DCC Connection Guidance

Guidance to assist SEC Parties understand the connections and connection types that are required to connect to the DCC Service

Author: Operations
Version: 1.0
Date: 19/01/2015

Document Control

Revision History

Revision Number	Revision Date	Summary of Changes	Name
0.1	15/01/15	Initial Version	DCC Operations
1.0	19/01/15	Issued	DCC Operations

Approvals

Name	Title / Responsibility	Release Date	Version
Dave Broady	Operations Director	19/01/2015	V1.0

Distribution

Name	Title & Organisation	Release Date	Version
All SEC Parties			
All RDPs			

Related Documents

Document	Version	Author	Date
Request for DCC Gateway Connection	V1.0	A Bradford	19/01/2015
Connection Request Quotation	V1.0	A Bradford	19/01/2015

Contents

1 Introduction

DCC Service Users require connections to the DCC Gateway to enable them to connect to the DCC Services as defined in the Smart Energy Code (SEC).

This document aims to provide guidance to DCC Service Users to help them understand:

- why connections are required?
- what options are available?
- the process to order, install and configure the different connections.

It also aims to predict the questions that Parties may have and provides guidance in these areas.

1.1 Governance

The ordering of DCC Gateway Connections is provisioned for by:

• SEC 4a Section H15	– designated 14 January 2015
• SEC section H	– switched on 26 January 2015
• SEC section E3	– already switched on
• DCC Gateway Connection Code of Connection	– designated 26 January 2015.

1.2 Commencement of Live Service

The live service for the ordering DCC Gateway Connections commences on 26 January 2015.

1.3 DCC Connection Ordering Service Delivery

The live ordering service will be managed by the DCC Operations department and supported by the DCC Service Desk.

Service Desk contact details are: 0844 225 4445 and servicedesk@smartdcc.co.uk.

The Connection installations will be managed by the DCC's Data Service Provider (CGI) using their appointed DCC Gateway Connection Provider – Gamma.

Installation of physical circuits will be arranged by Gamma with telecom providers including BT Openreach and Virgin Media.

The DCC Connection Request forms and Operