GBCS) to your child (the DCC User).
9. Fortunately, your child has downloaded the free Slovak-to-English app (Parse & Correlate) provided by the new, improved Royal Mail (the DCC) and uses this to translate the reply (Service Response/Alert) into English (DUIS).

Okay, as an analogy it's a bit contrived, but the same could be said about the workings of the DCC infrastructure. If it all sounds rather complicated, that's because it is, but I try to explain it in a bit more detail in the remainder of this chapter.

Service Requests/Responses

As I explain in Chapter 3, any smart device with aspirations of connecting to the DCC has to conform to a set of standards. So no matter what make or model, all DCC-connected devices of a given type offer a common set of functionality that allows the DCC to offer a single, common set of Service Request types to DCC Users. This set of Service Request types has grown over time. During the initial round of DCC procurement, a mere 62 existed. By the final round of procurement, this had grown to 83, and we're now at 115.

Service Request Variants

One of the reasons for the increase in the number of Service Requests is the need to align DUIS commands with GBCS commands. This has frequently resulted in splitting Service Requests into a number of Service Request Variants, each mapping onto a single GBCS command that delivers a subset of the functionality of the parent Service Request. For example, Service Request 4.11 Read Tariff is now the proud parent of two strapping Service Request Variants, namely 4.11.1 Read Tariff (Primary Element) and 4.11.2 Read Tariff (Secondary Element). However, not all Service Requests have decided to start a family: 6.11 Synchonise Clock, for example, has shown no inclination towards parenthood.

At time of writing, 83 Service Request types exist, 20 of which have children (or Service Request Variants). These 20 Service Request parents have 52 Service Request Variants between them (giving us 115 Service Requests/Service Request Variants in total).

You may well come across the terms *Service Reference* and *Service Reference Variants*. These terms refer to the numbers used to identify Service Request types and Service Request Variant types. A two-part Service Reference (such as '4.11') is used for a Service Request type whilst a three-part Service Reference Variant (such as '4.11.1') is used for a Service Request Variant type.

Critical and Non-Critical Service Requests

As with life, not all Service Requests are born equal. *Critical Service Requests* are those that if compromised could result in loss of supply, financial fraud or could compromise the security of the receiving device. In contrast, compromise of Non-Critical Service Requests is considered relatively harmless. A little under a third of all Service Request types and Service Request Variant types are designated as Critical.

You may also come across the term *Supply Sensitive Service Request*. This is a special case of a Critical Service Request that 'if it were to be executed on the relevant device, could affect (either directly or indirectly) the quantity of gas or electricity that is supplied to a consumer at premises', to quote the Smart Energy Code (SEC). In other words, it could turn the lights off (and/or the cooker). Before you send one of these, you need to have done a *Supply Sensitive Check* (although no one seems to be entirely sure what this is meant to entail).

Due to their elevated status, Critical Service Requests get special treatment:

1. As with all Service Requests, a DCC User submits a Critical Service Request to the DCC in DUIS format.
2. Having translated the Critical Service Request into GBCS, the DSP sends it back to the DCC User as a *Pre-Command* rather than sending it on to the device.
3. The DCC User checks that the DSP hasn't accidentally or maliciously changed the contents during translation and, providing the DSP's done its job correctly, digitally signs the GBCS payload in a way that enables the receiving device to authenticate the message has come from the DCC User and hasn't been tampered with en route (I cover signing and authentication in Chapter 6).
4. The DCC User sends the Pre-Command (now a *Signed Pre-Command*) back to the DSP, who sends it on to the device, adding its own signature.
5. The device can now check that the Critical Service Request has indeed come from the originating DCC User via the DSP.

The DCC requirements for P&C include a minimum requirement to support 34 transactions per second and a promise of scalability. Most large DCC Users are likely to far exceed this volume, so early testing of Parse and Correlate's scalability is advisable.

Sensitive Messages

Having DCC Users check the work of the DSP aims to avoid the DSP becoming a single point of failure. While on the subject of the untrustworthiness of the DSP, I should mention sensitive messages. *Sensitive* isn't a defined term in the SEC but is widely understood to describe data that's deemed to be personal to a customer under the Data Protection Act (DPA).

Parse and Correlate

You may have noticed that the process for handling Critical Service Requests assumes that DCC Users are au fait with GBCS (or fluent in Slovak, in my analogy). How else can they check that the DSP has done its translation job correctly? This is where Parse and Correlate (P&C) comes in. It's an application provided to DCC Users free of charge by the DCC and it has two functions:

- Translating the GBCS payload of Service Responses and Device Alerts received from devices into DUIS
- Checking Pre-Commands by translating them back into DUIS and comparing them with the original Critical Service Request

'Ah, but if the DCC provides P&C, isn't it marking its own homework?' I hear you cry. Well, the DCC has a Smart Energy Code (SEC) obligation to ensure that P&C is procured from an organisation independent of the DSP (who handles the day-to-day translation of Service Requests into GBCS) and to make P&C available to DCC Users if requested to do so.

In line with this obligation, the DCC has commissioned Critical Software to develop P&C. DCC Users aren't obliged to use the DCC-provided P&C and are at liberty to buy an alternative or develop their own. But because the DCC's internal costs include development costs for P&C (making P&C effectively free to DCC Users), we're unlikely to see a proliferation of P&C manufacturers.

For example, how many showers you have a day, when you choose to have them, how long you shower for and any debt you've run up due to your excessive showering may all be deemed to be of a personal nature. This type of information should be available to those who need to know (your psychiatrist, perhaps), but it shouldn't be available to the world at large. In this context, 'the world at large' includes the DCC and its service providers.

For this reason, SMETS2 devices are required to encrypt sensitive data prior to transmission in such a way that only the intended recipient can decrypt it (more on this in Chapter 6). However, not all data collected by smart devices is deemed sensitive. Export data, for example, isn't. Neither is any data relating to power quality (for example voltage and reactive power). A little over 10 per cent of Service Response types are deemed to contain data that's sensitive and requiring encryption.

Understanding the Mechanics of Sending/Receiving Messages

As a DCC User, you have access to a subset of 115 Service Requests, 91 Device Alerts and 40 DCC Alerts, depending on your DCC User Role(s). Whatever your DCC User Role, you have access to at least one Service Request, Device Alert and DCC Alert, and need the ability to process each message type. In some cases, you have no choice in the way you process a message. In others, you can select the timing and even the order you'd like messages to be sent and executed.

Modes of Operation

The main purpose of the DCC is to deliver messages between DCC Users and devices. Like most carriers, the DCC offers a range of delivery services, called *Modes of Operation*. There are nine Modes of Operation in total (as illustrated in Figure 4-1) but you don't always get to choose which Mode of Operation is used. For example, there's a *DCC-Only* Mode of Operation for sending DCC-Only Service Requests (those destined only for the DCC). Similarly, there are Modes of Operation for receiving DCC Alerts and Device Alerts.

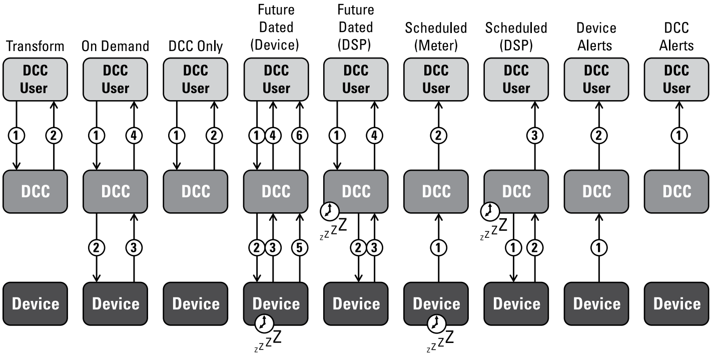


Figure 4-1: Modes of Operation.

The major decision you have to make when choosing which Mode of Operation to use is *when* you want a Service Request to be executed. The choices are:

- As soon as possible (using the *On Demand* Mode of Operation)
- At some specific time in the future (using the *Future Dated* Modes of Operation)
- On a recurring basis (using the *Scheduled* Modes of Operation)

Not all Modes of Operation are supported for all Service Request types. The most available is *On Demand*, which can be used with 86 per cent of Service Request types. By contrast, the *DCC Only* Mode of Operation applies only to the 13 per cent of Service Request types that are DCC Only.

Future dating

Where future dated execution is permissible, the way in which it's supported may differ depending on the type of Service Request:

- In the **Future Dated (Device) Mode of Operation**, the device is responsible for remembering what it's supposed to do and when. The DCC sends a *Future Dated (Device)* Service Request to the device and the device acknowledges it by sending back a Service Response, as with any other Service Request. It then executes the Service Request at the appropriate time, generating a set of Device Alerts in the process. Devices are able to support future dating for 11 per cent of device Service Request types.
- In the **Future Dated (DSP) Mode of Operation**, the DSP takes responsibility for remembering what to do and when. At the appropriate time, the DSP generates a Service Request on behalf of the DCC User and sends it to the device. As far as the device is concerned, it thinks it's received an On Demand Service Request and responds accordingly, sending a Service Response back to the originator of the Future Dated Service Request. The Future Dated (DSP) Mode of Operation can be used with 48 per cent of device Service Request types.

WARNING!

When executing a Future Dated (Device) Service Request, a device may actually perform many individual operations, each of which generates a response. This means the originator is likely to be bombarded with a multitude of unsolicited Device Alerts, all relating to a single Future Dated (Device) Service Request. It's the originator's responsibility to sort these out and decide whether the Future Dated (Device) Service Request was successful or not. To make this (slightly) easier, the DSP labels each response as 'x of y' where 'y' is the total number of expected responses.

Scheduling

The Scheduling Modes of Operation work in a similar way to future dating:

- In the **Scheduled (Device) Mode of Operation**, the device holds the schedule and periodically generates Device Alerts at the appointed times. Only one Service Request type supports the Scheduled (Device) Mode of Operation, and that's the one that sets up a billing calendar on the device, which the device then uses to send back Billing Data Log files (as Device Alerts) to allow the supplier to periodically bill the customer.
- In the **Scheduled (DSP) Mode of Operation**, the DCC User can instruct the DSP to set up a schedule (using a specific DCC-Only Service Request type) and the DSP then takes responsibility for generating Service Requests of the specified type at the appointed times on behalf of the DCC User (a bit like the Future Dated (DSP) Mode of Operation, but on an ongoing basis). Thirteen per cent of device Service Request types can be set up as DSP schedules.

Transforming

I should also mention the *Transform* Mode of Operation, which is a special type of DCC Only Mode of Operation used for the third of all device Service Request types that are designated as Critical. A DCC User uses the Transform Mode of Operation to instruct the DSP to translate a Critical Service Request and return it in GBCS format as a *Pre-Command*. Having checked the Pre-Command using Parse and Correlate (P&C – see the earlier sidebar), the DCC User signs it (thus elevating its status to that of a *Signed Pre-Command*), before sending it back to the DSP for delivery via the DCC User's chosen Mode of Operation (On Demand or Future Dated (DSP), for example).

If you elect to use future dating and/or DSP scheduling, the DCC keeps an eye on things for you and generates a DCC Alert to let you know if the device fails to respond at the expected time (see the later section 'Error Handling').

Command Variants

Like Modes of Operation, *Command Variants* tell the DSP how a DCC User wants a message to be sent. There are eight Command Variants to choose from but, like Modes of Operations, you don't always have a choice. For example, there are dedicated Command Variants for sending DCC Only Service Requests and transforming Critical Service Requests.

The only decision you have to make when selecting a Command Variant is the *route* you'd like the message to take when sending a Service Request to a device. The choices are simple:

- You can send the message via the DCC over the SM WAN.
- You can have the DCC return the message to you and then deliver it in person via a Hand Held Terminal (HHT – see Chapter 3).
- You can do both (get the DCC to send the message over the SM WAN *and* return it to you for local delivery).

All device-bound Service Requests can be sent over the SM WAN but only 85 per cent are available for local delivery. Regardless of which option you go for, the DCC still translates the message into a HAN-ready command and applies the required security signatures (which I attempt to explain in Chapter 6). Table 4-1 outlines the full set of Command Variants and the number of Service Request types that are eligible to use them.

There is, in fact, a ninth Command Variant, introduced in DUGIDS v0.8.1, but this is only used by the DSP for DSP Scheduled Service Requests and isn't visible to DCC Users.

Table 4-1 Command Variants

CV	*Description*	*Sync (S) or Async (A)?*	*Critical?*	*Returned to DCC User?*	*Send over SMWAN?*	*# Service Requests*
1	Non Critical Service Request sent to device over SM WAN	A	✗	✗	✓	67
2	Non Critical Service Request returned for local delivery	S	✗	✓	✗	60
3	Non Critical Service Request sent to device over SM WAN and returned for local delivery	A	✗	✓	✓	60
4	Transform of Critical Service Request into Pre Command	S	✗	✓	✗	33
5	Critical signed Pre Command sent to device over SM WAN	A	✓	✗	✓	33
6	Critical signed Pre Command returned for local delivery	S	✓	✓	✗	25
7	Critical signed Pre Command sent to device over SM WAN and returned for local delivery	A	✓	✓	✓	24
8	DCC Only Service Request	S	✗	✓	✗	15

The reason for having Command Variants that support local delivery of Service Requests is to allow DCC Users to communicate with their devices in the absence of the DCC and its SM WAN. A supplier, for example, may want to install devices in a premise located in an area for which the CSP has yet provide SM WAN coverage. In this instance, the supplier may want to turn up with a set of pre-prepared HAN-ready commands on an HHT and use these to install the devices. However, this approach has its own problems.

WARNING!

Suppliers intending to install smart devices using locally delivered Service Requests have the following options, each of which is problematic:

- **Pre-generate the complete set of Service Requests required to install a set of smart devices back in the office ahead of the site visit.** This restricts you to installing a specific set of devices at a specific premise so, if the customer isn't home, you're left with a load of boxes cluttering up your van. And worse still, if one of the devices is faulty, you may be left with a partial installation since you can't simply pull another device out of the van.
- **Generate the locally delivered Service Requests in the field at time of installation.** You don't have the issues of pre-generating, but you do require reliable remote connectivity with the back office systems that communicate with the DCC over the DCC User Gateway.

DECC is consulting on whether suppliers should be allowed to proactively 'install and leave' (that is, install smart meters in areas where they know that SM WAN coverage isn't yet available). If this is prohibited, locally-delivered Service Requests will only be required for 'reactive' install and leaves (premises where expected SM WAN coverage has gone AWOL for some reason at time of installation).

Protocols

When talking about the SMIP, it would be remiss (even in a For Dummies Guide) not to at least mention the subject of protocols. In this context, a *protocol* is the language used to converse with devices and systems, and, like real languages, there are many. Despite this being a GB smart meter rollout, the SMIP has ended up using an array of languages (a reflection, no doubt, of our multi-cultural society). For those whose eyes are already glazing over, there are really only two protocols that you need to worry about:

- **DCC User Interface Specification (DUIS):** What you use to talk to the DSP over the DCC User Interface. It sets out the format of Service Requests, Service Responses, DCC Alerts and Device Alerts and is delivered using XML (short for *Extensible Markup Language*, probably the one protocol that most people have heard of). Although fine for sending messages from DCC Users to the DCC, it's far too verbose for talking to devices.
- **GB Companion Specification (GBCS):** The language of devices and what the DSP converts DUIS into before sending messages over the SM WAN. Unlike the more verbose DUIS, GBCS is short and to the point and better suited to communicating with low-power devices. Sometimes also referred to as *HAN-ready protocol*, GBCS is actually an amalgam of various existing industry standard protocols plus a few SMIP-specific bits thrown in (see 'Breaking down the GBCS'). It's the DSP's job to decide which of these dialects are required depending on the type of Service Request and the receiving device.

These two protocols are defined in two *SEC Subsidiary Documents* of the same name (see Chapter 7). A third SEC Subsidiary Document, the *Message Mapping Catalogue (MMC)*, tries to stitch these two documents together (that is, map DUIS Service Requests to GBCS commands).

Service Responses and Device Alerts from devices are generated in GBCS protocol. However, as highlighted in my analogy, the DSP only translates Service Requests from DUIS to GBCS, so it's up to the DCC User to use P&C to translate the GBCS payloads contained in Service Responses and Device Alerts back into DUIS. P&C produces its DUIS output in XML.

Sequencing

Another service offered by the DCC is *Sequencing*. This allows a DCC User to fire off a whole load of Service Requests at the same time, specifying the order in which they should be processed. The DCC then takes responsibility for ensuring that they're executed in the specified order.

Breaking down the GBCS

GBCS comprises a number of existing and new protocol standards:

- **ZigBee:** An international protocol designed for low-power devices in the home to communicate with one another. Named after the waggle dance that bees perform after returning to the hive, ZigBee is based on another international standard, IEEE 802.15.4. ZigBee is typically used where data rates are low, battery life requirements are long and networking needs to be secure. Just to complicate matters, the SMIP has opted to use three different dialects of ZigBee:
    - *ZigBee Smart Energy (ZSE)*, which is specific to smart metering
    - *ZigBee Cluster Library (ZCL)*, which is more generic
    - *ZigBee Over The Air (OTA)*, which is used for firmware updates
- **DLMS COSEM:** (or Device Language Message Specification Companion Specification for Energy Metering, to give it its full title) is one of the international protocols traditionally used to communicate with electricity smart meters. Trouble is, it's a bit verbose and not well suited to smart gas meters with limited battery life (hence the need for ZigBee).
- **GBZ (DLMS):** This is a weird combination of ZSE and DLMS COSEM specific to the GB SMIP (hence the 'GB' in the title).
- **PPMID:** This is another weird combination of ZSE and DLMS COSEM to enable communication between a Gas Smart Metering Equipment (GSME) and a Prepayment Interface Device (PPMID – see Chapter 3). This new protocol is required because both devices can be battery-powered and, hence, asleep when the other attempts to communicate with it.
- **X.509:** This is an international standard that supports the implementation of the various flavours of Public Key Infrastructure (PKI – see Chapter 6) used by the SMIP.

To specify a sequence, you need to set the *First In Sequence* flag in the header of the first Service Request in the sequence and the *Preceding Sequence Request IDs* in subsequent Service Requests in the sequence. The last Service Request in the sequence is either the last one to have a Preceding Sequence Reference ID set or the 99th Service Request in the sequence (the maximum number allowed), whichever comes first.

Unfortunately, sequencing can't be used for all Service Requests. Sequences mustn't include transformations of Critical Service Requests into Pre Commands, submission of DCC Only or DCC Scheduled Service Requests, gas Service Requests that return sensitive data or Service Requests to be delivered locally.

Why sequence? Although entrusting a schedule to a device or the DSP makes eminent sense, think carefully before making use of the DCC's scheduling service. Firing off a batch of sequenced Service Requests is all very well if everything goes to plan, and may well enable you to outsource responsibility for orchestrating Service Requests. However, in addition to the restrictions on the Service Request types that you're allowed to sequence, be prepared to sort out the ensuing mess if the DCC notifies you that things have gone pear-shaped (which they do via an 'N14 Sequence Request Failure' DCC Alert or an 'N15 Sequenced Request Received Out of Order' DCC Alert). The error handling required to do this may well be more complicated than orchestrating the sequence in the first place!

Message IDs

One thing's for certain, a *lot* of messages are going to be passing through the DCC. In order to keep track of them all, every Service Request, Service Response, DCC Alert and Device Alert is required to have a unique Message ID and, in order for it to be unique, Message IDs are *big* numbers. I mean *really big*. A Message ID is a concatenation of three parts:

- **Business Originator ID:** A *Globally Unique Identifier (GUID)* that uniquely identifies the sender of the message.
- **Business Target ID:** A GUID that uniquely identifies the message's recipient.
- **Originator Counter:** A value that's numerically greater than the Originator Counter that the sender has previously used in any messages sent to that particular recipient.

Globally Unique Identifiers are 64-bit identifiers that use the Institute of Electrical and Electronics Engineers (IEEE) 64-bit Global Identifier (EUI-64) standard. In the context of the SMIP, GUIDs are used to uniquely identify DCC Users and devices across GB smart metering.

TECHNICAL STUFF

Once translated into GBCS, Message IDs also include a Command Response Alert (CRA) Flag which denotes whether the ID relates to a Service Request (‘C’), Service Response (‘R’) or Alert (‘A’). However, DCC Users don’t get to see this.

Take the example of a DCC User sending a Service Request to a device. The DCC User generates a Service Request ID comprising its own GUID (the Business Originator ID), the device’s GUID (the Business Target ID) and an Originator Counter larger than the one they last used when sending a Service Request to that particular device. When responding, the device generates a Service Response ID comprising its own GUID (the Business Originator ID), the DCC User’s GUID (the Business Target ID) and the same Originator Counter that was used in the Service Request ID (thus allowing the DCC User to match Service Response and Service Request).

REMEMBER

Recycling Service Request Originator Counters in Service Responses doesn’t mean that devices are let off the hook in terms of maintaining Originator Counters. Anyone or anything that wants to send an unsolicited message needs to be able to generate a Message ID, which means they need to maintain an Originator Counter. This includes devices generating Device Alerts and the DSP generating DCC Alerts, DSP Future Dated Service Requests and DSP Scheduled Service Requests.

Protection against replay

When a DCC User communicates with a specific device, the Business Originator ID and the Business Target ID don’t change but the Originator Counter must always increase. Well, that’s not strictly true. The need for an Originator Counter to constantly increase applies only to certain Service Request types: those that require *protection against replay.* These are Service Requests for which the safety of the civilised world depends on ensuring that they’re not processed more than once. That’s almost exactly half of device Service Request types. The obvious example is applying credit to a meter in prepayment mode but other examples include updating the meter’s debt and balance, disabling supply and updating security credentials.

Another point to note is that Originator Counters don’t need to be maintained for each individual recipient. For example, a DCC User could choose to hold a single Originator Counter and update it every time they send a Service Request, regardless of the intended device. Devices don’t insist on contiguous Service Request Identifiers, just ones that get bigger.

When generating multiple Service Requests of the same type and of a type that requires protection against replay, you need to ensure that they're sent in the right order and that receipt of each is confirmed before sending the next. Life gets even more complicated when sending combinations of Future Dated (DSP) and On Demand commands because an On Demand Service Request generated *after* having sent a Future Dated Service Request but *before* the execution date time of the Future Dated Service Request will cause the Future Dated Service Request to be rejected!

UTRN Counter

The most significant 32 bits of the Originator Counter are reserved for something called a *UTRN Counter*.

UTRNs (or *Unique Transaction Reference Numbers*, to give them their full title) are the smart replacement for the 50p pieces that you used to have to shove into prepayment meters. In the new smart world, if your smart meter is operating in prepayment mode, you buy credit from your supplier (via channels such as the web, phone, PayPoint or a PayZone) and your supplier sends a UTRN to your meter to top it up. Your supplier also provides you with a copy of the UTRN on your receipt so that, in the unlikely event that the UTRN fails to arrive via the SM WAN, you can enter the 20 digit number locally, either directly into the meter or via the Prepayment Interface Device (PPMID – see Chapter 3) if you've been provided with one.

Running out of Message IDs

DCC Users are going to be sending millions of messages so isn't there a danger that they'll use up their Originator Counters? Well, that's extremely unlikely to happen. Like the Business Originator ID and the Business Target ID, the Originator Counter is a 64 bit integer. The maximum number that you can hold in a 64 bit integer is 9,223,372,036,854,770,000. The estimated age of the universe is 13.7 billion years, or roughly 432,043,200,000,000,000 seconds. So, if you're an extremely keen early entrant to the market and you've been generating 20 Service Requests a second since the Big Bang, you'd only just be getting a little worried about running out of numbers (although you'd still have 923 million years to find a solution).

When sending the Service Request to credit your prepayment meter, your supplier increments the UTRN Counter (the most significant 32 bits of the Originator Counter). For all other Service Requests, they increment the least significant 32 bits. The maximum number you can hold in a 32 bit integer is a mere 2,147,483,647, which means if you were sending 20 Service Requests a second, this counter would only last 3.4 years.

But never fear. Every time the supplier sends a prepayment top-up and increments the UTRN Counter, they reset the least significant 32 bits and your 3.4 years starts again. ‘Ah, but what if my supplier doesn’t operate prepayment meters?’ I hear you cry. Well, if the least significant 32 bits of the Originator Counter do ever get used up, you’re allowed to start using the most significant 32 bits.

Oh, and the whole Originator Counter held on a device is also reset when a Known Remote Party updates their security credentials on that device, which happens on change of supplier or at least every 10 years (more on this in Chapter 6).

That’s almost certainly more than you ever wanted to know about Message IDs, but it’s probably worth mentioning too that a DCC User needs to use the same Service Request ID for a Critical Service Request and its corresponding Signed Pre-Command.

Sequence Diagrams

Not to be confused with Sequencing (see the earlier section), *Sequence Diagrams* are a useful pictorial representation of the end-to-end processing required for messages of different types. There are nine Sequence Diagrams in total and the choice of which to use depends on a combination of

- The type of message (Device Command, DCC Only Command, Device Alert, DCC Alert)
- Whether it’s Critical and/or Sensitive
- Whether the sender of the message is ‘known’ to the device (I explain what this means in Chapter 6)
- Whether or not the message is scheduled

After you've made the correct choice, the Sequence Diagram tells you in a step-by-step way what actions you need to take to process the message.

REMEMBER

Sequence Diagrams are immensely useful, so it's disappointing that they didn't make it into DUIS when it was translated from the *DCC User Gateway Interface Design Specification* (*DUGIDS* – see Chapter 7). Fortunately, they can still be found in DUGIDS even if their status has been relegated to that of 'for guidance only'.

Getting technical

So how do you actually send stuff to the DCC and get stuff back? Well, the technical implementation of the DCC User Interface is via web services, three to be precise:

- **Transform web service:** A synchronous interface for transforming Critical Service Requests into Pre-Commands.
- **DCC Only web service:** A synchronous interface for sending/receiving DCC Only Service Requests/Responses and/or HAN-ready commands for local delivery via an HHT.
- **Send Command web service:** An asynchronous interface for sending Non-Critical Service Requests or Signed Pre-Commands to devices.

In addition, a DCC User needs to provide their own *Receive Response web service* for receiving Service Responses and Alerts.

TECHNICAL STUFF

The DCC User Gateway accepts Service Requests or Signed Pre-Commands as XML documents submitted using an HTTP POST command. Similarly, the Receive Response web service provided by the DCC User needs to accept POSTed data. That's probably enough technical stuff for a For Dummies guide. For more info, go read the DUGIDS.

Coping When Things Go Wrong

Hard to believe, I know, but not everything is going to work perfectly all of the time. Smart meters are notoriously fickle and can object to garage doors being raised or trucks being parked nearby. DCC Users' systems may not be 100 per cent reliable, and the DCC itself may have the odd 'off' moment (indeed, its 99.95 per cent availability target equates to more than four hours of 'off moments' over the course of a year).

Error handling

So what happens if the DCC fails to deliver a Service Request? Well, it retries at least once – the number and frequency of retries depend on the nature of the Service Request. However, by the time it sends you back an N12 DCC Alert informing you that it's failed to deliver the message, you can be sure that it's tried pretty hard.

Even having successfully delivered a Service Request, the DCC doesn't just forget about it. If it doesn't see a corresponding Service Response, it tries sending the Service Request again, and only when this doesn't elicit a response does it send you a N13 DCC Alert to inform you of the failure.

Similarly, if you've sent off a Future Dated (Device) Service Request, the DCC keeps tabs on it for you and informs you if the expected response doesn't materialise (via an N10 DCC Alert). If it's a Future Dated (DSP) Service Request, the DCC tries to re-send the Service Request at least once before letting you know of the failure (via an N11 DCC Alert). The same applies for Scheduled (DSP) Service Requests (although you're on your own as far as Scheduled (Device) Service Requests are concerned).

And in the extremely unlikely event that your own systems are down when the DCC tries to send you something, it tries again in five minutes and keeps trying for two days before giving up.

Anomaly detection

Anomaly detection is really part of the SMIP end-to-end security model and, as such, you may have expected to find it in Chapter 6. However, it doesn't involve any cryptography and is very much involved in the logistics of sending/receiving messages, so I may as well cover it here.

The DCC has a SEC obligation to provide an anomaly detection service on incoming Service Requests, Service Responses and Alerts. What this means is that the DCC looks for suspicious transmission patterns where excessive numbers of messages of a given type are being sent or received. If it detects such behaviour, it will

1. Initially notify the DCC User in question.
2. *Quarantine* (hold on to) future messages of that type for subsequent release or deletion by the affected DCC User if the problem continues unabated.

The DCC operates two levels of anomaly detection:

- The first is across all DCC Users and is to protect the overall DCC service.
- The second level is DCC User-specific and operates against thresholds notified to the DCC by the DCC Users, themselves.

Anomaly detection thresholds are defined by Service Request Variant and can be set as a percentage of total expected monthly volume or as an absolute number. Both the DCC and DCC Users are only obliged under the SEC to define anomaly detection thresholds for Critical Service Requests and Service Requests that return sensitive data, but both are also at liberty to define anomaly detection thresholds for other types of Service Request Variant.

Anomaly detection thresholds could change over time. For example, a supplier putting up their prices for all their customers may need to temporarily increase the anomaly detection thresholds for the 1.2.1 Update Price (Primary Element) and 1.2.2 Update Price (Secondary Element) Service Requests. Unlikely, I know, but it could happen.

Communication of anomaly detection thresholds, notification of quarantined messages and instructions to release/delete quarantined messages is via an out-of-bounds interface with the DCC (so not via the DCC User Gateway).

Chapter 5

Messages

In This Chapter

- Cataloguing Service Requests
- Classifying DCC Alerts
- Compartmentalising Device Alerts
- Considering role-based access control

Whereas Chapter 4 describes some of the nuts and bolts involved in sending and receiving messages, this chapter focuses on the different types of messages that can be sent and received:

- Service Requests and their Responses
- DCC Alerts
- Device Alerts

I finish up by looking at how these message types map onto DCC User Roles (who's allowed to do what).

WARNING!

If a Technical Stuff alert could be applied to an entire chapter, it would certainly apply to this one. If you're going to be getting your hands dirty orchestrating Service Requests, Service Responses, DCC Alerts and Device Alerts, this is the chapter for you. If you're not, you have been warned.

Service Request Types

At time of writing 83 Service Requests exist, 20 of which have an additional 52 Service Request Variants between them. That's 115 commands in total, divided into 12 categories based on what they're for (as summarised in Table 5-1).

Table 5-1 Service Requests/Service Request Variants

Service	*No. of SRs*	*No. of SRVs*
Product Management (PMS)	5	4
Prepay (PS)	4	0
Customer Management (CMS)	5	0
Reading (RS)	15	17
Scheduling (SS)	3	0
Device Management (DMS)	19	20
Supply Management (SMS)	12	0
Device Estate Management (DEMS)	13	11
Customer Consent (CCS)	1	0
Firmware (FS)	3	0
Pre Device Installation (PDIS)	2	0
Record Network Data (RNDS)	1	0
Total	**83**	**52**

Based on DUGIDS v0.8.1.

Here's a quick guided tour of the categories and what they're for.

Product Management

The five Service Requests and four Service Request Variants that make up the Product Management Service are used to update the tariff and/or price held on a gas or electricity smart meter. As such, this category of Service Request is available only to import suppliers (that's Import Supplier (IS) and Gas Supplier (GS) DCC User Roles which correspond to electricity and gas suppliers, respectively). This category also includes Service Requests for import suppliers to

- Change the payment mode in which the meter is operating (from credit to prepayment or vice versa).
- Update a meter's balance including its debt registers.

Prepay

The four Service Requests that comprise the Prepay Service are available only to import suppliers (IS, GS) and are used to manage gas and electricity smart meters operating in prepayment mode. This includes

- Updating prepayment configuration (including emergency credit thresholds, debt recovery rates and non-disablement calendars).
- Updating debt registers.
- Activating emergency credit.

It also includes a Service Request for applying credit to meters by sending Unique Transaction Reference Numbers (UTRNs).

Customer Management

The Customer Management Service comprises five Service Requests that allow import suppliers (IS, GS) to manage the customer-facing aspects of a smart meter. This includes

- Displaying messages to the customer.
- Restricting access to historic data following a change of tenancy.
- Clearing event logs.
- Updating the name of the supplier displayed on the meter (following a change of supplier).
- Disabling privacy PINs set by the customer.

Reading

With 15 Service Requests and 17 Service Request Variants, the Reading Service is the second largest category of Service Requests. It contains Service Requests for reading the various measurements recorded by gas and electricity smart meters, including

- Consumption-related data (instantaneous, daily, profile reads and Billing Data Log files).

- Export-related data (instantaneous, daily and both active and reactive profile reads).
- Tariff-related stuff (tariffs, Time Of Use/Block matrices, Block Counters, meter balances).
- Prepayment-related stuff (instantaneous and daily reads, debt payments, credits and prepayment configuration).
- Network-related stuff (active import power reads, active/ reactive import profile reads, network data, maximum demands and load limits).

All DCC User Roles, with the exception of Registered Supplier Agents (RSAs), have access to the Read Service, the subset of Service Requests to which they have access depending on their role.

Scheduling

The Scheduling Service comprises three DCC Only Service Requests for creating, reading and deleting DSP schedules (see Chapter 4). These are available to all DCC Users with the exception of Registered Supplier Agents (RSAs).

Device Management

The 19 Service Requests and 20 Service Request Variants that make up the Device Management Service make it the largest category of Service Requests. It comprises Service Requests for reading and updating device configurations to which DCC Users have access, depending on their DCC User Role:

- Import suppliers (ISs and GSs) can perform a number of functions including
    - Synchronising a meter's clock.
    - Configuring its alert behaviour.
    - Updating the security certificates that it holds.
    - Setting the billing calendar that a meter uses to generate periodic, unsolicited billing reads.

    - Setting the import supply point with which a meter is associated.
    - Reading the device's make and model, and its security and event logs.

  In addition, ISs can set load limits, power thresholds and auxiliary load parameters, and GSs can set gas conversion and flow rates.

- Export Suppliers (ESs) can read details of the make, model and device ID of the electricity meter and its associated supply point, and set its export supply point.
- Network operators, that's Electricity Distributors (EDs) and Gas Transporters (GTs), can
    - Read how a device has been configured (by themselves or the import supplier).
    - Configure their own device alerts.
    - Read the device's event and security log.
    - Update their own keys on the device.
    - Read the device's make, model and device ID.

  In addition, EDs can set and reset maximum demand registers and read and update voltage thresholds.

- RSAs can read the device's configuration and its event and security logs.
- Other Users (OUs) are restricted to reading the device's make, model and device ID.

Supply Management

The 12 Service Requests that comprise the Supply Management Service allow an import supplier (IS, GS) to remotely manage the energy at a consumer premises (enable/disable supply and, in the case of ISs, control auxiliary loads).

Network operators (EDs and GTs) can read the supply status from the meters, as can RSAs. OUs get to read the configuration data relating to Home Area Network Connected Auxiliary Load Control Switches (HCALCSs) and Auxiliary Load Control Switches (ALCSs) and to read the details of any boost buttons present (see Chapter 3).

Device Estate Management

The common characteristic shared by the 13 Service Requests and 11 Service Request Variants that comprise the Device Estate Management Service is that they're associated with getting devices into or out of DCC service. This includes

- Commissioning/decommissioning of devices.
- Joining/unjoining devices to/from the Home Area Network (HAN).
- Opting non-domestic meters into or out of DCC service.

In addition, Service Requests exist for updating the DCC's Inventory and notifying the DCC of the plight of Communications Hubs (installed and connected/not connected to the SM WAN or returned to the DCC due to a fault or some other reason).

In terms of who gets access to Device Estate Management Service Requests,

- Import suppliers (ISs, GSs) get access to everything.
- Export Suppliers (ESs), network operators (EDs, GTs) and RSAs only get to read and update the DCC Inventory.
- In addition to reading and updating the DCC Inventory, OUs also get to join and unjoin Type 2 Devices (for example, Customer Access Devices (CADs) – see Chapter 3).

Customer Consent

The Customer Consent Service comprises a single Service Request that OUs can use to request a *Customer Identification Number (CIN)* for confirming the identity of a customer. On receipt of the request, the DCC generates a random four-digit number, sends this over the SM WAN to be displayed on the meter and also returns it to the requesting OU. The OU can then ask the customer to provide the CIN to verify he is who he says he is.

Firmware

The three Service Requests that comprise the Firmware Service are for import suppliers (ISs and GSs) to update and activate new versions of firmware on gas and electricity smart meters. In addition, import suppliers, network operators, RSAs and OUs are able to read the current version of firmware running on a meter.

Pre Device Installation

The Pre Device Installation Service comprises two Service Requests that are available to all DCC Users:

- The first allows a DCC User to find out whether there's Smart Metering Wide Area Network (SM WAN) coverage for a given address and, if so, what variant of Communications Hub (CH) should be used in that area.
- The second is for notifying the DCC Inventory of devices that are to be installed at some point in the future.

Record Network Data

The Record Network Data Service comprises a single Service Request available only to GTs to initiate recording of gas consumption data at six minute intervals over a four hour period in a gas smart meter. Too much detail? Let's move on.

DCC Alert Types

At time of writing, 40 different DCC Alert types exist. Table 5-2 categorises the DCC Alerts according to function.

Power Outage

This solitary DCC Alert is sent to the import supplier (IS) and the Electricity Distributor (ED) when a CH has detected a loss of mains power at a customer's premises of three minutes or more in duration. This is the fabled 'last gasp' which has got EDs mildly excited.

Table 5-2 DCC Alerts

Category	*DCC Alerts*
Power Outage	AD1
Device Status Change Event	N1, N2, N8, N9, N16, N28, N29
DSP Schedule Removal	N4, N5, N6, N17, N37
Command Failure	N3, N7, N10, N11, N12, N13, N14, N15, N33, N34, N35, N36, N38
Firmware Distribution Failure	N18, N19, N20, N21, N22, N23
Update HAN Device Log Result	N24, N25
Change of Supplier	N26, N27
Device Log Restored	N30, N31
CHF Post Commissioning Incomplete	N32
PPMID Alert	N39

Based on DUGIDS v0.8.1.

At time of writing, there was some debate as to exactly when a power outage DCC Alert (AD1) is generated. Originally thought to be three minutes after loss of supply, it transpires that it may be as long as 13 minutes following a loss of supply before Telefónica sends some AD1s.

Device Status Change Event

As the name suggests, these seven DCC Alerts notify DCC Users of changes to the status of Devices resulting from commissioning, decommissioning, suspension, restoration or change of identity (in terms of the supply point to which the device is associated). This includes notification that the DCC has automatically removed a device from the DCC Inventory that's been notified for more than a year but has never been installed.

DSP Schedule Removal

These five DCC Alerts notify DCC Users of the removal of DSP Schedules that they've previously set up. This could be due to a change of tenancy, a change of supplier, a device opt-out or a device being withdrawn or decommissioned.

Command Failures

These 13 (unlucky for some) DCC Alerts notify DCC Users of problems with the execution of Service Requests. As the large number of DCC Alerts in this category suggests, there are many reasons why a Service Request could fail. These include:

- **Cancellation of Future Dated (DSP) Service Requests:** In response to a change of tenancy, change of supplier, opt-out, withdrawal or decommissioning
- **Sequence-related failures:** Either the failure of a sequenced Service Request or a failure to receive a preceding Service Request in the sequence
- **Authorisation failures:** Failure of a DSP Scheduled or Future Dated (DSP) Service Request because the originating DCC User is no longer authorised to issue the Service Request
- **General Service Request failures:** Missing Future Dated (Device) Service Responses and failures of DSP Schedule, Future Dated and On Demand Service Requests (see 'Error Handling' in Chapter 4)

Firmware Distribution Failure

These six DCC Alerts are for notifying import suppliers (ISs and GSs) of problems related to firmware updates. Problems include validation failures when loading firmware images and errors passing firmware updates to the Communication Service Providers (CSPs).

Update HAN Device Log Result

These two DCC Alerts notify DCC Users of successful and unsuccessful attempts to update a CH's Device Log (something that needs to be done when adding or removing a device on the HAN).

Change of Supplier

There are two change of supplier-related DCC Alerts, both of which are sent to import suppliers (IS or GS). One notifies a losing supplier that their security credentials have been replaced with those of the gaining supplier following a change of supplier (the DUIS equivalent of a 'Dear John' letter). The other notifies an import supplier that their Service Request has failed due to the fact they're no longer the registered supplier for the meter.

Device Log Restored

These two DCC Alerts notify import suppliers (IS or GS) of the successful restoration of a CH's Device Logs upon replacement of said CH. The two DCC Alerts relate to the CH's two Device Logs – one relating to the Communications Hub Function (CHF) and the other to the Gas Proxy Function (GPF).

CHF Post Commissioning Incomplete

This solitary DCC Alert notifies tardy import suppliers that they've failed to meet their obligation to replace device Certificates within the allotted seven-day period following installation (you learn all about Certificates in the Chapter 6).

PPMID

This solitary DCC Alert is used by the DSP to forward Device Alerts from Prepayment Interface Devices (PPMIDs) to import suppliers (ISs and GSs). This is necessary because PPMIDs can be shared across the IS and GS who may not necessarily be the same supplier and the PPMID can't, therefore, get away with holding a single set of supplier Certificates (see Chapter 6). To get around this, the DSP acts as a trusted intermediary, forwarding all PPMID Device Alerts to the appropriate recipient(s).

Device Alert Types

At time of writing, there are 126 mandated Device Alert types (866 if you include the optional ones!). Before getting into what they're all for, it's probably worth looking at the different types of Alert that a device can generate.

- **Destination:** Not all Device Alerts are sent to DCC Users. Some only make it as far as the device's log or, possibly, as far as the Home Area Network (HAN) in order to notify other devices that something's happened. A total of 91 Device Alert types make it as far as DCC Users.
- **Payload or no payload:** All Device Alerts include an alert code and a timestamp but some contain additional information. For example, a supply restoration Device Alert contains the times of the interruption and subsequent restoration. Of the 91 Device Alerts sent to DCC Users, about 15 per cent carry a payload.
- **Critical or non-critical:** Like Service Requests, not all Device Alerts are born equal. Some are considered more important than others. Those relating to supply, financial or security matters are deemed *Critical* and must be digitally signed by the device (this applies to a little over 40 per cent of the 91 Device Alerts sent to DCC Users).
- **Sensitive or non-sensitive:** Only one Device Alert carries a payload that's deemed to be sensitive and that's the Billing Data Log Updated Device Alert. Its sensitivity is due to the fact that it contains consumption information which is considered personal data under the Data Protection Act.

As to what they're all for, I've grouped the 91 Device Alerts received by DCC Users into the 12 categories listed in Table 5-3.

Access Control

These three Device Alerts are used by the device to notify import suppliers (ISs and GSs) of authentication failures (the device doesn't recognise the supplier) or attempts to instigate commands by those not authorised to do so.

Table 5-3 Device Alerts

Category	*No. of Device Alerts*
Access Control	3
Battery	3
Clock	1
Command Confirmation/Failure	3
(De)Commissioning	2
Firmware	2
Billing Data Log	1
Prepayment	4
SMKI	1
Supply Enablement/Disablement	16
Tamper	7
Voltage	48
Total	**91**

Based on DCC MMC v0.8.1.

Battery

These three Device Alerts are sent to gas import suppliers (GSs) in response to problems with the battery of a gas smart meter.

Clock

This solitary Device Alert is sent to import suppliers (ISs and GSs) in response to an unsuccessful attempt to adjust a meter's clock.

Command Confirmation/Failure

These three Device Alerts are sent to import suppliers (ISs and GSs) to notify successes and failures in executing HAN commands.

(De)Commissioning

These two Device Alerts notify import suppliers (ISs and GSs) of successfully commissioned devices and devices that have successfully joined the HAN.

Firmware

These two Device Alerts are used to notify import suppliers (ISs and GSs) whether or not a device has successfully validated a new set of firmware.

Billing Data Log

This is the one single Device Alert that contains a sensitive payload. It's generated by a meter according to the Billing Calendar set up by the meter's import supplier (IS for an electricity meter, GS for a gas meter). When generating the Device Alert, the meter encrypts the sensitive payload (namely, the consumption data) in such a way that only the receiving import supplier can decrypt it.

Prepayment

These four Device Alerts notify import suppliers (ISs and GSs) of prepayment-related events such as

- Credit being added to a meter locally
- Credit falling below the configured low credit and disablement thresholds
- Activations of emergency credit

WARNING!

Prepayment-related Device Alerts will give suppliers much greater visibility of how many customers self-disconnect through lack of credit, how often this happens and for how long. Some network operators are concerned that the improved visibility of power outages provided by power outage and restoration alerts could lead to a tightening of Ofgem incentives relating to Customer Minutes Lost (CML). Suppliers should be equally concerned that improved visibility of self-disconnections may lead to more incentives in this area.

SMKI

This Device Alert notifies DCC Users of a successful update of Certificates held by the device to authenticate messages it receives (see Chapter 6).

Supply Enablement/Disablement

These sixteen Device Alerts inform import suppliers (ISs and GSs) and network operators (EDs and GTs) of

- Planned supply disablement and enablement
- Restoration of unplanned supply outages
- Supply loss and re-enablement following a load limit breach

Tamper

These seven Device Alerts inform import suppliers (ISs and GSs) and network operators (EDs and GTs) of different flavours of unauthorised physical access to the meter (such as removal of a battery cover, meter cover or terminal cover, or the presence of a strong magnetic field).

Voltage

By far the largest group, these 48 Device Alerts are sent to EDs to notify of voltage-related events such as the average Root Mean Square (RMS) voltage going above or below thresholds that have been pre-configured by EDs using Device Management Service Requests. Again, it's not inconceivable that greater visibility of voltage problems could allow Ofgem to focus incentives in this area.

Role-Based Access Control

Another way to look at Service Requests, Service Responses, DCC Alerts and Device Alerts is to consider who gets to do what. The DUIS defines which Service Request and DCC Alert types each DCC User Role is allowed to access, and the GB

Companion Specification (GBCS) does the same for Device Alerts. Table 5-4 shows the number of Service Request types, DCC Alert types and Device Alert types available to each DCC User Role.

Table 5-4 Service Requests/DCC Alerts/Device Alerts by DCC User Role

DCC User Role	*Service Request Types*	*DCC Alert Types*	*Device Alert Types*
IS	101	37	27
GS	78	37	27
ES	16	18	0
ED	33	23	68
GT	21	23	5
RSA	15	13	0
OU	22	19	0
Dual Fuel Supplier (IS, GS, ES, OU)	111	38	32

Based on GBCS v0.8.1.

As Table 5-4 shows, access to DCC Services varies significantly between different DCC User Roles.

Energy suppliers

The average import supplier (IS and GS) has access to more than three times as many Service Request types as a network operator. There's very little a supplier can't access in terms of smart functionality and data. (The notable exceptions are configuration of voltage thresholds and maximum demand registers.) Export Suppliers (ES) are largely restricted to using export-related functionality and, other than RSAs, have access to the least number of DCC Services.

Network operators

Network operators (EDs and GTs) are mainly restricted to reading information from devices including

- Consumption and export
- Network-related data (voltage, reactive power, maximum demand and so on)
- What load limiting, if any, has been configured by the supplier

Their only Critical Service Request is for changing their Organisation Certificate (more on this in Chapter 6), and the only other things they can change on the meter are voltage thresholds and alert behaviour.

Registered Supplier Agents

Registered Supplier Agents (RSAs) have the most restricted access to DCC Services of any DCC User Role. They can

- Read meter configurations, event and security logs.
- Read supply status and firmware versions.
- Pre-notify devices to the DCC.

As Chapter 2 discusses, this meagre set of Service Requests doesn't allow an RSA to install a meter without direct intervention from the registered import supplier and the RSA DCC User Role appears to be aimed primarily at Meter Asset Providers (MAPs) monitoring the health of their assets.

Other Users

Other Users (OUs) get to read

- Profile data (active import, reactive import and export)
- Daily consumption
- Tariffs
- Device and auxiliary load configurations
- Firmware versions

OUs also get to add Type 2 devices to the HAN (for example, they can offer a binding service for Customer Access Devices – see Chapter 3).

Chapter 6

End-to-End Security

In This Chapter

- ▶ Deciphering cryptography
- ▶ Picking over PKI
- ▶ Knowing about Known and Unknown Remote Parties
- ▶ Recovering when everything goes pear shaped

‘Security by design’ has been the mantra of the SMIP since the get-go, and if you spend any time around the programme, you won’t be able to avoid talk of Public/Private Key Pairs, Message Authentication Codes, Smart Metering Key Infrastructures, Certificates and Certificate Signing Requests. In *GB Electricity Industry For Dummies*, smart meter security received three paragraphs, concluding that the SMIP security model probably warranted a *For Dummies* guide in its own right. Here, it gets a whole chapter (but still probably warrants its own guide).

Very few of us aspire to be security experts, but security is such a driver within the SMIP that a basic understanding of how the end-to-end security model works is probably worth having. That said, feel free to bail out of this chapter whenever you like!

WARNING!

Not only is the security model unique to the SMIP, a case could be made for it being the primary reason for the programme’s delay. Changes to the security model relatively late in the procurement cycle, combined with the move to a new hybrid version of cryptography, has led to delays in agreeing the protocols to be used by devices, documented in the GB Companion Specification (GBCS). Consequentially, this has delayed the production of the devices themselves.

Rethinking the Security Model

While the Department of Energy and Climate Change (DECC) were in the throes of procuring the Data Communications Company (DCC), Data Service Provider (DSP) and Communication Service Providers (CSPs), CESG (the Communications Electronics Security Group, a.k.a. the National Technical Authority for Information Assurance, the government's security experts) took a belated interest in the programme and insisted on a major change to its security model.

Prior to their interest, much faith had been placed in the DSP as custodian of the cryptographic keys required to communicate with all devices. In simple terms, DCC Users told the DSP what they'd like to do, and the DSP was responsible for telling the device over a secure connection. This did mean, however, that the DSP was a single point of failure. If the DSP was ever compromised (for example, externally hacked or attacked by a disgruntled employee), then every device was also potentially compromised.

To remove this single point of failure, CESG insisted on an alternative end-to-end security model in which DCC Users were made responsible for securing communications all the way from their back office systems to the device, effectively relegating the DSP to a delivery mechanism. Under this system:

- A **device** knows about individual DCC Users and is able to authenticate that the messages it receives have come from someone it trusts.
- **DCC Users** know about individual devices and are able to authenticate that messages come from a known device.

This knowledge of one another comes through the sharing of cryptographic keys that are used to sign, authenticate and, where necessary, encrypt messages sent between DCC User and device.

Cryptography

Before going any further, you need a basic knowledge of cryptography. The security experts among you will want to skip this section. (As may the non-security experts.)

Cryptography comes from the Greek words *kryptós*, meaning 'hidden, secret', and *graphein*, meaning 'writing', and is the practice and study of techniques for secure communication in the presence of third parties. Cryptography can be used for

- **Encryption:** Encoding a message so that only authorised parties can read it.
- **Authentication:** Proving that a message is from whom it says it's from.
- **Ensuring integrity:** Proving that the message hasn't been tampered with in transit.

This is done using a combination of cryptographic keys and algorithms. To explain, I enlist the help of Alice, Bob and Eve, three fictional characters frequently used in cryptographic circles to explain how cryptography works. Suppose Bob wants to send Alice a secret message, but Eve is a third party trying to eavesdrop. . . .

Symmetric cryptography

In *symmetric cryptography*, the same key is used to encrypt and decrypt (analogous to a single key used to lock or unlock a door – hence symmetric). It requires both the sender (Bob) and recipient (Alice) to possess the *same* cryptographic key. If Bob wants only Alice to be able to see the message, he encrypts it using his copy of their shared symmetric key, and Alice decrypts the message using her copy of the key.

If Bob wants Alice to be able to authenticate the message (prove that the message is from him and no one else) and ensure its integrity (that it hasn't been interfered with by Eve in transit), he can take a portion of the message (a so-called *hash*), encrypt this using the shared symmetric key and attach the result (called a *Message Authentication Code* or *MAC* for short) to the message itself before sending it on to Alice. On receipt, Alice recalculates the MAC using the received message and her copy of the symmetric key. If the recalculated MAC matches the one attached to the message, Alice knows that the message can only be from Bob (because Bob is the only person who has a copy of their shared key) and that it hasn't been tampered with by Eve in transit (if it had, the MAC calculated using the corrupted message wouldn't have matched the MAC that it came with).

Symmetric keys work well and have been used in smart metering for some time, but they do have one major problem. For symmetric cryptography to work, Alice and Bob need to share the same symmetric key. How then do they exchange these keys without them falling into the unsavoury hands of Eve? This is where asymmetric cryptography comes in.

Asymmetric cryptography

In *asymmetric cryptography*, encryption and decryption are performed using *separate* keys: a *Public Key* and a *Private Key*. As its name suggests, the Public Key is made public (you can shout it from the rooftops) but the Private Key is kept secret.

For those interested, the Private Key comprises two really big prime numbers (numbers only divisible by themselves and 1). The Public Key is the number you get when you multiply these two really big prime numbers together.

The clever bit is that data encrypted using the Public Key can only ever be decrypted by the Private Key and, conversely, data encrypted using the Private Key can only ever be decrypted using the Public Key (an ironic bit of symmetry in asymmetric cryptography).

So Alice generates two very large prime numbers, multiplies them together and publishes the result as her Public Key, but keeps the two very large prime numbers (her Private Key) secret. As its name suggests, Alice can publish the Public Key to the world.

Now when Bob wants to send Alice a secure message, all he needs to do is look up Alice's Public Key, use it to encrypt the message and, bingo, he has an encrypted message that only Alice can decrypt using her Private Key. Similarly, if Alice wants to prove that she's the sender of a message and that it hasn't been tampered with in transit, she can encrypt a hash of it using her Private Key and add it to the message, and Bob can authenticate Alice as the sender by decrypting the hash with Alice's Public Key. Clever, huh?

The asymmetric equivalent of a MAC is a called a *digital signature*. Digital signatures include the name of the hashing algorithm used in generating the signature.

Clearly, if Eve had a big enough computer and enough time, she could work out Alice's Private Key by trial and error (a process called *factoring* in which she multiplies every possible combination of prime numbers until she finds the two that were used to generate Alice's Public Key). However, factoring is very time-consuming and gets harder the larger the prime numbers are. The prime numbers used in Private Keys tend to be *very* large, making it computationally infeasible for them to be factored.

Asymmetric versus symmetric cryptography

The major advantage of asymmetric cryptography over symmetric cryptography is that Bob and Alice no longer need to exchange keys other than Public Keys, which are, well, public. The major disadvantage is that asymmetric cryptography requires more processing power. This isn't a problem for your average computer these days, but it does present a challenge for a smart meter, especially a gas meter that's required to eke out its 10 to 15 year life on the power of a single battery. For this reason, smart metering has traditionally used symmetric cryptography, which requires less processing power.

Symmetric cryptography was fine when smart meters weren't that smart and only tended to provide meter readings. However, meters are getting smarter and can now be used to remotely switch load, disable supply, change tariff and add credit. Compromise of these critical messages (called *Critical Service Requests* – see Chapter 4) could lead to loss of power, financial fraud or security breaches.

For this reason, the SMIP has gone for a hybrid asymmetric/ symmetric security model that uses

- **Asymmetric cryptography** for authenticating and integrity checking of Critical Service Requests, and for authentication between the DCC and its users.
- **Symmetric cryptography** for the authentication and integrity checking of more mundane messages and the encryption of sensitive data.

Asymmetric cryptography trumps symmetric cryptography in that *anyone* can authenticate and integrity check an asymmetrically generated digital signature because you only need the message and the sender's Public Key. A MAC, however, can only be authenticated by the intended recipient (the person with the shared symmetric key). Allowing multiple parties to authenticate the same message has its advantages. Say a DCC User makes a change to a smart device that the DCC would like to know about and record in their Inventory. Assuming the device has signed its Service Response asymmetrically, both the DCC User and the DCC can authenticate that the Service Response has come from the expected device, allowing both to update their systems accordingly.

Another major advantage of asymmetric cryptography is that it solves the key distribution challenge facing symmetric cryptography. Thanks to some cryptographic magic, Bob and Alice can combine their own Private Key with the other's Public Key to generate a common symmetric key that they can then use for authentication, encryption and integrity checking.

'Very clever!' I hear you exclaim. 'But why bother? Why not use the asymmetric keys themselves?' Well, if you remember, encrypting or decrypting something using symmetric keys is less cryptographically strenuous than using asymmetric keys, whereas the overhead of generating symmetric keys using asymmetric key pairs is relatively low.

So a device can digitally sign the really important stuff (Critical Service Responses and/or Alerts) using its asymmetric key and sign less important stuff by generating MACs using a symmetric key generated from its asymmetric key. This judicious use of both asymmetric and symmetric cryptography is what gives the hybrid security model its name.

The cryptographic magic that allows two Public/Private Key Pair owners to generate a common symmetric key (often referred to as a 'shared secret') is even cleverer than it first appears. By introducing some information taken from the message, a different symmetric key is generated for every message. The use of so called 'one-time' shared secrets makes this process even more secure.

The SMIP's security model insists on separate Public/Private Key Pairs for digitally signing messages and for generating shared symmetric keys. The former is the *Digital Signing Public/Private Key Pair* and the latter is called the *Key Agreement Public/Private Key Pair*. There's also a separate Key Agreement Public/Private Key Pair for generating Unique Transaction Reference Numbers (UTRNs – see Chapter 4). They're all asymmetric cryptographic key pairs, just used for different purposes.

REMEMBER

Like DCC Users, devices need to hold separate Key Agreement and Digital Signing Public/Private Key Pairs. When kicking a device to regenerate its Public/Private Key Pairs (which, as a supplier, you have a Smart Energy Code (SEC) requirement to do within seven days of installing a meter), don't forget to tell it which one to regenerate.

Public Key Infrastructure (PKI)

Being able to ensure that a message has come from the owner of a specific Public/Private Key Pair is great so long as you know who the owner is. With the computing power available these days, anyone can generate a pair of large prime numbers. So how do you know that the DCC's Public Key really *is* the DCC's Public Key and doesn't belong to someone pretending to be the DCC?

This is where a *Public Key Infrastructure (PKI)* comes in. It's a means of binding Public Keys to user identities by means of a trusted third party known as a *Certificate Authority (CA)*. The binding is achieved through a registration and issuance process:

1. A would-be Public/Private Key Pair owner registers with a CA by providing a sufficient proof of identity.
2. When the CA's convinced that the party is who they claim to be, they issue a *Certificate* that incorporates the Public Key within a set of *Credentials* that affirm the identity of the owner and that of the issuer.

The 'Infrastructure' in PKI refers to all the hardware, software, people, policies and processes needed to create, manage, distribute, store and revoke these Certificates.

Certificates and Public Keys are two different things. A *Public Key* is the number you get when you multiply together the two very large prime numbers that make up a Private Key. A *Certificate* is issued for a Public Key to bind it to an identity and incorporates the Public Key itself, together with information about its owner and the issuer of the Certificate. Certificates are also sometimes referred to as *Credentials*.

PKI Roles

In its simplest form, a PKI comprises:

- **A Root CA:** A trusted third party who can authenticate one or more Issuing CAs.
- **An Issuing CA:** The party responsible for issuing Certificates.
- **A Registration Authority (RA):** The party responsible for receiving Certificate Signing Requests (CSRs) from Subscribers (those wishing to prove ownership of a Public/Private Key Pair) and verifying the Subscriber's identity.
- **A CA Repository:** A store of all the Certificates that have been issued by the Issuing CA.

Here's the process:

1. The RA receives a Certificate Signing Request (CSR) from a Subscriber (someone wanting to be able to prove that a Public Key belongs to them) and verifies that the Subscriber is who they say they are.
2. The RA passes the CSR on to the Issuing CA, who issues a Certificate to the Subscriber and places a copy of the Certificate in the CA Repository so that anyone interested in authenticating or checking messages from the Subscriber can get hold of the Subscriber's Public Key.

RAs can also receive *Certificate Revocation Requests (CRRs)* from Subscribers if they need to revoke a Certificate (in the event of a key compromise, for example). This results in the status of the Certificate being updated in the CA Repository to reflect its revocation and the Certificate being added to a

Certificate Revocation List (CRL) that's periodically sent out to all Subscribers.

PKIs are commonplace and the chances are you use one every day. That little padlock that appears in your browser when you're making an online purchase, for example, is an indicator that you're in the presence of a PKI.

SMKI, DCCKI and IKI

Sounding suspiciously like a trio of lovable Disney characters, these are actually all different flavours of PKI used within the SMIP:

- Smart Metering Key Infrastructure (SMKI)
- Data Communications Company Key Infrastructure (DCCKI)
- Infrastructure Key Infrastructure (IKI)

They're PKIs, and so they all comprise a Root CA, Issuing CA, RA and CA Inventory. Figure 6-1 attempts to explain what they're all for.

Smart Metering Key Infrastructure (SMKI)

The *SMKI* is used for authenticating messages sent between parties within the SMIP. That could be a DCC User authenticating an alert from a device or the DCC authenticating a Service Request from a DCC User. Authentication could use Digital Signing SMKI keys or symmetric keys generated using Key Agreement SMKI keys, depending on whose doing the signing and what it is they're signing. SMKI keys will also probably be used to digitally sign the registration files exchanged between the Registration Data Providers (RDPs) and the DCC (see Chapter 2).

The SMKI has separate Root CAs and Issuing CAs for

- **Organisation Certificates:** Used to identify DCC Users. Organisation Certificates are obtained by manually accessing the SMKI Portal.
- **Device Certificates:** Used to identify devices. Device Certificates can be obtained manually via the SMKI Portal or via a web service and/or file interface.

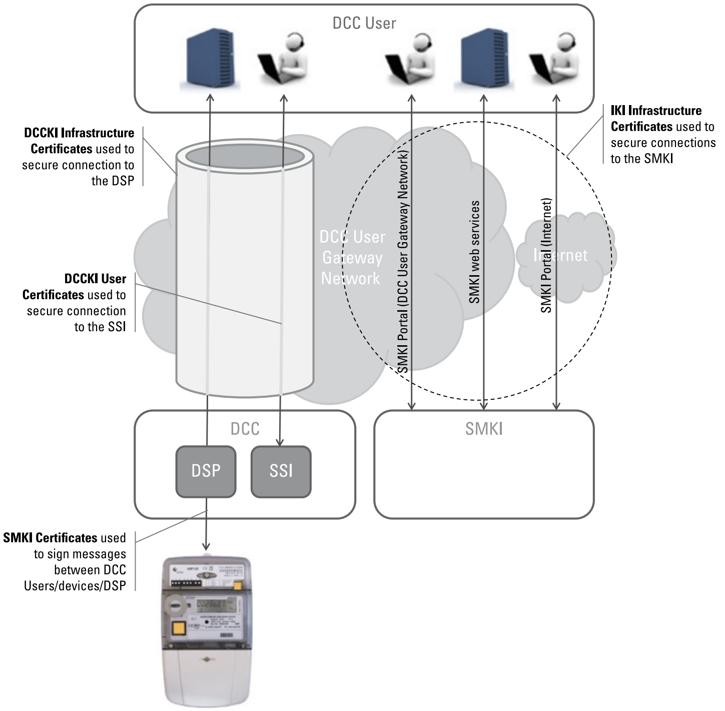

DCC User
DCCKI Infrastructure Certificates used to secure connection to the DSP
IKI Infrastructure Certificates used to secure connections to the SMKI
DCC User Gateway Network
SMKI Portal (DCC User Gateway Network)
SMKI web services
SMKI Portal (Internet)
Internet
DCCKI User Certificates used to secure connection to the SSI
DCC
DSP
SSI
SMKI
SMKI Certificates used to sign messages between DCC Users/devices/DSP

Figure 6-1: IKI, SMKI and DCCKI.

CSRs can also be submitted for both Organisation and Device Certificates via an Internet version of the SMKI Portal for Non-Gateway Suppliers (see Chapter 2).

Three types of Organisation Public/Private Key Pairs exist. The Digital Signing Key Pair is used for signing messages, whereas the two sets of Key Agreement Key Pairs (one for general use and one for generating UTRNs) are used to create ‘shared secrets’ (symmetric keys for MAC’ing and encryption).

Installing suppliers have a SEC obligation to instruct a smart meter to regenerate its Public/Private Key Pairs within seven days of installation. When actioning this Service Request, the device returns a CSR for its new Public Key in its Service Response, which the supplier then signs and submits to the Registration Authority. The supplier then uses another Service Request to place the Certificate returned by the RA back onto the device.

Data Communications Company Key Infrastructure (DCCKI)

The *DCCKI* is used for securing the links between DCC Users and the DCC User Gateway Network and for authenticating individual users accessing the DCC's *Self Service Interface* (*SSI* – see Chapter 9).

The DCCKI has two Issuing CAs, one for each of its functions.

- **Issuing Infrastructure CA:** Issues infrastructure Certificates for DCC Users to use when establishing *Transport Layer Security (TLS)* sessions between their *Policy Enforcement Point (PEP)* and the DCC (essentially a secure pipe into the DCC).
- **Issuing User CA:** Issues Certificates to be used by individuals wishing to log on to the DCC's Self Service Interface.

REMEMBER

In addition to securing the DCC User Gateway Network interface between DCC Users and the DCC, DCCKI keys are also used for securing the interfaces between *Registration Data Providers* (*RDPs* – see Chapter 2) and the DCC.

Infrastructure Key Infrastructure (IKI)

The *IKI* (great name, huh?) is used for securing the interfaces into the SMKI, of which there are several:

- **SMKI Portal Interface** accessible to DCC Users via the DCC User Gateway Network and a Non-Gateway, internet equivalent for Non-Gateway Suppliers (suppliers who aren't yet DCC Users)
- **SMKI web service** for submitting device CSRs
- **SMKI automated batch web service** interface for submitting batch CSRs for Device Certificates

The structure of the various flavours of PKI is illustrated in Figure 6-2. The SMKI and IKI are provided by BT, the DCC's *Trusted Service Provider* (*TSP* – see Chapter 2). The DCCKI is provided by the DCC's *Data Service Provider (DSP)*. The DSP is also responsible for providing both the DCCKI and SMKI Repositories.

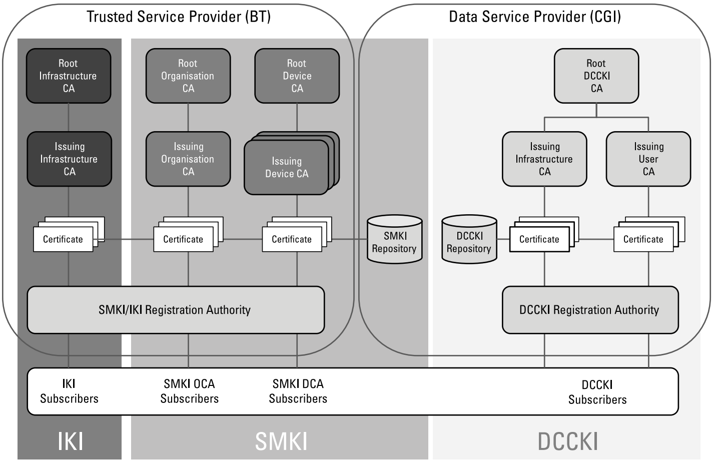


Figure 6-2: IKI, SMKI and DCCKI.

One Issuing OCA, many Issuing DCAs

The eagle-eyed among you might have noticed that the SMKI has a single Issuing Organisation CA (OCA) but multiple Issuing Device CAs (DCAs). This is because there's a DCC-imposed limit on the number of live Certificates that can be issued by a SMKI Issuing CA (currently, 100,000). Although it's highly unlikely that the Issuing OCA is ever going to reach this figure (especially because Organisation Certificates can be revoked), an Issuing DCA will reach this number without even breaking sweat (especially because Device Certificates can't be revoked). So, having issued its quota of Device Certificates, an Issuing DCA closes its doors for new business and a new Issuing DCA takes over. Its predecessor remains open, however, to service the Certificates that it's issued.

In addition to the DCC User Gateway Network, there's also a Non-Gateway Interface for use by Non-Gateway Suppliers (suppliers who have yet to become DCC Users). The Non-Gateway Interface allows Non-Gateway Suppliers to get Organisation Certificates from the SMKI and request the DSP to put these on DCC-serviced meters that they happen to have gained through the change of supplier process. Given that the Non-Gateway Supplier can't access any other DCC services, the meter is, to all intents and purposes, dumb, but at least it's ready for when the Non-Gateway Supplier becomes a DCC User.

Known and Unknown Remote Parties

One of the features of the SMIP security model is the ability for some smart devices to know about individual DCC Users and be able to authenticate that the messages they receive have come from trusted parties. In this context, *knowing* someone means holding their Organisation Certificate in something called an *anchor slot* within the device.

Figure 6-3 illustrates the anchor slots within the different types of smart device. As you can see, all devices have Root OCA and Recovery anchor slots containing DCC Organisation Certificates. These are used for recovering the device in the event that its keys are compromised (more in the later 'Recovery' section).

PARTY	CERTIFICATE	ESME	GSME	CHF	GPF	PPMID	HCALCS
DCC	Root OCA	■	■	■	■	■	■
	Recovery	■	■	■	■	■	■
Supplier	Digital Signature	■	■		■		■
	Key Agreement	■	■		■		
	Key Agreement (UTRN)	■	■				
Network Operator	Digital Signature	■			■		
	Key Agreement	■			■		
DCC	Digital Signature (ACB)			■		■	
	Key Agreement (ACB)	■	■	■	■	■	■
	Digital Signature (tCoS)	■	■		■		■
	Digital Signature (WAN)			■			

■ Anchor slot populated with Certificate

ACB: Access Control Broker
tCoS: Transitional CoS
WAN: WAN Provider

Figure 6-3: Device anchor slots.

If a device holds a DCC User's Organisation Certificate in one of its anchor slots, the DCC User is said to be *known* to the device or, in other words, the DCC User is a *Known Remote Party (KRP)* with respect to that device. Conversely, if the device doesn't hold a DCC User's Organisation Certificate, the DCC User is *unknown* to the device and is an *Unknown Remote Party (URP)* with respect to that device.

URPs can still talk to devices but need the DSP's help to do so. When submitting a Service Request to the DSP, the URP includes its Organisation Certificate. The DSP (who is known to, and trusted by, *all* devices) adds the URP's Organisation Certificate to the Service Request it sends to the device, and the device uses said Organisation Certificate to generate a shared secret for encrypting and/or MAC'ing the Service Response/Device Alert (URPs don't get to do any Critical Service Requests, therefore, the device never has to digitally sign anything that it sends to a URP). URPs include Registered Supplier Agents (RSAs) and Other Users (OUs).

TIP

Anchor slots must *always* be populated. Clearly, despite their name, not all Known Remote Parties are known at the time the meter is manufactured. The supplier may be known (if they placed the order for the meter, for example), but the network onto which the meter will be installed probably isn't, so it's not possible to populate the network operator anchor slots with the correct Organisation Certificates. In this case, the meter manufacturer can use either the supplier's Organisation Certificate or the DSP's Access Control Broker (ACB) Organisation Certificate (the Certificate the DSP uses to communicate with the device) as a placeholder until the meter's installed and the supplier can change the Certificate to the Organisation Certificate of the appropriate network operator (the one whose network the meter has ended up on).

TECHNICAL STUFF

Prepayment Interface Devices (PPMIDs) don't hold supplier Certificates, relegating the supplier to the lowly status of URP even though the PPMID is a Type 1 Device (can issue and execute Home Area Network (HAN) commands – see Chapter 3). This may seem a bit strange at first sight; however, the explanation is that a PPMID can be shared between two different suppliers if the customer has elected to buy the gas and electricity from two different companies. For this reason, the DSP acts as a trusted intermediary, using its ACB Certificate to sign messages to the PPMID on behalf of the supplier(s).

Recovery

So what happens if, despite your best endeavours, one of your Organisation Private Keys is compromised (nicked, pilfered, lost, stolen, abducted, held against its will and so on)?

The first option is to try to sort it out yourself by updating the Organisation Certificates in every affected device using the compromised key pair. Trouble is, you need to do this ahead of whatever nefarious scheme the perpetrator who compromised your security had in mind (hence this approach is often referred to as 'winning the race'). Should you choose to try this anyway (and, given the alternatives I go on to describe, you'd be stupid not to), you'll need to:

- Generate a new Organisation Public/Private Key Pair and obtain an associated Certificate (or, alternatively, have some spare keys and Certificates to hand).
- Contact the DCC to temporarily change your Anomaly Detection Thresholds relating to the 6.15.1 Update Security Credentials (KRP) Service Requests so that you can send lots of them (see Chapter 4).
- Send out the messages as fast as you can.

Convening a Key Ceremony

In order for the DCC to attempt a recovery with either the Recovery Key or Root OCA Key, a *Key Ceremony* must be convened. A Key Ceremony is a meeting of *Key Custodians*: a set of nominated individuals charged with protecting the security of the smart metering infrastructure. As with gatherings at Masonic lodges, what happens at a Key Ceremony is something of a mystery, but suffice to say that a sufficient number of nominated Key Custodians (the so-called 'n of m') must turn up to provide access to the Private Recovery Key necessary for the recovery exercise to proceed.

However, if that doesn't work, things start to get a bit more complicated (and expensive) because you're forced to turn to the DCC for help. The DCC has two ways of recovering keys on a meter, neither of which is trivial:

- Use a Recovery Key installed in one of the anchor slots on the device.
- Use a Contingency Key that's hidden in the Root OCA Key, also installed in one of the device's anchor slots.

Both methods require the co-operation of not only the DCC but also other stakeholders in the industry.

Avoid becoming a Key Custodian! You will be expected to be on call 24 hours a day. The SMKI PMA will ask parties to nominate Key Custodians from bodies such as the SMKI PMA, DCC, SEC Panel and DCC Users and, similar to an Authorised Responsible Officer (ARO), a Key Custodian is a named individual. If you take my advice, keep your head down!

Using the Recovery Key

The least drastic form of recovery is to use the Recovery Key, the Certificate of which sits on every device and allows the DCC to replace KRP Certificates on behalf of a compromised party.

If the compromised party is capable, it could provide the DCC with the alternative Certificate that the DCC should use when replacing the compromised Certificate. However, if they're not in a state to be able to do this (and, let's face it, they're probably having a bad day), the DCC can replace the compromised key with its own ACB Certificate and the compromised party can then request control to be handed back at a later date when they're ready by issuing a 6.21 Request Handover of DCC Controlled Device Service Request.

DECC's original intention was that, should the Recovery Key ever need to be used, it should then be replaced (the rationale being that it had now been 'exposed to the world' and, therefore, the threat of compromise). After they realised that this would mean replacing the Recovery Certificate in *every single* device, whether installed on someone's wall, sitting in a meter operator's van, stowed in a warehouse or trundling along a production line, they relented.

However, to reduce the amount of time that the Recovery Key is exposed, DSP recovery environments need to be brought up for a limited period only when required and then taken down again immediately afterwards. The time required to do this, combined with that required to assemble 'n of m' Key Custodians, suggests that recovery process isn't going to be especially quick. Or cheap. In fact it's likely that there will be need to be a minimum threshold of compromised devices before a recovery process can be instigated.

Armageddon

The disaster scenario is that a DCC Private Key is compromised and with it every smart device in the country (plus any that have elected to go on holiday). Should this happen, the DCC can resort to using the *Contingency Key*.

REMEMBER

Just to remind you, the *Root OCA Certificate* is contained on every device. This is the Certificate from which the chain of trust stems. Embedded within this Certificate is the encrypted Public Key of a Contingency Public/Private Key Pair. As its name suggests, the Contingency Key is only for use in dire circumstances (I'm talking 'in case of emergency, break glass' situations).

So how did there come to be an encrypted Contingency Public Key embedded in the Root OCA Certificate? Well, the Contingency Public/Private Key Pair was originally generated by the DSP who passed the Public Key to the Trusted Service Provider (TSP). The TSP then encrypted the Contingency Public Key using a symmetric key. This symmetric key was then broken up into bits and the bits stored securely in multiple locations. The encrypted Contingency Public Key was then embedded in the Root OCA Certificate before the latter was made available to device manufacturers for use in populating the Root OCA anchor slot during manufacture.

In the unhappy event that the Contingency Key is needed:

1. A Key Ceremony is convened.
2. The bits of the symmetric key that was used to encrypt the Contingency Public Key are retrieved from their various secure hiding places.
3. The symmetric key is reassembled and included as plain text in an instruction to devices to replace the Root OCA Certificate.
4. The DSP signs the instruction with the Contingency Private Key and sends it to every device.
5. On receipt of the instruction, a device uses the symmetric key included in plain text within the instruction to decrypt the Contingency Public Key embedded in the Root OCA Certificate.
6. The device uses the decrypted Contingency Public Key to authenticate the instruction to replace the Root OCA Certificate.
7. Assuming all is well, the device replaces the Root OCA Certificate with the new Root OCA Certificate contained in the instruction.

Because the replacement Root OCA Certificate contains a new embedded, encrypted Contingency Public Key, Contingency Keys are, by definition, one-time-use-only.

WARNING!

The recovery process is destined to be documented in a couple of SEC Subsidiary Documents (one on the overall Recovery Procedure, the other focusing on the SMKI – see Chapter 7). These have all the hallmarks of becoming the cryptographic equivalent of ‘Protect and Survive’ – the public information booklet produced by the government in the late 1970s to inform the public what they should do in the event of a nuclear attack.

Chapter 7

The Smart Energy Code (SEC)

In This Chapter

- Sauntering through the Smart Energy Code
- Totting up SEC Subsidiary Documents
- Naming Named Documents
- Looking for guidance

If you're going to get involved in the SMIP, you can't avoid the fact that you'll be spending an inordinate amount of time wading through reams of documentation. At the heart of this pile, lies the *Smart Energy Code (SEC)*, the word of DECC and, as such, the definitive text to which all defer as the single source of truth. Yet the nearly 140,000 words that make up the main body of the SEC represent just the tip of the SMIP documentation iceberg. In addition to the SEC's six schedules, there are currently another 44 SEC Subsidiary Documents (there may be more) plus another 22 non-SEC Subsidiary Documents that are named within the SEC.

This chapter attempts to give you an overview of the available reading matter, sorting out the wheat from the chaff to help you make best use of your reading time. I start with a brief outline of how SEC governance works, move on to a rapid tour of the SEC itself, take a quick peek at its Schedules and then try to make sense of the myriad of SEC Subsidiary Documents that the SEC has spawned. Finally, I take a fleeting glance at the other documents named within the SEC but not considered worthy of the status of 'SEC Subsidiary Document' including the new breed of 'guidance document'.

Getting to Know the SEC

Starting at the tip of the iceberg, what is the SEC and how did it come about?

The SEC is a multi-party agreement that defines the rights and obligations of energy suppliers, network operators and other relevant parties involved in the end-to-end management of smart metering in Great Britain. It comes into force under the Data Communications Company (DCC) Licence and is unique in being the only dual-fuel industry code (it applies to both gas and electricity).

The DCC, network operators and energy suppliers with domestic customers are required, by the terms of their licences, to sign up to the SEC, as is anyone else who wants to make use of the DCC's services. Becoming a SEC Party is a relatively painless process, as revealed in Chapter 9.

Though appointed, the SEC Change Board (a sub-committee appointed by the SEC Panel to manage the SEC and its Subsidiary Documents – see Chapter 2) is essentially dormant at present and doesn't get its hands on any SEC modifications until after Transition (after the DCC goes live). Until then, it's the Department of Energy and Climate Change (DECC) that's managing development of the SEC (unless urgent or fast-track SEC Modifications are raised). Similarly, Ofgem only gets to rule on SEC modifications after Transition is complete.

The SEC has had a long and protracted birth (one that's still in progress at time of writing). Given its size and complexity, it's been delivered in tranches, with each new chunk going out to industry consultation before going to the Secretary of State for designation. The first version of the SEC was designated on 23 September 2013, and the latest version at time of writing (SEC4.2) came into effect on 18 March 2015. We're probably going to have reached SEC5.0 before the DCC goes live.

The SEC is maintained on a day-to-day basis by the Smart Energy Code Administrator and Secretariat (SECAS), a role currently held by Gemserv (see Chapter 2). You can find the SEC itself at www.smartenergycodecompany.co.uk.

The SEC is a legal document and, as such, isn't the easiest of reads. Recognising this, SECAS has kindly produced a set of guidance documents that attempt to explain what the various sections of the SEC are for, and I'd recommend these as a good place to start.

Anatomy of the SEC

The SEC comprises 14 sections. Here's a quick summary of each section and who may be interested in reading it.

- **Section A: Definitions and Interpretations** (80 pages): The set of defined terms used throughout the SEC. Essentially, if a term is capitalised, it means something specific and this is the section that tells you what that is. Split into two bits, section A1 contains 570 defined terms and the much slimmer two and a bit pages of A2 tells you how to interpret certain non-defined terms in the context of the SEC (for example, 'day' means calendar day, not working day). But be warned: you won't find all defined terms in this section. Some are embedded in other sections or, indeed, SEC Subsidiary Documents. An essential reference but, like this guide, don't try to consume it in one sitting.

  When asked at the Christmas pub quiz which is the most popular letter in SEC Section A, the answer is 'S' with an impressive 105 defined terms.

- **Section B: Accessions** (7 pages): How you go about becoming a SEC Party. Essential reading for would-be SEC Parties.

- **Section C: Governance** (35 pages): The objectives of the SEC, the objectives of the DCC Charging Methodology and the governance arrangements for looking after the SEC (including the details of the SEC Panel, Sub-Committees and Code Administrator). Save for the beach.

- **Section D: Modification Process** (36 pages): How to modify the SEC, the parties involved and their roles in the process. Doesn't fully kick in until after transition, so shouldn't be at the top of your reading list.

- **Section E: Registration Data** (10 pages): What it's for, what needs to be provided and when. You can safely ignore this unless you're a Registration Data Provider (RDP – see Chapter 2).
- **Section F: Smart Metering System Requirements** (17 pages): The role of the Technical Sub Committee, how you go about getting a device on the Certified Products List (CPL – the list of devices that are allowed to connect to the DCC) and how suppliers get Communications Hubs (CHs) from the DCC. Of particular interest to device manufacturers, test houses and suppliers.
- **Section G: Security** (68 pages): System, organisation and information security obligations on the DCC and DCC Users including Anomaly Detection obligations (see Chapter 4), the need for security assurance and how you go about getting it. Essential reading for any would-be DCC User (unfortunately).
- **Section H: DCC Services** (37 pages): A description of the services provided by the DCC including the Parse and Correlate software (see Chapter 4), testing services and DCC Gateway Connections. Worth a read (you may as well find out what you're paying for), although at the time of writing it's far from complete.
- **Section I: Data Privacy** (16 pages): Obligations on the DCC and DCC Users when accessing customers' consumption data, the requirement on DCC Users with a DCC User Role of 'Other User' to undergo User Privacy Audits and how to go about getting one. Essential reading for anyone intending to collect consumption data and/or 'Other Users' (see Chapter 2).
- **Section J: Charges** (16 pages): The DCC Charges that DCC Users have to pay and how they go about paying or disputing them, how the DCC reviews, amends and forecasts them, and the obligations on DCC Users to provide credit cover. Essential reading if you're a DCC User that will incur DCC Charges (currently, Import Suppliers, Export Suppliers, Gas Suppliers and Electricity Distributors).
- **Section K: Charging Methodology** (48 pages): The methodology for deriving the Charging Statement used to determine the DCC Charges detailed in section J. To be avoided unless you like equations.

- **Section L: Smart Metering Key Infrastructure** (37 pages): Description of the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA), how you go about getting SMKI assurance, the services SMKI provides and how you interface with it, the SMKI Repository and how you interface with that, the tests you need to pass to use the SMKI, how the performance of the SMKI is measured, SMKI documents and how the SMKI recovery process is supposed to work. A rollicking good read (if you're a security analyst, that is).
- **Section M: General** (43 pages): As its name suggests, a dumping ground for miscellaneous stuff such as liabilities, force majeure, disputes and expulsions. Leave this one to the lawyers.
- **Section N: SMETS1 Meters** (17 pages): How you go about getting your SMETS1 meters adopted and enrolled in the DCC (more on adoption in Chapter 10). A must read for those suppliers who are active in the Foundation phase (and their Foundation service providers).
- **Section T: Testing During Transition** (39 pages): The Device Selection Methodology, Systems Integration Testing, Interface Testing, End-to-End Testing, SMKI and Repository Testing and Enduring Testing. A must read for test managers.
- **Section X: Transition** (34 pages): Describes the process for getting the SEC in place including which bits don't apply during the Transition phase and when they'll come into effect. Essential reading to understand whether what you've just read in the other sections applies or not in the run up to Go Live, but you can probably get away with reading the one-page SECAS guidance document.

SEC Schedules

As if the 540-odd pages that comprise the main body weren't enough, there are also six schedules to the SEC. As per the main body, here's a brief summary.

- **Schedule 1: Framework Agreement** (6 pages): The agreement that the original SEC Parties had to sign when the SEC first came into effect. Of historical interest only, unless you're one of the original SEC Parties.

- **Schedule 2: Accession Agreement** (6 pages): The form you fill in to sign up to the SEC. Essential reading for any would-be SEC Party (always read the small print).
- **Schedule 3: Specimen Bilateral Agreement** (9 pages): A template for a bi-lateral contract with the DCC. Only of relevance to those DCC Users wanting to procure a brand new DCC service (for example, support for additional smart device functionality). Unlikely to be used in the near future.
- **Schedule 4: SECCo** (25 pages): All you ever wanted to know about the SEC Company (SECCo) and more. Essential reading for those seeking a job with SECAS.
- **Schedule 5: Accession Information** (2 pages): How to go about filling in Schedule 2 (always read the instructions).
- **Schedule 6: Form of Letter of Credit** (4 pages): To be completed by those DCC Users who are obliged to provide credit cover. Not surprisingly, that's all the DCC Users that incur DCC Charges (currently Import Suppliers, Export Suppliers, Gas Suppliers and Electricity Distributors).

SEC Subsidiary Documents

Complex and voluminous though it is, the SEC and its Schedules represent just a fraction of the Smart Energy Code documentation set. The SEC also includes a set of appendices, each comprising a SEC Subsidiary Document. These designated appendices are currently lettered ('A', 'B', 'C' and so on), which may prove to have been a mistake as the current best estimate of the total number of SEC Subsidiary Documents is 44 (I assume we'll be seeing appendices 'AA', 'AB' and so on). You'll be delighted to hear that I don't intend to list them all (go to the SECAS website: `www.smartenergycodecompany.co.uk` if you're interested), but Table 7-1 attempts to group them into subject matter areas.

Interface Specifications

The largest category of SEC Subsidiary documents (comprising 11 documents) is a set of technical specifications describing interfaces used by a variety of SMIP stakeholders. The most notable of these are as follows:

- **DCC User Interface Specification (DUIS):** Defines the language used by DCC Users to communicate with the DCC.
- **GB Companion Specification (GBCS):** Defines the language understood and spoken by devices.
- **Message Mapping Catalogue (MMC):** Attempts to stitch the DUIS and GBCS together.

Table 7-1 SEC Subsidiary Documents

Document Type	*Number of SEC Subsidiary Documents*
Interface Specifications	11
Security	10
Codes of Connection	8
Communications Hubs	4
Service Management	3
Testing	3
Other	5
Total	**44**

Keeping up with the DUIS

Service Requests are defined in the DUIS, although this has changed its name during the course of the programme. It started off as the DCC User Gateway Catalogue, morphed into the DUGIS (DCC User Gateway Interface Specification), spent a brief time as the DUGIDS (DCC User Gateway Interface Design Specification) and is now living as an emaciated shadow of its former self under the alias of DUIS (DCC User Interface Specification). Confused? We all are.

The other eight interface specifications define other key DCC interfaces, including

- The interface used by Registration Data Providers (RDPs) to provide the DCC with registration data and receive updates on smart installations.
- The interfaces used by DCC Users to access the SMKI, SMKI Repository, DCC SMKI (DCCKI) and DCCKI Repository.
- The Non-Gateway Interface used by Non-Gateway Suppliers (suppliers who have yet to become DCC Users).
- The Self-Service Interface used by DCC Users.

This category also includes a yet-to-be-titled document on Service Request processing that is tipped for SEC Subsidiary Document status but probably won't emerge until section H4 of the SEC appears.

Security

SMKI, DCCKI and Infrastructure Key Infrastructure (IKI) have been responsible for spawning a flurry of SEC Subsidiary Documents. The majority of these are *Certificate Policies (CPs)*, a standard PKI document that sets out the principal parties, and their roles and duties within a Public Key Infrastructure (PKI – see Chapter 6).

There are CPs for the IKI and DCCKI and no less than three for the SMKI (SMKI, SMKI Device and SMKI Organisation). There are also a couple of *Registration Authority Policies and Procedures* (*RAPPs* – one for the SMKI one for the DCCKI) that set out the procedures by which nominated individuals can become Senior Responsible Officers (SROs) and/or Authorised Responsible Officers (AROs) – essentially, security bods authorised to do security stuff on behalf of an organisation.

This category also includes a SMKI Recovery Procedure and a more generic 'Recovery Procedures' document (neither of which are hopefully destined to become well thumbed). There's also a separate *Threshold Anomaly Detection Procedures (TADP)* document that sets out how Users can submit Anomaly Detection Thresholds to the DCC (email) and how the DCC will notify Users of threshold breaches (email and via a Service Management Service Request). See Chapter 4 for more on anomaly detection.

Codes of Connection

Eight of the SEC Subsidiary Documents are Codes of Connection that set out rules for connecting to, and use of, interfaces to the DCC. There are Codes of Connection (or 'CoCos' as they're affectionately known) for the

- DCC User Gateway
- DCC User Interface
- Registration Data Interfaces
- Self-Service Interface
- DCCKI and DCCKI Repository
- SMKI and SMKI Repository

The DCC User Gateway Network and DCC User Interface are two different beasts. The former is a connection to the DCC that you buy and secure using your DCCKI Keys, whereas the latter is the interface over which you submit Service Requests and receive Service Responses, DCC Alerts and Device Alerts. Needless to say, you access the DCC User Interface via the DCC User Gateway Network.

Communications Hubs

Four of the SEC Subsidiary Documents are related to Communications Hubs. Three of these are related to support, installation and maintenance, but the most notable among them is the *Communications Hub Technical Specification* (*CHTS* – the Communications Hub equivalent of SMETS; see Chapter 3).

Service Management

The service management-related SEC Subsidiary Documents comprise two service management policies (Incident and

Registration Data Incident) and an Error Handling Strategy. Enjoy.

Testing

The three testing-related SEC Subsidiary documents comprise the Enduring Test Approach Document, the SMKI and Repository Entry Process Testing Scenarios Document (SREPTSD) and Common Test Scenarios Document (CTSD). The latter two will be of particular interest to Test Managers.

Other

There are five SEC Subsidiary Documents that don't neatly fit into any of the preceding categories:

- A services schedule for the DCC User Gateway
- A services schedule for the DCC User Interface
- A yet-to-be-titled document on Inventory, Enrolment and Withdrawal Procedures
- A document on the Minimum Communication Services for SMETS1 Meters
- The *Smart Metering Equipment Technical Specification (SMETS)*, which sets out the minimum functional requirements for Electricity Smart Metering Equipment (ESMEs), Gas Smart Metering Equipment (GSMEs), In Home Displays (IHDs), Prepayment Interface Devices (PPMIDs) and HAN Connected Auxiliary Load Control Switches (HCALCS) (see Chapter 3)

SEC Named Documents

The next tier of documentation is a set of documents that didn't quite make it into the SEC's appendices but are, nonetheless, named within the SEC. Best current guess is that there are 23 of these. I've split them into four categories for the purposes of describing them, as summarised in Table 7-2.

Table 7-2 SEC Named Documents

Document Type	*Number of SEC Named Documents*
Security	8
Testing	4
Service Management	2
Other	9
Total	**23**

Security

Eight of the named documents are security-related. Five of these are Certificate Practice Statements (SMKI Device, SMKI Organisation, DCCKI, IKI and Test). The other three comprise:

- End-to-End Security Architecture (worth a read)
- Security Requirements Document (developed by the Security Sub-Committee and specifying the security controls considered appropriate for mitigating security risks across the end-to-end smart metering system)
- Test Certificate Policy (another Certificate Policy but this time aimed at Certificates for use in testing)

Testing

There are four testing-related named documents, all describing the approach to different testing phases (Systems Integration Testing, SMKI and Repository Testing, Interface Testing and End-to-End Testing). Another must read for Test Managers.

Service Management

Two of the named documents are service management-related and both are release management policies (one for the DCC releases and one for Panel releases).

Other

As with SEC Subsidiary documents, a hotchpotch of named documents don't easily fit into any of the previous categories. They include, in no particular order:

- Device Selection Methodology (the methodology used by the DCC to select devices to be used in SIT and IT)
- ID Allocation Procedure
- Panel Budget and Panel Information Policy
- Performance Measurement Methodology
- Privacy Controls Framework
- Technical Architecture Document
- Reported List of Service Provider Performance Measurements
- SMETS version 1.0, which sets out the functionality required of a SMETS1 meter (a meter installed in the pre-DCC Foundation phase that will be eligible for adoption by the DCC at some future date – see Chapter 10)

Guidance Documents

There may well be some more documentation in the pipeline thanks to the work of lawyers. A bunch of documents started life in SMIP Working Groups but ended up being incorporated in the SEC as SEC Subsidiary documents. In doing so, they were translated into 'legalese', which delighted the lawyers but left those people who use the documents severely put out. Most notable of the documents to suffer this fate was the DCC User Gateway Interface Design Specification (DUGIDS) which morphed into the DCC User Interface Specification (DUIS).

Industry stakeholders, not normally known for complaining, raised sufficient protest to save the DUGIDS, albeit in the demoted form of a guidance document and with no certainty that it will be maintained beyond its current version (0.8.1). DCC Users are free to make use of DUGIDS, but should there be any discrepancy between DUGIDS and DUIS, DUIS takes precedent. It's possible that more guidance documents may appear as a result of other documents having been 'SEC'ified'.

A cynic may say that the move from DUGIDS to DUIS was a victory of lawyers over technicians. They may also say that in making the move we've exchanged a fit-for-purpose technical document for legalese, and as a consequence we should be asking the lawyers responsible for this travesty to take on responsibility for developing the solution. Fortunately, as we all know, the utility industry is devoid of cynics.

Enduring Responsibility

The as-yet-unspecified number of guidance documents will probably fall to the DCC to maintain, but as shown by Figure 7-1, the bulk of the literary burden is likely to fall on the SEC Panel and its sub-committees.

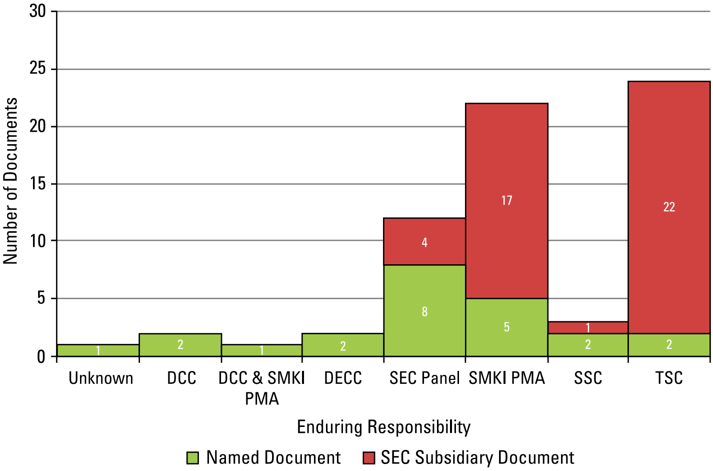


Figure 7-1: Enduring responsibility for SEC Subsidiary and Named Documents.

Chapter 8

The SMIP

In This Chapter

- Skimming over the SMIP regulatory framework
- Singling out the notable working groups
- Reviewing the various phases of the SMIP

Given the title of the book, it would be remiss not to include a chapter on the SMIP itself. It's probably the largest change programme ever undertaken in the British utility market and will almost certainly be the most publicly visible. It's already attracting close scrutiny from the Commons Energy and Climate Change Select Committee, whose support was tempered with criticism, primarily around customer engagement but also about the cost of the programme.

In this chapter, I pay a fleeting visit to the regulatory framework on which the SMIP is based, touch on some of the more notable working groups within the programme and then walk through the various phases of the programme, their objectives and participants.

Regulatory Framework

Start any section with the word 'regulatory' and you've immediately lost 95 per cent of your readership, so I'll keep the info here intentionally high level and, more importantly, brief.

The British energy sector is regulated primarily through the Electricity Act 1989 and the Gas Act 1986, which prohibit you from doing a bunch of stuff unless you hold a licence. Holding a licence often requires you to comply with another bunch of conditions specified in said licence, including compliance with a set of industry codes.

A national rollout of smart metering has required not only changes to existing licences but also the creation of a brand new licensed franchise for providing a smart metering communication service, namely *the Data Communications Company (DCC) licence*. It also requires a brand new industry code called the *Smart Energy Code* (SEC – see Chapter 7), the first industry code to apply to both the electricity and gas industries. As I explain in Chapter 7, the SEC and its vast array of SEC Subsidiary documents all need to be designated by the Secretary of State before they can come into force.

There's also the small matter of the European Commission to keep happy. The EU Technical Standards and Regulations Directive 98/34/EC says that if you intend to impose any rules or guidance that regulate products or services provided over the Internet or by other electronic means, you have to notify the European Commission of these before you can adopt them in national law. The Commission and other Member States then have three months to raise concerns if the proposed measure is considered to be a potential barrier to trade. In the case of GB smart metering, this means notifying the Smart Metering Equipment Technical Specification 1 (SMETS1), SMETS2, GB Companion Specification (GBCS) and Communications Hub Technical Specification (CHTS), all of which have now been notified and deemed to have passed muster.

Working Groups

Not surprisingly, shed loads of people are involved in the SMIP. The 51 working groups identified in the Department of Energy and Climate Change (DECC)'s 'Transition Governance Overview' represent just the tip of the iceberg. Given limitations of space and the will to live, here are a few of the more notable groups charged with making the SMIP a success.

Smart Metering Steering Group (SMSG)

This is a strategic forum charged with advising on the high level direction of the SMIP in the context of policy, implementation objectives and benefit realisation.

Appropriate to its eminent status, its attendees include the great and the good within the energy industry, including executives from

- The six largest energy suppliers
- Two of the smaller energy suppliers
- The Energy Network Association (ENA)
- Energy UK
- Consumer Futures
- The DCC
- The SEC Panel
- DECC

This is where enthusiastic and less enthusiastic stakeholders come together with their disparate political, regulatory and commercial drivers and attempt to steer the programme towards success. Oh, to be a fly on the wall. . .

Smart Metering Delivery Group (SMDG)

This is a senior operational forum focused on delivery of the SMIP. It commands attendance from a similar set of organisations as the SMSG, but at a programme director level. The group is charged with identifying and mitigating risks, resolving issues and generally driving delivery of the programme. Not surprisingly, given their criticality to the programme, metering equipment manufacturers get to attend this forum.

Technical and Business Design Group (TBDG)

Described as ‘a working level forum’, the TBDG comprises lead designers and architects charged with assisting DECC with producing the baseline technical and business design documents destined for inclusion in the SEC. For example, a Home Area Network (HAN) Strategy TBDG sub-group has been looking at the alternative HAN solutions required to support 100 per cent of British premises (more on this in Chapter 10).

Implementation Managers Forum (IMF)

Another working level forum, but this time comprising programme and implementation managers charged with monitoring progress of individual parties and resolving issues.

Others

In addition to the four preceding working groups, another 47 exist. Enough already? Well, here's just a few more:

- **Regulatory Group (RG):** Advises DECC on the smart metering regulatory framework.
- **Transitional Security Expert Group (TSEG):** an invitation-only bunch of security experts charged with ensuring security of the end-to-end solution (not to be confused with the **Testing Design and Execution Group (TDEG)**, which has been set up for the DCC to inform SEC Parties of the DCC's test programme).
- **Transitional SMKI Policy Management Authority Group (TPMAG):** A DCC-led operational group responsible for shepherding the Smart Metering Key Infrastructure (SMKI – see Chapter 6) until such times as it makes it into the SEC and its Subsidiary Documents.
- **Benefits Monitoring and Review Group (BMRG):** Tasked with keeping tabs on the performance of the SMIP and the benefits that it's delivering.

SMIP transition working groups

Only a handful of the 51 working groups cited in DECC's 'Transition Governance Overview' are enduring, the majority handing over their responsibilities to the appropriate enduring SEC Sub-Committee (SMKI PMA, SSC, TSC, Change Board or TAG – see Chapter 2) before disbanding at the end of the SMIP.

For example, having seen all the SMKI SEC Subsidiary Documents designated, the TPMAG (Transitional SMKI Policy Management Authority Group, as I'm sure you remember) will pass over governance of these to the enduring SMKI PMA SEC Sub-Committee. In practice, the SMKI PMA is likely to compromise the same individuals as the TPMAG, thus ensuring continuity. Similarly, the Transitional Security Expert Group (TSEG) is likely to morph in the Security Sub Committee (SSC) and the Technical and Business Design Group (TBDG) into the Technical Sub Committee (TSC). New business cards all round then. . . .

SMIP Phases

Figure 8-1 below sets out the various phases that go to make up the overall SMIP. I've deliberately left out dates because these have been changing and will probably continue to change. Hopefully, the dependencies between phases should stay pretty much the same (famous last words).

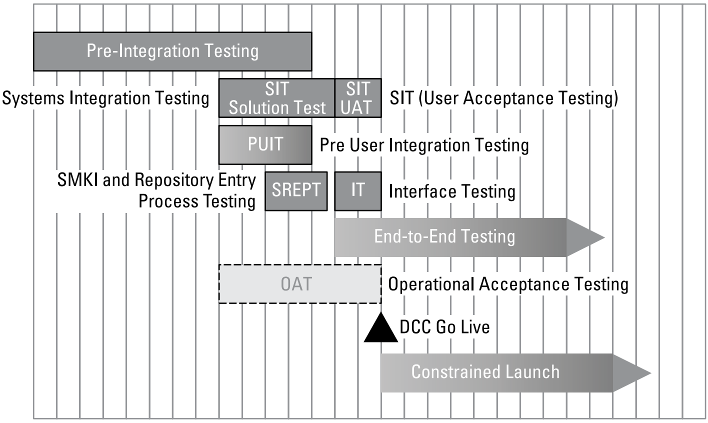

Pre-Integration Testing
Systems Integration Testing
SIT Solution Test
SIT UAT
SIT (User Acceptance Testing)
PUIT
Pre User Integration Testing
SMKI and Repository Entry Process Testing
SREPT
IT
Interface Testing
End-to-End Testing
OAT
Operational Acceptance Testing
DCC Go Live
Constrained Launch

Figure 8-1: SMIP phases.

Pre-Integration Testing

As with most things in SMIP, the programme phases are very DCC-centric. At time of writing, we're in the *Pre-Integration Testing (PIT)* phase where *Integration* refers to the assembly of the various components that go to make up the DCC service. During this phase, the DCC and its service providers, the Data Service Provider (DSP), Communication Service Providers (CSPs), Trusted Service Provider (TSP) and Parse and Correlate Provider, are all busy building, unit testing, link testing and system testing their own bits of the overall DCC solution. Each component of the solution will then undergo Factory Acceptance Testing with the DCC before being ready for inclusion within Systems Integration Testing.

Systems Integration Testing

System Integration Testing (SIT) is where the DSP, as the DCC's Systems Integrator, takes the deliverables from PIT and attempts to bolt them together into a single working solution. SIT is in two parts:

- **Solution Test:** In which the DSP tries to get everything to work.
- **User Acceptance Test:** In which the DCC looks over the DSP's shoulder to check that everything's working as it should be.

After SIT is complete, the DCC will be ready to start formal testing with SEC Parties. However, in the revised industry plan, only the Solution Test part of SIT needs to complete before formal testing with DCC Users can commence.

Devices and the DCC

Although devices aren't within their scope of delivery (other than Communications Hubs), the DCC would like to include some real devices in their testing. Indeed, section T1 of the SEC requires the DCC to use actual devices in Systems Integration Testing (SIT), Interface Testing (IT) and User Entry Process Testing (UEPT) 'to the extent that is reasonably practical'.

However, there's a problem. For device manufacturers to have some working, tested devices ready for SIT, they ideally need to have done some testing in a DCC environment. And here's the catch. The earliest DCC environment that a device manufacturer will be able to use is the End-to-End Test environment (see later in this chapter), which becomes available only when Interface Testing completes (which, itself, comes *after* SIT).

In attempt to bend the space–time continuum, the DCC has commissioned Critical Software to develop GBCS Interface Testing (*GIT) for Industry* (or *GFI* – see Chapter 3) to allow device manufacturers to generate 'gold standard' GBCS commands on a ZigBee HAN to which they can connect and test their devices.

In addition to providing GFI, the DCC is also taking a fairly relaxed view regarding the level of assurance that devices require for inclusion in SIT. They don't require ZigBee, Device Language Message Specification (DLMS) or Commercial Product Assurance (CPA) certificates, for example, although the devices do need to be 'SMETS complaint' (whatever this means in the absence of a SMETS-compliant certification). All this is defined in section T1 of the Smart Energy Code (SEC), which also states that the DCC must use a minimum of two different models of gas and electricity smart meters from manufacturers who aren't also Communications Hub manufacturers.

Clearly, there's kudos in being one of the first manufacturers to produce a device that talks to the DCC. Recognising this, the DCC has written a Device Selection Methodology to be open, transparent and impartial in its choice of devices. However, should suitable devices not be available in time, the DCC can resort to using test stubs for SIT and, possibly, also for Interface Testing (although the latter needs the blessing of the Secretary of State).

Pre-User Integration Testing

The DCC commences formal testing with SEC Parties in the *Interface Testing* phase of the programme (see the later section). However, SEC Parties may get the opportunity to do some Informal Testing with the DCC prior to this. Although not an explicit SEC requirement, the DCC has agreed to provide a *Pre-User Integration Testing (PUIT)* environment (affectionately referred to as the *Sandpit*) for SEC Parties to do some early integration testing with the DCC. The current industry plan suggests this will be available five months prior to the start of Interface Testing.

At time of writing, it's not entirely clear what the PUIT environment will support by way of testing. At the extremes, this could be support for a handful of Service Requests without cryptographic signatures, through to a full set of Service Requests operating against virtual meters that aren't only capable of signing and authenticating messages but can also remember what's been done to them (they're 'stateful').

Clearly, the latter offers the best opportunity for SEC Parties to get their systems and processes ready in parallel with the DCC's preparations but requires more effort on the part of the DCC (and, hence, more cost to the industry).

SMKI and Repository Entry Process Testing

As I explain in Chapter 6, security and, in particular, Public Key Infrastructure (PKI) is central to the SMIP. You won't get anywhere near the DCC without first being security assessed and obtaining the keys and Certificates required to connect securely. *SMKI and Repository Entry Process Testing (SREPT)* is about proving that you can successfully interface with the Smart Metering Key Infrastructure (SMKI) to submit Certificate Signing Requests (CSRs), obtain Certificates and so on (see Chapter 6). This involves completing a couple of dozen test scenarios defined in a SEC Subsidiary Document called the *SREPT Scenarios Document* (*SREPTSD* – see Chapter 7).

Interface Testing

In order to become a DCC User, you have to pass *User Entry Process Testing (UEPT)*. This testing is designed to prove that you can successfully access the DCC Services to which you're entitled according to your DCC User Role. It's a bit like passing your driving test with the DCC as your examiner.

UEPT is an enduring process because there are always likely to be new SEC Parties wanting to become DCC Users (a continuous stream of learner drivers). However, when the DCC test centre first opens its doors for business, the DCC also needs to prove that it's capable of supporting real live DCC Users. Only after two large suppliers have passed UEPT and become DCC Users is the DCC deemed to be ready to go live. So during the first couple of driving tests, both the learner and the examiner are being assessed.

The period between the first SEC Party starting UEPT and DCC Go Live (defined as occurring when two large suppliers have successfully complete their UEPT) is called the *Interface Testing* phase. To be strictly accurate, there's a little bit more multi-party testing to be done before Interface Testing is deemed to have completed successfully (for example, change of supplier testing), but it's not likely to be onerous enough to dissuade the large suppliers from wanting the kudos of being the first ever accredited DCC User.

To pass UEPT, you need to complete the test scenarios defined in the *Common Test Scenarios Document (CTSD)* appropriate to your DCC User Role(s) (the CTSD is another of those SEC Subsidiary Documents described in Chapter 7). The objective of UEPT is to

- Demonstrate that you can submit every Service Request to which you have access using a variety of valid combinations of Modes of Operation and Command Variant (see Chapter 4).
- Process the corresponding Service Responses.

There are also scenarios for receiving DCC Alerts and Device Alerts and a couple of scenarios around installing and commissioning a device which require execution of a number of Service Requests in a defined order. For an import supplier, UEPT is likely to require getting on for 300 individual tests. The good news is that these are all positive ('happy path') tests.

Because UEPT requires you to have security keys and Certificates, you need to complete SREPT before you can start UEPT.

Operational Acceptance Testing

Operational Acceptance Testing (OAT) is the final shakedown of the DCC prior to live operation. Conducted in the Production environment, it's designed to check that DCC systems and processes are ready for the onslaught of Service Requests, Alerts, device installations, DCC User queries, disasters, failovers, malicious attacks and everything else that may occur during an average day-in-the-life of the DCC.

Amongst other things, OAT will test that the DCC can install new releases, rollback installations, failover to an alternative data centre during a data centre outage and then recover to the primary data centre once the outage has been rectified, respond to DCC Users' queries and do it all within its agreed Service Levels.

OAT isn't, however, recognised as a separate test phase from a regulatory perspective. As such, the OAT results will be published as part of Interface Testing.

DCC Live!

At some point, two large suppliers will complete UEPT and the additional activities required by Interface Testing and the DCC will be declared live.

WARNING!

Don't expect too much to happen immediately. There's likely to be an extended hiatus while the newly accredited DCC Users set up their Remote Test Labs and get down to doing some real testing. Only when a supplier has a high degree of confidence in their back office systems, processes and selected set of devices are they likely to start rolling out smart meters in earnest

End-to-End Testing

After you've passed UEPT and become a DCC User, you're granted access to the DCC's End-to-End Test environment (a bit like being given the loan of your dad's car). More importantly, you're now allowed to set up a test lab and start testing your own devices. This is where the real testing begins (see Chapter 9).

WARNING!

A recent DECC consultation suggests that large suppliers will be required to have installed the lesser of 1,500 meters or 0.025 per cent of their meter estate within six months of the DCC going live. This is likely to curtail End-to-End Testing and turn the heat up significantly on suppliers' preparations for rollout.

Constrained launch

The DCC (rather optimistically, in my humble opinion) has expressed some concern that following Go Live there may be something of a rush to install SMETS2 meters, and that this may lead to some unforeseen teething problems with

DCC services. As such, they'd like the ability to apply some constraints on the initial use of the DCC. Whether these constraints are imposed and what form they make take has yet to be agreed. Whether they'll be needed is another matter.

The Pre-User Integration Test and End-to-End Test environments are enduring test environments in order to accommodate new SEC Parties wanting to become DCC Users and manufacturers/test houses wanting to test new devices. Similarly, existing DCC Users will need an environment within which they can test the inevitable changes they'll need to make to their back office systems and processes.

Chapter 9

Life as a DCC User

In This Chapter

- Becoming a DCC User
- Surviving as a DCC User

Data Communications Company (DCC) Users are Smart Energy Code (SEC) Parties that are allowed to access the live DCC environment. To reach these heady heights, a SEC Party needs to jump through a number of hoops. In this chapter, I examine these hoops and speculate on what a DCC User needs to do once in possession of the coveted User Entry Process Test (UEPT) Completion Certificate.

Becoming a DCC User

So who gets to talk to smart devices via the DCC and how do they go about doing it? Well, practically anyone can become a DCC User if they put their mind to it. All this involves is becoming a Smart Energy Code (SEC) Party, completing the processes set out in the Registration Authority Policies and Procedures (RAPP), undergoing a security assessment and, possibly, a privacy assessment, generating some Public/ Private Keys and getting some test Certificates, connecting to the DCC, passing Smart Metering Key Infrastructure (SMKI) and Repository Entry Process Testing (SREPT) to become an Authorised Subscriber, generating some live Public/ Private Keys and Certificates, ordering a DCC User Gateway connection, buying or renting a DCC Adapter, passing User Entry Process Testing (UEPT), putting some credit in place (if you're a DCC User who incurs fixed charges), integrating your back office systems and processes with the DCC, testing everything works (including your devices) and, bingo, you're ready to go. Simples.

Trivial though it may sound, there's actually more to it than meets the eye. And because (at time of writing) no one's actually been through it yet, you may anticipate a few teething problems first time around.

Becoming a SEC Party

Becoming a SEC Party is probably the least painful part of the whole process. There's a form to fill in (a copy of which you can find in Schedule 2 of the SEC) and it will cost you £450, but that's about it. You'll then be free to give your two penny's worth to any of the industry forums that you're (a) allowed to attend and (b) are lucky enough to find out about.

You won't be alone. As of 15 May 2015, there were 139 SEC Parties signed up under 91 organisations (some organisations choose to sign up as multiple SEC Parties, each SEC Party relating to a different geographic region or part of the business).

Getting security assessed

It's not entirely clear when you need to do this, but at some stage you'll need to go through a Full User Security Assessment to check compliance with system, organisational and information security as defined in sections G3 to G6 of the SEC.

This assessment is carried out by the *User Independent Security Assurance Service Provider (UISASP)*, which is a role performed by the *Competent Independent Organisation (CIO)* appointed by the SEC Panel (whose appointment is still pending at time of writing). It's not clear exactly what form this assessment is likely to take but best guess is that it will take a couple of weeks.

REMEMBER

This is an annual assessment, although if you're a small supplier (you have fewer than 250,000 customers), you only need a lighter weight verification assessment in year two and can get away with a self-assessment in year three. The same rules apply to network operators, but Other Users (OUs) can self-assess in years two and three. It's a rolling three-year cycle so, come year four, everyone's back to a full assessment.

Getting privacy assessed

If you aspire to be a DCC User with a DCC User Role of Other User (OU), you'll also need to get a full privacy assessment (other DCC User Roles are already required to do privacy assessments as part of their existing licence obligations). This is done by the *Independent Privacy Auditor (IPA)*, another hat worn by the CIO, and checks compliance according to section I2 of the SEC.

It's an annual assessment but you can self-assess in years two and three before being required to do another full privacy assessment in year four.

Getting RAPP'ed

Safe to say there's not much you can do in the SMIP without Public/Private Key Pairs and Certificates. Even Non-Gateway Suppliers (suppliers who have yet to become a DCC User) need them! This means accessing SMKI services and, as I explain in Chapter 6, you have to go through the *SMKI Registration Authority Policies and Procedures (RAPP)* with the *SMKI Registration Authority (RA)* before you can do this. This is a multi-stage process:

1. The RA needs to verify your organisation is what it claims to be, which requires your company secretary, director or chief information security officer (CISO) to fill in some forms and turn up for a face-to-face meeting.
2. When the RA's happy with the validity of your organisation, you can appoint one or more *Senior Responsible Officers (SROs)*. This requires your company secretary, director or CISO to nominate one or more individuals (more forms) and another face-to-face meeting with the RA in which they can verify that your nominated SROs are, indeed, who they say they are and are authorised to be an SRO for your organisation.
3. Once appointed, the SRO can nominate one or more *Authorised Responsible Officers (AROs)* – more forms and face-to-face meetings with the RA.

4. When you've got an ARO, you can get hold of the necessary Infrastructure Key Infrastructure (IKI) Certificates for accessing the test SMKI environments (SMKI Portal Interface, SMKI Repository, web service, batched Certificate Signing Request (CSR) web service and Secure File Transfer Protocol (SFTP) access – see Chapter 6). If you're a Non-DCC Gateway user, you get to use the internet version of the SMKI Portal Interface.

Passing SMKI and Repository Entry Process Testing

Now that you've been RAPP'ed, you can apply to go through *SMKI and Repository Entry Process Testing (SREPT)*. To do this, your SRO has to fill in an *Authorised Subscriber* application form. SREPT is about proving to the DCC that you can successfully interface with the SMKI and involves completing a couple of dozen test scenarios defined in the *SREPT Scenarios Document (SREPTSD)*. These tests are conducted using test Certificates generated in the test SMKI environment, but after you've passed SREPT, you get the IKI Certificates for accessing the live SMKI.

REMEMBER

You should probably know about two other terms. After your organisation has become an Authorised Subscriber, you can submit CSRs. When your ARO submits your first CSR, you become an *Eligible Subscriber*. Then, on receipt of your first Certificate, you become a *Subscriber* to that Certificate under the Issuing CA.

Sorting out your key strategy

Having passed SREPT, you're now allowed to request real SMKI Certificates from the live SMKI. As a minimum, you'll need one or more Organisation Certificates, and if you're an installing supplier, you'll need potentially millions of Device Certificates.

Device Certificates

Let's start with the easy one. If you're an installing supplier, your chosen device manufacturer(s) will provide you with a file containing the Public Keys of the devices that you've purchased. These will have been generated by the devices themselves while still on the production line. Your job is to submit these over the SMKI Portal and return the resulting file of Device Certificates for the manufacturer(s) to load onto the devices. Registered Supplier Agents (RSAs) are also able to do this so, if you're lucky, your Meter Asset Provider (MAP) may do this for you. Either way, you'll need to provide the meter manufacturer with the installation Organisation Certificates that you want populated in the devices' anchor slots (see Chapter 6).

Organisation Certificates

You now need to decide on your Organisation Key strategy. This could be as simple as using a single Organisation Certificate on all devices and replacing it when it expires in ten years' time. However, if the single Public/Private Key Pair corresponding to your Organisation Certificate is compromised, so is your entire meter estate. This may not be such a problem if you're a lowly network operator with limited access to Critical Service Requests, but if you're a supplier with the power to turn the lights out, this may be frowned upon by CESG (the secret bit of the Government that gets excited about these things).

REMEMBER

Given that most DCC Users will probably elect to generate and manage their Public/Private Keys within a *Hardware Security Module* (*HSM* – a physical computing device that safeguards and manages digital keys), the chances of a single key pair being compromised could be pretty remote. You're more likely to lose an HSM than you are an individual key, and DCC Users may want to consider this when formulating their key strategies.

In practice, most DCC Users will probably elect for some form of 'key chunking': that is, using a relatively small number of Organisation Public/Private Key Pairs and associated Certificates and distributing these across their device estate to limit the impact of a compromise of any single Organisation Public/Private Key Pair.

Organisation Certificates are good for ten years, so in theory the job of ARO (the nominated individual responsible for generating keys and requesting Certificates) looks fairly cushy. AROs do, however, need to be on call in the event of a key compromise, so the role's probably more like that of military personnel – long periods of boredom interspersed with short episodes of sheer terror.

REMEMBER

If you're an installing supplier, remember that in addition to your standard set of Organisation Certificates you'll need one or more *installation* Organisation Certificates (the ones initially placed in the anchor slots by your device manufacturer). There's an expectation (yet to appear in SEC) that you'll need to replace these with another set of Organisation Certificates within seven days of the device going on the wall (along with kicking the device to regenerate its own Device Public/Private Key Pairs and uploading the resulting new Device Certificates).

Connecting to the DCC

If you've aspirations to be a DCC User, you'll need to connect to the DCC, and for this you'll need a DCC Gateway Connection. These come in Low Volume (LV) and High Volume (HV) varieties and are likely to set you back between £2,000 and £15,000 for a one-off connection charge and between £600 and £32,000 for an ongoing annual charge.

TIP

The lead time for ordering LV and HV connections is 30 and 90 working days respectively, so don't forget to get your order in early.

As Chapter 6 explains, you need to secure your DCC Gateway Connection using DCCKI keys and Certificates. This means first going through the DCCKI RAPP, although hopefully the DCCKI Registration Agent (DCCKI RA) will take into account the fact that you've already been through SMKI RAPP and will give you a relatively easy ride. Indeed, you're expected to have been through SMKI RAPP before trying to access DCCKI services because you have to sign your DCCKI *Certificate Signing Request (CSR)* with your SMKI Digital Signing Key.

After you've got your DCCKI Certificates, you can use these and your DCCKI keys to secure your DCC Gateway Connection by establishing a *Transport Layer Security (TLS)* session between your *Policy Enforcement Point (PEP)* and the DCC. Acronyms aside, this essentially means that you set up a secure pipe between yourself and the DCC.

Buying, building, renting or stealing a DCC Adapter

So you're now security and privacy vetted, a bona fide IKI, SMKI and DCCKI Authorised Subscriber, and you've got a secure connection to the DCC. It's time to start sending some Service Requests. However, as I highlight in Chapter 4, submitting Service Requests and making sense of what comes back isn't trivial. You need to

- Call web services with the correct parameters depending on your chosen Service Request Variant, Mode of Operation and Command Variant.
- Follow the many steps defined in the appropriate Sequence Diagram depending on the nature of the message you're processing, who you're sending it to and your relationship with them.
- Authenticate, sign, MAC, encrypt, decrypt, parse and correlate as required.
- Follow up to 16 individual steps to complete the technical orchestration of a single Service Request/ Response, including
    - Checking and removing DSP signatures.
    - Parsing and correlating Pre-Commands.
    - Checking device signatures.
    - Parsing responses (often more than once).
    - Decrypting sensitive data.

Fortunately, these common requirements lend themselves to product-based solutions, and there are products and services on the market that address these needs, offering a simple plain text interface to the DCC. Email `enquiry.uk@cgi.com` for details.

Having a practise

As Chapter 8 describes, would-be SEC Parties are likely to get the chance to integrate with the DCC's *Pre User Integration Test (PUIT)* environment prior to attempting UEPT. The amount of time you choose to spend in PUIT is likely to depend on the functional richness of the PUIT environment. If only a handful of Service Requests are supported, the potential for testing is small and this isn't likely to take very long. If, however, a full set of Service Requests with full cryptographic support is provided, time spent testing in PUIT could verify not only integration with the DCC but could also be used to dry run your UEPT test scripts. And if the PUIT environment were to include intelligent virtual devices capable of remembering what state they're in (for example, prepayment mode and supply status) then even business process testing in PUIT becomes possible.

Passing User Entry Process Testing

As Chapter 8 describes, UEPT is primarily about demonstrating that you can successfully submit a Service Request of every type that you're entitled to according to your chosen DCC User Role(s), using a variety of combinations of Mode of Operation and Command Variant (see Chapter 4). For a supplier, this means executing nearly 300 individual tests to demonstrate compliance with the scenarios defined in the *Common Test Scenarios Document (CTSD)*. There's also a SEC requirement for would-be DCC Users to demonstrate that they can access the DCC's Self-Service Interface, though this may not amount to much more than being able to log on.

REMEMBER

UEPT needs to be completed for each DCC User Role under which you intend to operate.

The vast majority of Service Requests you're required to generate for UEPT can be issued in any order. However, there are a few that need to be done in an order specified in the SEC (mainly to do with device installation and commissioning). And remember, UEPT has to be done using devices provided by the DCC in CSP Test Labs (unless there aren't any devices ready and the Secretary of State says UEPT can be conducted using test stubs instead).

REMEMBER

SEC Parties are required to conduct UEPT using devices installed in one of the two Test Labs provided by the CSPs. Clearly, there's a limit to the number of devices that will be available in a CSP Test Lab (if, indeed, any are ready in time) and there's also a limit on the human resources available to operate them (the so-called '*smart hands*'). Access to device sets and smart hands is likely to be restricted with SEC Parties required to book time-boxed testing slots well in advance. SEC Parties also don't get to choose which CSP Test lab they'll be sent to (although they can express a preference) or the devices they get to test with (which will be selected according to the DCC's published *Device Selection Methodology – DSM;* see Chapter 7).

TIP

The CTSD specifies what needs to be tested, but it's up to the individual SEC Party to write their own UEPT test scripts. Here are some things to bear in mind when writing these scripts.

- The scripts may need to execute against real devices and the order in which you execute Service Requests should reflect this. For example, if you're going to issue a 2.2 Top Up Device, make sure that you've previously executed a 1.6 Update Payment Mode to put the meter into prepayment mode first.
- Given the limited resources within the CSP Test Labs and the long queue of SEC Parties wanting to undergo UEPT, make sure that your CTS test scripts use the *minimum* number of device sets and execute in the *shortest* possible time.
- Group any manual intervention required into one segment of testing to make the most efficient use of the CSP's smart hands.

Passing Interface Testing

If you're lucky enough (?) to be one of the first two large suppliers to go through UEPT, you'll need to complete some additional Interface Testing. This will involve co-ordination with the DCC and another large supplier to execute joint test scenarios predominantly focusing on the change of supplier process.

Assuming this all goes swimmingly, congratulations! You're now a DCC User!

Surviving as a DCC User

Now that you're a bona fide DCC User, you can access the DCC's End-to-End test environment and start some real testing.

Smartening up your business processes

Until now, all the testing has been aimed at demonstrating the ability to rattle off a set of Service Requests of each type available to the DCC User Role in question. For the most part, the DCC doesn't care in what order these are generated or how a SEC Party goes about generating them (manually typing commands into a screen and pressing a button is fine). However, given the volume of smart meters, DCC Users will need fully integrated, automated processes if they're to maximise the benefits of smart metering.

For DCC Users who don't currently have much access to domestic metering (for example, network operators), integration with the DCC represents an opportunity to create new ways of working. However, for those DCC Users for whom domestic metering is an integral part of their existing business processes (for example, suppliers), integration with the DCC represents substantial change to a host of existing business processes (and the systems that support them) while still retaining support for traditional meters.

TIP

Experience says that an average supplier will need between 40 and 50 smart-enabled business processes to function effectively in the smart retail market. These range from the relatively simple (pre-notifying the DCC of devices to be installed) to the extremely complex (installing and commissioning a device set). Putting these business processes in place involves modifying existing back office interfaces to plug into the 115 Service Requests, 40 DCC Alerts and 91 Device Alerts now available via the DCC.

Take a change of tenancy, for example. How a supplier goes about managing a change of tenancy is up to them, but they may well choose to

- Take a closing/opening reading
- Restrict access to historic consumption data so that the new tenant can't see what his or her predecessor consumed
- Delete schedules agreed with the previous tenant and cancel any outstanding future dated commands (or, at least, check that the DCC's done this)
- Change to a default tariff, possibly including a change of payment mode and the setting up of a new billing calendar
- Disable the previous tenant's PIN
- Send a message to welcome the new tenant

This requires designing, building and testing a new business process involving calls to ten or more Service Request types, all of which could fail and require exception handling.

Similarly, given that meters could appear on a network operator's network at rates of 5,000 or more a day, it's highly likely that network operators may choose to automate the configuration of smart meters, possibly triggering configuration at time of installation. What this configuration involves is up to the individual network operator and how interesting they think the meter is likely to be in the context of their overall network, but may include:

- Reading the DCC Inventory (to find out a bit more about the device that's been installed)
- Changing the network operator's Organisation Certificates
- Reading what, if any, load limits have been set by the supplier
- Setting voltage thresholds
- Configuring maximum demand registers
- Configuring the alert behaviour of the meter

- Setting up schedules to collect one or more of reactive import profiles, export profiles, network data, maximum demand import/export registers, load limit data, active power import and daily consumption logs

This requires designing, building and testing a new event-triggered business process involving calls to a dozen or more Service Requests types.

Hopefully, these new processes will have all been designed, built and internally tested by the time you've become a DCC User. But now that you're a DCC User, you have the opportunity of testing these processes with the DCC in the End-to-End Test environment (it's highly unlikely that the PUIT environment will be functionally rich enough to support this complexity of testing).

Given the scale and complexity of the task of integrating with the DCC, End-to-End testing isn't likely to be quick. The number and complexity of test scripts required to adequately test your back office systems and processes is likely to be an order of magnitude more complex than those used in UEPT, not least because UEPT test scenarios are all 'happy path' (positive tests) whereas much of the real testing will be around failures and exception handling.

Setting up your own test lab

Now you're a DCC User, you're considered grown up enough to have your own test lab (a room where you can install your own devices and talk to them via the DCC's End-to-End Test environment). Regardless of where you choose to locate this, you can buy Smart Metering Wide Area Network (SM WAN) connectivity from the DCC, which means you can test using Communications Hubs from both CSPs within the same test lab (the DCC will also flog you the required test Communications Hubs).

Section H14.32 of the SEC allows non-SEC Parties (like testing houses) to connect to a DCC test environment in order to test device interoperability. It's becoming clearer what a SEC Party needs to do to be able to connect to the DCC, but it's less clear what hoops a non-Party will need to jump through (although assuming it will be similar to those of a SEC Party is probably a pretty good starting point).

Setting up a test lab is fine if you happen to be a supplier who intends to buy and install vast numbers of devices, but may not be such an attractive proposition if you're a DCC User who doesn't intend to install any meters. Worse still, if you're not an import supplier, your DCC User Role prevents you from accessing the Service Requests necessary to install and commission devices. Fortunately, the DCC has realised this and has said that they will provide a complete set of DCC User Roles for testing purposes on request.

TIP

A supplier has a SEC obligation to only operate Smart Metering Equipment Technical Specification 2 (SMETS2)-compliant meters via the DCC. However, SMETS2 functionality extends beyond that available to a supplier. Take network functionality, for example. Installing suppliers can't set maximum demand registers or read network data but are responsible for ensuring that this all works. Hence there's a need for suppliers (or their nominated test houses) to have access to a complete set of test DCC User Roles to allow full functional testing of the device.

Setting up test labs isn't cheap and is something that non-import suppliers would probably like to avoid if at all possible. Of course, there's always the option of using the CSP Test Labs, but demand for these is likely to be at a premium. It may be possible to do a deal with a friendly supplier to use devices installed in their test lab or, alternatively, rent some meter time from a test house.

Outsourcing device testing

In addition to commissioning new/modified business processes, suppliers are also obliged to ensure that the devices they intend to install and operate are adequately tested. For some types of testing (see Chapter 3), they'll be able to rely on the device manufacturer to provide the necessary test certificates to prove compliance (for example Measuring Instruments Directive (MID) 2004/22/EC seals, ZigBee, Device Language Message Specification (DLMS) and Commercial Product Assurance (CPA) certificates). Assuming the Smart Meter Device Assurance (SMDA) operator is up and running, this reliance could extend to SMDA certificates for Interoperability and Interchangeability. However, that still leaves SMETS2 compliance and accelerated life testing.

Suppliers have enough on their plate testing their back office processes and systems without having to worry about device testing (which, based on Foundation experience, is time consuming). And however much testing you undertake on the devices you intend to install, you also need to consider the meters that you'll invariably gain through change of supply (you're also responsible for ensuring that these are SMETS-compliant). And don't forget that it's your responsibility to make sure that *all* SMETS2 functionality works (including that which you can't access as a supplier).

TIP

Consider outsourcing as much device testing as you can to established, accredited test houses and focus your testing efforts on your business processes.

REMEMBER

Before you install your first smart meter, make sure you're fully confident in the DCC, your back office systems and processes (including exception handling), your chosen devices and the ability of your systems and processes to scale (especially if the number of devices they will have to cope with is not within your control, as is the case with network operators).

WARNING!

Don't forget to test Disaster Recovery. Recovery will be easier/safer to test at low volumes rather than when the rollout's in full swing.

Making use of the SSI

The DCC provides a *Self Service Interface (SSI)*, a web-based portal accessed via the DCC User Gateway that's intended as your first port of call when contacting the DCC. You probably only had to log on to it to pass UEPT, but now it's time to start using it in earnest. It's predominantly read-only, although you can raise and track service management incidents and, if you're an installing supplier, gain access to the CSP's websites for ordering Communications Hubs.

The SSI provides

- Details of SM WAN coverage by postcode
- Information on what variant of Communications Hub you should install at a given premise
- DCC service status

- Answers to frequently asked questions
- The ability to run parameterised reports against DCC data
- The ability to query a property in the DCC Smart Inventory using MPAN/MPRN, device GUID, postcode, property filter or UPRN and find out what smart devices are installed there

If you're a supplier, don't forget to forecast and order your Communications Hubs. Forecasting and ordering is done via the CSPs, but you can access their order management systems via the SSI.

Paying your dues

If you're a supplier or a network operator, you have to pay monthly fixed charges per meter and per Communications Hub to finance the DCC. Costs are split between Import Suppliers, Export Suppliers, Gas Suppliers and Electricity Distributors (Gas Transporters, Registered Supplier Agents and Other Users get off scot free).

The DCC is currently costing a little over £3.5 million per month, with Import Suppliers picking up the majority of this (57 per cent); Gas Suppliers a fair whack (35 per cent) and Electricity Distributors picking up the rest (8 per cent). The DCC monthly spend is forecast to rise to an estimated £14 million per month in 2017/18.

Section K7.5 (j) of the SEC allows the DCC to impose a charge for every message handled. In the DCC's indicative charging statement 2015/2016, the DCC has decided not to impose this charge based on the fact that it's likely to be very small and would probably cost more to bill than would be recovered. Instead, the DCC intends to bundle this in with the fixed charges per meter/Communications Hub. Good news for budding Other Users!

Given the initial lack of explicit charges for messages, why not put the devices through their paces and read everything that's available to you? Having a full set of smart data will help you assess its worth to your organisation and shape your enduring smart operations.

Chapter 10

The Future

In This Chapter

- Adopting Foundation meters
- Extending HANs
- Centralising registration
- Electing for Elective Communication Services
- Settling half-hourly
- Coping with mobile mayhem
- Preparing for change

At time of writing, the SMIP is just starting to gear up. Milestones are looming, implementation plans compressing and the monumental event of the first Data Communications Company (DCC)-supported meter being deployed in an unsuspecting customer's home seems a long way away. So considering what comes after the smart metering rollout seems a bit like discussing space exploration post the Mars landings. However, here goes.

Foundation Adoption

Suppliers have a licence obligation to provide all domestic customers and small businesses with a smart meter by 2020, but not just any old smart meter. For a smart meter to count towards a supplier's smart meter quota and thus be spared replacement, it must either be a Smart Metering Equipment Technical Specification 2 (SMETS2) meter installed under the DCC or a SMETS1 meter.

Truth be told, a SMETS1 meter isn't that dissimilar from a SMETS2 meter in terms of its functionality; however, instead of the new hybrid cryptographic end-to-end security model (see Chapter 6), SMETS1 meters tend to use a more traditional symmetric cryptographic security model.

Some suppliers have chosen to deploy smart meters in the period prior to DCC Go Live (referred to as the *Foundation* phase, which, according to the Department of Energy and Climate Change's (DECC's) website, officially started in March 2011). In the absence of a DCC, suppliers must either manage their own smart metering infrastructure or outsource provision of this to a third party.

However, it has always been the government's intention that at some time in the future SMETS1 meters will be eligible for adoption and enrolment into the DCC. In this context, *adoption* means that the DCC will take on the communications contract from the Wide Area Network (WAN) provider (the Foundation equivalent of the Communication Service Provider – CSP) and *enrolment* means that it will include the meter within its vast smart metering estate, enabling all parties to interface with it via the DCC User Interface.

Why should a supplier choose to give away their beloved SMETS1 meter for adoption? Well, the adoption costs will be smeared across all DCC Users and the costs of operating a SMETS1 meter via the DCC are likely to be substantially less than those of operating the meter yourself or via a small service provider. It also removes the burden of being obliged to continue to operate the meter after its fickle customer has decided to desert you for another supplier (an obligation that came into force via condition 25B of the Electricity Supplier Licence and Gas Supplier Licence).

On 24 March 2015, DECC directed the DCC to start work on the *Initial Enrolment Project Feasibility Report* (*IEPFR* – yes, yet another linguistically challenging acronym). This is an impact assessment conducted by the Data Service Provider (DSP) to determine the cost of supporting Foundation meters (bearing in mind that their symmetric key-based security model means that they need to be kept at arm's length from their SMETS2 cousins).

By the time you read this, the DCC should have wheeled its cart around the industry, crying 'Bring out your SMETS1 meters!', so that the impact assessment can be based on the largest possible population of meters and thus realise the maximum economies of scale. However, the IEPFR isn't likely to be submitted to the Secretary of State until the latter part of 2016 and is itself only the first step on the road to adoption, so it may be sometime before SMETS1 meters make it into the DCC.

Dual Band Communications Hub

Suppliers are likely to be paying very close attention to the DCC's Self Service Interface (SSI) before dispatching their meter operators to install smart meters. The SSI is the mechanism by which the DCC will meet its obligation to provide SM WAN coverage information by postcode. In the case of the Central and Southern CSP Regions, the SSI will also tell you what variant of Communications Hub (CH) to install (cellular, mesh or cellular/mesh).

The contractual requirements that have been placed on Arqiva and Telefónica in terms of SM WAN coverage have been redacted in the versions of the contracts published on the DCC's website. However, DECC previously stated that they expected the CSPs to commit to eventual coverage of at least 97.5 per cent of properties.

Having SM WAN coverage doesn't necessarily mean you'll be able to install a smart meter, though. You also need to be able to establish a Home Area Network (HAN). DECC-funded research suggests that the 2.4 GHz HAN specified in SMETS2 and CHTS is expected to work in only 70 per cent of premises. For the other nine million odd homes, the distance between smart devices and/or the thickness of the walls is likely to defeat a 2.4GHz HAN.

The solution (or, at least, part of it) is to use an alternative 868MHz HAN that, operating at a lower frequency, has better penetration. The same DECC-funded research suggests that adding the 868MHz solution will enable HANs to be established in 95 per cent of premises. However, the bandwidth available at this spectrum is more limited than that available at 2.4GHz. Therefore, the 868MHz solution should only be used when it's really needed. For this reason, the DCC's been charged with providing a dual band CH in addition to its existing 2.4GHz variant. The new dual band CH should be capable of communicating with devices on the HAN at either frequency – using 2.4GHz for devices where this is possible and 868MHz where it isn't.

At time of writing, DECC is still consulting on the dual band CH, and the earliest you can expect to see one is, apparently, the second half of 2017. And the old adage 'never trust timescales expressed in seasons or quarters' suggests you should treat even this date with caution.

WARNING!

Although the DCC's Self Service Interface will tell you whether a property is likely to have SM WAN coverage, it won't tell you whether it's likely to support a 2.4GHz HAN. It's up to suppliers to source information concerning housing stock and to take this into account when planning their rollout strategies.

An Alternative HAN Solution

The mathematically astute amongst you will have noticed that even with an 868MHz HAN solution, 5 per cent of premises (around 1.5 million) will still remain beyond the reach of the DCC. Many of these premises will be *Multiple Dwelling Units (MDUs)*, communal residences such as blocks of flats where meters may be co-located some way from the living areas. These premises are likely to require additional kit shared by all residents.

However, given customer switching, it's extremely unlikely that all residents will be served by the same supplier, so it's not obvious who should pay for this communal paraphernalia. A recent government consultation is minded to force suppliers to work together to provide a collective solution to this problem but, as with the dual band CH, it's early days and this could take a while.

Centralised Registration

As with the adoption of SMETS1 meters, the government has always intended for the DCC to appoint a centralised registration agent. *Registration agents* perform the essential role of remembering who your supplier is (okay, they do a bit more than this but that's the gist of it). Currently, this honour falls to the 19 distribution network operators (DNOs) and independent distribution network operators (iDNOs) for your electricity supply, and Xoserve for your gas supply.

Not surprisingly, registration agents are at the heart of the change of supply process, the epic ordeal that customers need to undertake when seeking to reduce their energy bills. Currently, separate switching processes exist for gas and electricity dating back to the 1990s and these can take up to eight weeks to complete.

Ofgem, protector of the energy consumer, would like us all to change our supplier as often as possible in order to inject some much needed competition into the retail market. They see fast, reliable switching as the catalyst for this to happen.

The SMIP offers key building blocks for making this a reality:

- A joint gas/electricity code (namely, the Smart Energy Code – SEC) within which a new dual-fuel switching process can be defined
- A central body for managing and operating a centralised registration service (namely, the DCC)

Ofgem estimate the cost of establishing next day switching as a one-off £4.21 per dual fuel customer with a £0.27 per year ongoing charge. Given that many customers could save in the order of £200 per year by switching supplier, this seems a small price to pay.

Centralised registration offers the prospect of a 'golden property record' – a single definitive view of a property that brings together the gas supply point *(Meter Point Reference Number – MPRN)* and electricity supply point *(Meter Point Administration Number – MPAN)* into a single record indexed by *Unique Property Reference Number (UPRN)*. In the future, this record could be enriched with additional information (for example, a water supply reference number).

Elective Communication Services

The SEC has provision for a DCC User to enter into a bi-lateral agreement with the DCC for the provision of an *Elective Communication Service* (essentially, an extension to the DCC User Interface solely for use by that DCC User). Such an agreement could be used to access additional bespoke device functionality above and beyond that defined in SMETS.

Say a supplier comes up with a killer product that offers customers online access to their energy consumption, disaggregated to individual appliances (‘Did you know that your son’s X-Box costs £5.79 per week to run?’). Having commissioned an enhanced SMETS2 meter to log the one minute consumption data required to do this, the supplier could enter into a bi-lateral agreement with the DCC to provide a new Service Request for pulling back the resultant log files.

Given everything else that’s going on, it may take a while for Elective Communication Services to take off, but a pro forma for the bi-lateral agreement is ready and waiting in Schedule 3 of the SEC.

REMEMBER

Elective Communication Services can only relate to the supply or use of energy, and you’re not allowed to add any meter functionality that’s deemed Critical (see Chapter 4).

Other Services

The DCC is a commercial organisation and is at liberty to seek new opportunities for extending its footprint by leveraging its national communications network. The example that’s frequently cited is offering communication services to smart water meters, but ‘other services’ could equally apply to central registration services to enable water competition. That said, any change would probably require consent from the Secretary of State and, possibly, primary legislation.

Half Hourly Settlement

Retail electricity demand in this country is currently split pretty evenly between

- **Half hourly (HH) customers:** Those with demands in excess of 100kW whose consumption must be measured every half hour for settlement purposes.
- **Non-half hourly (NHH) customers:** Those with demands of less than 100kW whose meagre consumption doesn't warrant half hourly measurement.

HH customers account for a daily consumption of around 400,000 MWh all year round, whereas NHH customers account for a daily consumption of between 400,000 MWh to 600,000 MWh depending on the time of year. However, although their consumption is similar, their numbers aren't. There are around 115,000 HH customers compared to 29 million NHH customers.

NHH customers vary in size from tiny domestic dwellings up to small factories. The largest 164,000 NHH customers, although only 0.5 per cent of NHH customers by number, account for 10 per cent of the total NHH consumption. It's now mandatory for these customers (Profile Classes 5 to 8) to be half-hourly metered, and there's also a plan to move them into HH settlement (Balancing and Settlement Code (BSC) Modification P272 – see the nearby sidebar). In 2011, ELEXON, who run electricity settlements in Britain, had a look at whether there was a business case for moving the remaining 28,836,000 NHH customers into half hourly settlement after they'd been given smart meters. At the time, ELEXON concluded that it was 'intuitively the right thing to do' but couldn't establish a business case for doing so. Were this to change, the DCC could be a key enabler in the demise of NHH settlement.

The long road to HH settlement

P272 has been long in gestation and it's been a far from straightforward birth. First raised in May 2011, it underwent an industry impact assessment and two working group consultations before being recommended for rejection. Ofgem wasn't convinced and asked for P272 to be re-assessed. There followed a cost–benefit analysis and two further consultations, but still the working group recommended rejection. However, Ofgem reprieved P272, albeit delaying its implementation until a related industry code change had gone through. Two further delays were approved, and at time of writing the BSC Panel is proposing a third delay that will result in P272 being implemented on 1 April 2017, almost six years after it was first raised.

Mobile Workforce Mayhem

While the DCC Go Live date gradually slips to the right, the 2020 target for everyone to have smart meters hasn't moved. As the time available for rollout compresses, the number of meter operators required to achieve the 2020 deadline proportionally increases (a bit like Boyle's Law). And this becomes a recurring problem because most of the devices will reach the end of their lives and require replacing at the same time (so don't forget to invest in meter operation businesses in 2031!).

Things are looking up for meter operators, at least for the next five years, but I can't say the same for meter readers, who are destined for extinction over the same period.

SEC Changes

Whenever a new industry code comes into effect, there follows an inevitable flurry of change requests as unforeseen problems arise and the signatories struggle to make the code fit for purpose. Take the Balancing and Settlement Code, for example. As Figure 10-1 shows, almost half of the 320 BSC Modifications that have been raised during its fifteen year history were raised in the first three years. And there's no reason to believe that the same won't be true of the SEC. So, if you work for the Smart Energy Code Administrator and Secretariat (SECAS), don't plan any sabbaticals for the next few years. . . .

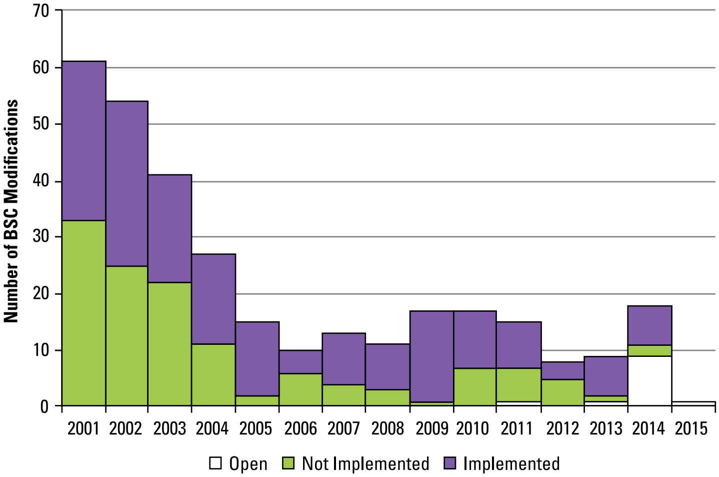


Figure 10-1: Balancing and Settlement Code Modifications.

Chapter 11

Ten Top SMIP Tips

In This Chapter

- Suggestions on strategy
- Tips on testing
- Ideas on implementation
- Opinions on operation

Where to start? Here are ten semi-serious observations on the SMIP to take away with you.

Don't Go for a Supplier-Led Rollout

This has to be the most complex smart meter rollout ever attempted. Any country considering a smart meter rollout should take note and get the distribution network operators to do it.

Get Through User Entry Process Testing (UEPT) as Quickly as You Can

Real testing of your back office systems and processes can only start when you have unfettered access to your own smart devices installed in your own test environment. Unfortunately, this requires you to have passed UEPT and become a Data Communications Company (DCC) User.

Tighten Up Your UEPT Scripts

Given the limited device sets and smart hands available in CSP Test Labs, combined with the likely high demand for UEPT testing slots, make sure your UEPT test scripts use the minimum number of devices and complete in the shortest possible time. Oh, and make sure they'll run against real devices as well as dumb test stubs (in the unlikely event that there are real devices available for UEPT).

Don't Hold Your Breath

Don't expect to see many smart meters appearing on customers' walls immediately after the DCC goes live. DCC Go Live happens when two large suppliers become DCC Users. However, you can only start the *real* testing after you've become a DCC User with access to the End-to-End Test environment, and this is likely to take some time.

Fill Your Boots

The DCC has decided not to levy explicit charges on messages, at least initially, so why not make the most of it? So, if you're a Distribution Network Operator (DNO), for example, you may as well collect as much data as you can to see whether it's of any use.

Take Control

When your business processes require Service Requests to be performed in a specific order, consider orchestrating these in your back office rather than relying on DCC sequencing. You'll have more control when handling exceptions.

Why Wait When You Can Have It Now?

In the absence of explicit charges for messages, Scheduled Service Requests and On Demand Service Requests (with Service Levels of 30 seconds and 24 hours, respectively) cost the same. In addition to having to wait for a Scheduled Service Response, you'll also have no control over when the response arrives, so you'll have to size your systems for the worst case of everything arriving at the same time. Using On Demand Service Requests gives you greater control (and saves you hanging about!).

Beware Hand Held Terminals (HHTs)

Delivering pre-generated Service Requests via an HHT rather than over the Smart Metering Wide Area Network (SM WAN) is fraught with challenges. Such Service Requests are device-specific. This means you've either got to pre-allocate device sets to specific customers or rely on remotely accessing back office systems from your HHT to enable locally delivered commands to be generated at time of installation. Pre-allocation causes problems if one of the devices proves faulty, and if your HHT's got remote connectivity, chances are SM WAN coverage exists.

Keep the Lawyers Away

While clearly relishing the challenge of deciphering technical documentation written in legalese, developers responsible for implementing the SMIP would probably say they have enough challenges already.

Outsource Your Device Testing

As a supplier, you'll have enough on your plate testing your back office processes and systems. Outsource as much of the device testing as you can by finding a reputable, established test house.

Glossary

ACB (Access Control Broker): A DSP function when the DSP communicates with a device as a Known Remote Party. ACB Certificates may also be used as placeholders in anchor slots where the correct Organisation Certificate is not known or unavailable. (See page 94.)

Adoption: The process by which the communication contract for an enrolled Foundation meter is transferred to the DCC. (See page 143.)

ALCS (Auxiliary Load Control Switch): An integral bit of an ESME that switches auxiliary load circuits. (See page 29.)

Anchor slot: A holder for an Organisation Certificate within a device. (See page 93.)

Anomaly Detection: A service provided by the DCC to detect anomalously large volumes of messages. (See page 62.)

ARO (Authorised Responsible Officer): A nominated, vetted individual authorised to access the SMKI to request and revoke Certificates on behalf of an organisation. (See page 127.)

Asymmetric cryptography: Cryptography in which encryption and decryption are performed using different keys. (See page 84.)

Authentication: Checking that a message is from the party that claims to have sent it. (See page 83.)

Authorised Subscriber: An individual, organisation or device that has gone through the RAPP and is permitted to request Certificates from an RA. (See page 128.)

BMRG (Benefits Monitoring and Review Group): A work group set up to keep tabs on performance of the SMIP and the benefits it's delivering. (See page 116.)

CA (Certificate Authority): A trusted entity that issues Certificates. (See page 87.)

CAD (Customer Access Device): A Type 2 Device that can access the same data set as an IHD and provide a bridge between the regulated SM HAN and the non-regulated Customer HAN (or C HAN). (See page 33.)

Certificate: An electronic document used to prove ownership of a Public Key. Comprises the Public Key itself and details of the authenticating Issuing Certificate Authority (CA). Also known as Public Credentials. (See page 88.)

Certification: The process by which a device gains evidence of compliance with a specific assurance scheme (for example, ZigBee certification). (See page 26.)

CESG (The National Technical Authority for Information Assurance): The bit of GCHQ that ultimately gets to rule on security-related SMIP issues. (See page 37.)

CH (Communications Hub): A CSP-provided device that connects the HAN to the SM WAN and also includes a GPF. (See page 27.)

CHF (Communications Hub Function): Everything in the Communications Hub that isn't the GPF. (See page 27.)

CHTS (Communications Hub Technical Specification): A document that sets out the minimum physical, functional, interface and data requirements that apply to a Communications Hub (the Communications Hub equivalent of SMETS). (See page 27.)

CIO (Competent Independent Organisation): An agent appointed by the SECCo on behalf of the SEC Panel to provide the UISASP and IPA functions. (See page 22.)

CoCo (Code of Connection): A SEC Subsidiary Document setting out the rules for connecting to and using a DCC interface. (See page 107.)

Contingency Key: A DCC Public/Private Key Pair, the Public Key of which is embedded in encrypted form within the Root OCA Certificate. Used by the DCC in the event of a major security compromise. (See page 97.)

CP (Certificate Policy): A standard PKI document that sets out the principal parties, their roles and duties within a PKI. (See page 109.)

CPA (Commercial Product Assurance): A CESG scheme for evaluating commercial products against published security and development standards. (See page 36.)

CRA (Command Response Alert) Flag: A flag (either ‘C’, ‘R’ or ‘A’) that’s included in a Message ID. (See page 58.)

Critical Service Request: A Service Request that has the potential to affect supply, result in financial fraud or the compromise of the security of a smart device. (See page 46.)

CRL (Certificate Revocation List): A list of revoked Certificates sent out periodically to Subscribers by the Issuing CA. (See page 89.)

CRR (Certificate Revocation Request): A request sent by a Subscriber to a Registration Authority (RA) to revoke a Certificate and place it on a CRL. (See page 88.)

CSR (Certificate Signing Request): A request sent by a Subscriber to a Registration Authority (RA) for a Certificate to prove ownership of a Public Key. (See page 88.)

CTS (Common Test Scenarios): A set of tests that a SEC Party needs to complete as part of User Entry Process Testing (UEPT) before becoming a DCC User. (See page 121.)

CTSD (Common Test Scenarios Document): A SEC Subsidiary Document containing the tests that comprise User Entry Process Testing (UEPT). (See page 121.)

CV (Command Variant): An input parameter to a Service Request that tells the DSP how it should be delivered. (See page 52.)

CSP (Communication Service Provider): An agent of the DCC responsible for providing the SM WAN and CHs over which the DCC Data Systems communicate with smart devices. Currently Arqiva (northern CSP region) and Telefónica (central and southern CSP regions). (See page 13.)

DCC (Data Communications Company): The DCC licence holder responsible for establishing and managing the smart metering communications infrastructure – currently Smart DCC Ltd (DCC), a subsidiary of Capita plc. (See page 12.)

DCC Alert: An alert generated by the DCC in DUIS format. (See page 71.)

DCC Data Systems: The central IT system provided by the Data Service Provider (DSP) though which DCC Users communicate with smart devices. (See page 8.)

DCCKI (DCC Key Infrastructure): A PKI used to secure interfaces to the DCC. (See page 91.)

DCCKI Repository: A database containing the DCCKI Certificates issued by the DCCKI Issuing CAs. (See page 91.)

DCC Only Service Request: A Service Request sent to the DCC only (as opposed to one destined for a device). A.k.a. non-Device Service Request. (See page 44.)

DCC User: A SEC Party that's passed User Entry Process Testing (UEPT). (See page 14.)

DCC User Gateway Network: The WAN connecting the DSP to the DCC Users. (See page 8.)

DCC User Role: A category of DCC User that dictates the DCC services to which the DCC User has access. (See page 15.)

DSP (Data Service Provider): An agent of the DCC responsible for the DCC Data Systems (currently CGI). (See page 13.)

DECC (Department of Energy and Climate Change): The government department responsible for instigating the smart meter rollout. (See page 20.)

Device Alert: An alert generated by a device in GBCS format. (See page 75.)

Device Certificate: The Certificate relating to a Device Public/ Private Key Pair, issued by the Issuing DCA. (See page 89.)

Device Log: A log maintained by a device that contains the Public Keys of other devices with which it communicates over the HAN. (See page 31.)

Digital Signature: An asymmetrically encrypted message hash added to the message for the purpose of authentication and integrity checking. (See page 84.)

Digital Signing Public/Private Key Pair: An asymmetric key pair used for signing messages. (See page 87.)

DLMS/COSEM (Device Language Message Specification/ Companion Specification for Energy Metering): One of the two industry application layer protocols to be used for British smart meters. (See page 56.)

DNO (Distribution Network Operator): A company licensed to distribute electricity in Great Britain. (See page 14.)

DUGIDS (DCC User Gateway Interface Design Specification): A technical document describing the DCC User Interface, now relegated to a guidance document. (See page 110.)

DUIS (DCC User Interface Specification): A SEC Subsidiary Document based on the DUGIDS (but without the useful bits). (See page 105.)

ED (Electricity Distributor): A DCC User Role for a Distribution Network Operator (DNO). Also known as ENO (Electricity Network Operator). (See page 16.)

EES (Electricity Export Supplier): A DCC User Role for the supplier to whom you sell your surplus electricity generation (also known as ES – Export Supplier). (See page 15.)

EIS (Electricity Import Supplier): A DCC User Role for the supplier from whom you buy your electricity (also known as IS – Import Supplier). (See page 15.)

Encryption: Encoding a message such that only authorised parties can read it. (See page 83.)

End-to-End Testing: A SMIP test phase in which DCC Users can test their systems, processes and devices in an enduring DCC test environment using remote test labs. (See page 122.)

ENO (Electricity Network Operator): A DCC User Role for a Distribution Network Operator (DNO). Also known as ED (Electricity Distributor). (See page 16.)

ES (Export Supplier): A DCC User Role for the supplier to whom you sell your surplus electricity generation (also known as EES – Electricity Export Supplier). (See page 15.)

ESME (Electricity Smart Metering Equipment): Another name for an electricity smart meter. (See page 29.)

Enrolment: The process by which a certified meter is included within the DCC's service. (See page 142.)

Foundation: Relating to the period before the DCC goes live and to smart meters installed during this period. (See page 142.)

Future Dated (Device): A Mode of Operation in which a Service Request is sent to a device for execution at a later date/time. (See page 50.)

Future Dated (DSP): A Mode of Operation in which a Service Request is sent to the DSP for instigation at a later date/time. (See page 50.)

GBCS (GB Companion Specification): A SEC Subsidiary Document that describes the HAN interfaces of the ESME, GSME, CH, HCALCS, IHD and PPMID. (See page 105.)

GBZ (DLMS): A weird combination of ZSE and DLMS/COSEM specific to the GB SMIP. (See page 56.)

GFI (GIT for Industry): A HAN-based tool, based on GIT, for device manufacturers to test their device's compliancy to GBCS in the absence of the DCC. (See page 36.)

GIT (GBCS Interface Testing): A tool developed by Critical Software for the DCC to electronically validate the GBCS. (See page 36.)

GNO (Gas Network Operator): A DCC User Role for a company licensed to distribute gas in Great Britain. Also known as GT – Gas Transporter. (See page 17.)

GPF (Gas Proxy Function): An integral part of the Communications Hub that handles commands to and from the GSME when it's asleep. (See page 30.)

GIS (Gas Import Supplier): A DCC User Role for the supplier from whom you buy your gas. A.k.a. GS – Gas Supplier. (See page 15.)

GS (Gas Supplier): A DCC User Role for the supplier from whom you buy your gas. A.k.a. GIS – Gas Import Supplier. (See page 15.)

GSME (Gas Smart Metering Equipment): Another name for a gas smart meter. (See page 30.)

GT (Gas Transporter): A DCC User Role for a company licensed to distribute gas in Great Britain. Also known as GNO – Gas Network Operator. (See page 17.)

GUID (Globally Unique Identifier): A 64 bit number that conforms to the IEEE EUI-64 standard. (See page 57.)

HAN (Home Area Network): The ZigBee SEP 1.2 network over which smart devices communicate in the home. (See page 7.)

HAN-Ready Protocol: Another term for GBCS. (See page 55.)

HCALCS (HAN Connected Auxiliary Load Control Switch): An ALCS that's grown up, left the ESME and has set up for itself on the HAN. (See page 30.)

HHT (Hand Held Terminal): A device for communicating with Communications Hubs other than via the SM WAN or HAN. (See page 34.)

IEPFR (Initial Enrolment Project Feasibility Report): An impact assessment conducted by the DSP to determine the cost of adopting SMETS1 meters into the DCC. (See page 142.)

IHD (In Home Display): A Type 2 Device for displaying consumption and usage data to consumers. (See page 33.)

IKI (Infrastructure Key Infrastructure): A PKI used to secure interfaces to the SMKI. (See page 91.)

IMF (Implementation Managers Forum): A working level forum charged with monitoring progress of individual parties and resolving issues. (See page 116.)

Integrity check: A check to ensure a message hasn't been tampered with in transit. (See page 83.)

IPA (Independent Privacy Auditor): A function of the CIO that conducts privacy assessments. (See page 23.)

IS (Import Supplier): A DCC User Role for the supplier from whom you buy your electricity (also known as EIS (Electricity Import Supplier). (See page 15.)

Issuing CA (Issuing Certificate Authority): A trusted third party that issues Certificates that prove ownership of Public Keys. (See page 88.)

Issuing DCA (Issuing Device Certificate Authority): The Issuing CA for SMKI Device Certificates. (See page 89.)

Issuing OCA (Issuing Organisation Certificate Authority): The Issuing CA for SMKI Organisation Certificates. (See page 89.)

IT (Interface Testing): A SMIP testing phase in which the DCC solution is tested with SEC Parties. (See page 120.)

Key Agreement Public/Private Key Pair: An asymmetric key pair used for generating shared secrets. (See page 87.)

Key Ceremony: A quorate group of nominated industry Key Custodians who get together in the event of a security incident that requires the DCC to use either the Recovery Key or Contingency Key. (See page 95.)

Key Custodian: A nominated individual charged with protecting the security of the smart metering infrastructure. (See page 95.)

KRP (Known Remote Party): A DCC User who is 'known' to a device by virtue of having its Organisation Certificate in one of the device's anchor slots. (See page 94.)

MAC (Message Authentication Code): A symmetrically encrypted message hash added to the message for the purpose of authentication and integrity checking. (See page 83.)

MAM (Meter Asset Manager): An agent appointed by a gas supplier to install and maintain gas meters. (See page 18.)

MAP (Meter Asset Provider): The owner of a device to whom the registered supplier pays rents. (See page 18.)

Mode of Operation: The way in which a DCC User would like a message to be delivered. (See page 49.)

MOP (Meter Operator): An agent appointed by an electricity supplier to install and maintain electricity meters. (See page 18.)

MPAN (Meter Point Administration Number): A number used to uniquely identify electricity supply points in Great Britain. (See page 145.)

MPRN (Meter Point Registration Number): A number used to uniquely identify gas supply points in Great Britain. (See page 145.)

MPRS (Meter Point Registration System): A system used by DNOs and iDNOs to manage registration data. (See page 14.)

MDU (Multi Dwelling Unit): Essentially, a block of flats. (See page 144.)

Named Document: A document referenced in the SEC but not included as a SEC appendix. (See page 108.)

NAN (Neighbourhood Area Network): An RF mesh network provided by some Telefónica CHs to communicate back to the CSP when direct communication over the cellular WAN network isn't possible. (See page 28.)

Non-Critical Service Request: A Service Request that can't result in loss of power, financial fraud or a security breach (see Critical Service Request). (See page 46.)

Non-Device Service Request: A Service Request sent to the DCC only (as opposed to one destined for a device). A.k.a. DCC Only Service Request. (See page 44.)

Non-Gateway Supplier: A supplier who has yet to become a DCC User. (See page 19.)

OAT (Operational Assurance Testing): A SMIP test phase in which the DCC tests the non-functional aspects of the DCC overall system to ensure that it's fit for operation. (See page 121.)

Organisation Certificate: The Certificate relating to a SMKI Organisation Public/Private Key Pair, issued by the Issuing Organisational CA. (See page 89.)

Originator Counter: A counter maintained by the sender of an unsolicited message that's included within the message's Message ID. (See page 57.)

OTA (ZigBee Over The Air): A ZigBee dialect used for firmware updates. (See page 56.)

OU (Other User): A DCC User Role for a DCC User that's not a supplier, network operator or Registered Supplier Agent (RSA). (See page 18.)

P&C (Parse and Correlate): An application provided to DCC Users by the DCC free of charge to parse GBCS into DUIS and correlate Pre-Commands with their corresponding Critical Service Requests. (See page 48.)

P&C Provider: An agent of the DCC responsible for delivering the P&C application. Currently Critical Software. (See page 14.)

PAN (Personal Area Network): A lower level communications mechanism to enable close proximity communication between HHTs and CHs during installation. (See page 34.)

PEP (Policy Enforcement Point): A logical entity that enforces a DCC User's policies for accessing its systems. It forms the DCC User's end of the TLS session that secures the connection between the DCC User and the DCC. (See page 91.)

PIT (Pre Integration Testing): A SMIP phase in which the DCC and its service providers test their individual components of the overall DCC solution. (See page 117.)

PPMID (Prepayment Interface Device): A Type 1 Device used to display prepayment-related information to customers and for local entry of UTRNs. (See page 32.)

Pre-Command: A Critical Service Request that's been transformed into GBCS. (See page 47.)

Private Key: A key, comprising two very large prime numbers, used in asymmetric cryptography. (See page 84.)

Public Key: A key, comprising the product of the two very large prime numbers that make up the corresponding Private Key, used in asymmetric cryptography. (See page 84.)

Public/Private Key Pair: A pair of keys used in asymmetric cryptography, one comprising two very large prime numbers (the Private Key) and the other comprising the product of these two very large prime numbers (the Public Key). (See page 87.)

PUIT (Pre User Integration Testing): An informal SMIP testing phase in which SEC Parties get an opportunity to test with a DCC environment prior to the start of formal Interface Testing. A.k.a the Sandpit. (See page 119.)

RA (Registration Authority): A PKI role responsible for verifying the identity of an individual, organisation or device and carrying out administration functions on behalf of a Certificate Authority. (See page 88.)

RDP (Registration Data Provider): Network operators charged under licence obligation with providing registration data to the DCC (Xoserve for gas registration data, the Distribution Network Operators (DNOs) and independent DNOs (iDNOs) for electricity registration data). (See page 14.)

Recovery Key: A DCC Public/Private Key Pair, the Certificate of which resides on every device. Used by the DCC to recover Organisation Certificates. (See page 96.)

RG (Regulatory Group): A work group that advises DECC on the smart metering regulatory framework. (See page 116.)

Root CA (Root Certificate Authority): A trusted third party who can authenticate one or more Issuing CAs. (See page 88.)

Root OCA Key: A DCC Public/Private Key Pair, the Certificate of which is on every device and contains an encrypted Contingency Key. (See page 97.)

RSA (Registered Supplier Agent): A DCC User Role for either the Meter Operator (MOP) appointed for an MPAN, the Meter Asset Manager (MAM) appointed for an MPRN or the Meter Asset Provider (MAP) for either. A.k.a SNA – Supplier Nominated Agent. (See page 18.)

Scheduled (Device): A Mode of Operation in which a device executes a command on a recurring basis. (See page 51.)

Scheduled (DSP): A Mode of Operation in which the DSP sends a Service Request to a device on a recurring basis. (See page 51.)

SEC (Smart Energy Code): A new dual fuel industry code governing the relationship between the DCC and DCC Users. (See page 99.)

SECAS (SEC Administrator and Secretariat): An agent appointed by SECCo on behalf of the SEC Panel to provide day-to-day management of the SEC. Currently Gemserv. (See page 22.)

SECCo (Smart Energy Code Company): A corporate vehicle for the SEC Panel to use when contracting services with third parties. (See page 22.)

SEC Change Board: A SEC Sub Committee charged with assessing modifications to the SEC. (See page 21.)

SEC Panel: An elected industry body charged with managing the SEC. (See page 21.)

SEC Party: A signatory to the SEC. (See page 23.)

SEC Subsidiary Document: A document under SEC Panel governance that forms an appendix to the SEC. (See page 104.)

Sensitive: Applied to Service Responses and/or Device Alerts that contain consumer information deemed to be of a personal nature (for example, consumption data). (See page 47.)

Sequence Diagrams: A set of pictorial representations of the steps that need to be performed to send messages of different types over the DCC User Interface. Found in the DUGIDS. (See page 60.)

Sequencing: A service offered by the DCC for controlling the order of execution of Service Requests. (See page 55.)

Service Request: A command issued by a DCC User to a device or the DCC. (See page 45.)

Service Request Variant: A child of a Service Request, created to provide a one-to-one mapping with a GBCS command. (See page 46.)

Service Response: A response to a Service Request, generated by either the DCC (for DCC Only Service Requests) or the receiving device. (See page 45.)

Signed Pre-Command: A Pre-Command that a DCC User has signed using their Private Digital Signing Key. (See page 47.)

SIT (Systems Integration Testing): A SMIP testing phase in which the DSP, acting as the DCC's System Integrator, integrates and tests the various components of the overall DCC solution. (See page 118.)

Smart Energy GB: A not-for-profit organisation charged with raising public awareness and demand for smart meters. (See page 24.)

SMDA (Smart Metering Device Assurance): A scheme operator tasked with establishing an independent assurance scheme covering interoperability and interchangeability device testing. Currently Gemserv. (See page 41.)

SMDG (Smart Metering Deliver Group): A senior operational work group focused on delivery of the SMIP. (See page 115.)

SMSG (Smart Metering Steering Group): A strategic forum charged with advising on the high level direction of the SMIP in the context of policy, objectives and benefit realisation. (See page 114.)

SM WAN (Smart Metering Wide Area Network): The network that connects the Home Area Networks (HANs) to the Data Service Provider (DSP). (See page 8.)

SMETS (Smart Metering Equipment Technical Specification): A standard that sets out what ESMEs, ALCSs, GSMEs, IHDs, PPMIDs and HCALCSs must do to become certified. (See page 26.)

SMIP (Smart Metering Implementation Programme): Government-instigated programme to roll out out smart electricity and gas meters to domestic customers and small businesses by 2020. (See the rest of the book.)

SMKI (Smart Metering Key Infrastructure): A PKI used for authenticating DCC Users and devices. (See page 89.)

SMKI Portal: A SMKI GUI accessed via the DCC User Gateway Network. (See page 91.)

SMKI Portal (Internet): A SMKI GUI accessed via the Internet. (See page 91.)

SMKI PMA (SMKI Policy Management Authority): A SEC Sub-Committee responsible for the governance of the SMKI Document Set. (See page 21.)

SMKI Repository: A database containing the SMKI and IKI Certificates issued by the SMKI and IKI Issuing CAs. (See page 91.)

SNA (Supplier Nominated Agent): A DCC User Role for either the Meter Operator (MOP) appointed for an MPAN, the Meter Asset Manager (MAM) appointed for an MPRN or the Meter Asset Provider (MAP) for either. A.k.a RSA – Registered Supplier Agent. (See page 18.)

SREPT (SMKI and Repository Entry Process Testing): The testing phase that a SEC Party must pass in order to gain access to the live SMKI service. (See page 120.)

SREPTSD (SMKI and Repository Entry Process Test Scenarios Document): A SEC Subsidiary Document containing the test scenarios that a SEC Party must execute in order to pass SREPT. (See page 120.)

SRO (Senior Responsible Officer): A nominated, vetted individual authorised to nominate AROs and submit applications to become an Authorised Subscriber. (See page 127.)

SSC (Security Sub-Committee): A SEC Sub-Committee responsible for developing and maintaining security documents. (See page 22.)

Subscriber: Someone possessing a Certificate proving ownership of a Public Key. (See page 88.)

Supply Sensitive Check: The check you need to do before sending a Supply Sensitive Service Request. (See page 47.)

Supply Sensitive Service Request: A Critical Service Request that can affect the supply of gas or electricity at a property. (See page 46.)

Symmetric cryptography: Cryptography in which encryption and decryption are performed using the same key. (See page 83.)

TBDG (Technical and Business Design Group): A working level forum assisting DECC with the production of baseline technical and business documents for inclusion in the SEC. (See page 115.)

TDEG (Testing Design and Execution Group): A working group set up to inform SEC Parties of the DCC's testing programme. (See page 116.)

TLS (Transport Layer Security): A protocol that ensures privacy between communicating applications. (See page 91.)

TPMAG (Transitional SMKI Policy Management Authority Group): A DCC-led operational group responsible for shepherding SMKI until it's incorporated into the SEC and its Subsidiary Documents. (See page 116.)

Transform: A Mode of Operation for translating Critical Service Requests (in DUIS format) into Pre-Commands (in GBCS format). (See page 51.)

TSC (Technical Sub-Committee): A SEC Sub-Committee responsible for providing support and advice on technical specifications. (See page 21.)

TSEG (Transitional Security Expert Group): An invitation-only bunch of security experts charged with ensuring the security of the end-to-end solution. (See page 116.)

TSP (Trusted Service Provider): An agent of the DCC responsible for providing the Smart Metering Key Infrastructure (SMKI) and Infrastructure Key Infrastructure (IKI). Currently BT. (See page 13.)

Type 1 Device: A smart device that has a Device Log for storing Certificates relating to other devices on the HAN and, as such, is able to execute or issue HAN commands (currently either a PPMID or HCALCS). (See page 32.)

Type 2 Device: A smart device that doesn't have a Device Log and, as such, is restricted to 'read only' functions on the HAN (currently either an IHD or a CAD). (See page 32.)

UEPT (User Entry Process Testing): The testing phase that a SEC Party must pass to become a DCC User. (See page 120.)

UISASP (User Independent Security Assurance Service Provider): A function of the CIO that conducts security assessments. (See page 22.)

UPRN (Unique Property Reference Number): A unique identifier for every addressable location in Great Britain, created by Local Authorities (see page 145).

URP (Unknown Remote Party): A DCC User who is 'unknown' to a device by virtue of the fact that its Organisation Certificate is absent from the device's anchor slots. (See page 94.)

UTRN (Unique Transaction Reference Number): A 20 digit number used to add credit to an ESME or GSME operating in prepayment mode. (See page 59.)

X.509: An international standard for implementing PKIs. (See page 56.)

ZCL (ZigBee Cluster Library): A generic part of the ZigBee protocol used in smart metering. (See page 56.)

ZigBee SEP v1.2 (ZigBee Smart Energy Protocol v1.2): The application layer protocol used over the HAN. (See page 56.)

ZSE (ZigBee Smart Energy): Another term for ZigBee SEP. (See page 56.)

Author's Acknowledgements

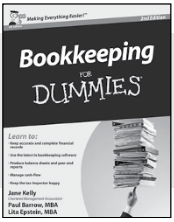
I'd like to thank everyone who contributed to this book, particularly: Richard Ascough, David Barber, Stefania Bortolotti, Oliver Bridges, Beth Brown, Chris Dann, Paul French, David Leck, Richard Lush, Tara McGeehan, Raj Nag, Ricardo Wissmann-Alves and all at Wiley. And Symon Brown for the MeerCAD joke.

FOR DUMMIES®

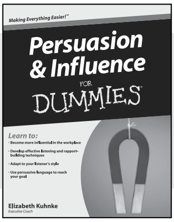
Making Everything Easier!™

UK editions

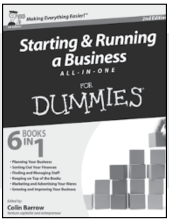
BUSINESS



978-0-470-97626-5



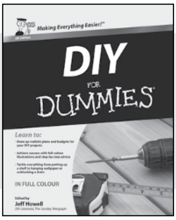
978-0-470-74737-7



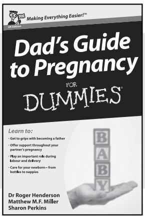
978-1-119-97527-4

REFERENCE

978-0-470-68637-9

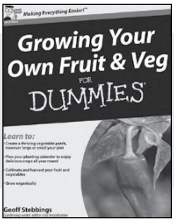


978-0-470-97450-6

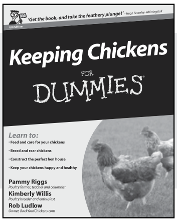


978-1-119-97660-8

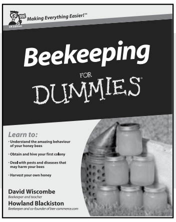
HOBBIES



978-0-470-69960-7



978-1-119-99417-6



978-1-119-97250-1

Asperger's Syndrome For Dummies
978-0-470-66087-4

Basic Maths For Dummies
978-1-119-97452-9

Body Language For Dummies, 2nd Edition
978-1-119-95351-7

Boosting Self-Esteem For Dummies
978-0-470-74193-1

British Sign Language For Dummies
978-0-470-69477-0

Cricket For Dummies
978-0-470-03454-5

Diabetes For Dummies, 3rd Edition
978-0-470-97711-8

Electronics For Dummies
978-0-470-68178-7

English Grammar For Dummies
978-0-470-05752-0

Flirting For Dummies
978-0-470-74259-4

IBS For Dummies
978-0-470-51737-6

Improving Your Relationship For Dummies
978-0-470-68472-6

ITIL For Dummies
978-1-119-95013-4

Management For Dummies, 2nd Edition
978-0-470-97769-9

Neuro-linguistic Programming For Dummies, 2nd Edition
978-0-470-66543-5

Nutrition For Dummies, 2nd Edition
978-0-470-97276-2

Organic Gardening For Dummies
978-1-119-97706-3

Available wherever books are sold. For more information or to order direct go to
www.wiley.com or call +44 (0) 1243 843291

11–37870

CGI's highly successful *For Dummies* series with Wiley includes the following titles:

GB Water Industry For Dummies

GB Electricity Industry For Dummies

Implementing Enterprise Asset Management For Dummies

New Nuclear For Dummies

Smart Grids For Dummies

Smart Metering For Dummies

Coming soon! ***GB Gas Industry For Dummies***

To download or request a copy of any of the *For Dummies* series, visit **www.cgi-group.co.uk/the-dummies-series** or **email enquiry.uk@cgi.com.**

The Smart Metering Implementation Programme (SMIP) explained!

Smart Metering Implementation Programme For Dummies is your essential pocket guide to this government-driven initiative that will see 53 million gas and electricity smart meters installed in over 30 million premises across Great Britain by 2020.

This book makes a ludicrous but entertaining attempt to summarise the key features of the programme, including the stakeholders, devices, infrastructure, documentation and the fiendishly complicated security model that underpins the largest GB retail utility change programme to date.

- ***Take an overview of the SMIP* — understand what SMIP is for, who the key players are, how the end-to-end solution will work and how it's being tested to ensure that it does**
- ***Learn more than you ever wanted to know about messages* — get to grips with different types of message, what they're for, how they're sent/received and the security model that keeps them safe and secure**
- ***Become a DCC User* — understand the hoops to jump through and how to negotiate them**

Open the book and find:

- Who's who in the SMIP
- The difference between an HCALCS and an ALCS
- The industry documentation that's worth reading
- How to become a DCC User
- Life after DCC Go Live
- The definitive jargon busting glossary

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Chris Beard is one of CGI's leading Subject Matter Experts in energy markets. Author of *Smart Metering For Dummies*, *Smart Grids For Dummies* and *GB Electricity Industry For Dummies*, Chris has spent the last 20 years working across all parts of the energy industry, helping companies to adapt and thrive within de-regulated markets.

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-12229-6
Not for resale

WILEY END USER LICENSE AGREEMENT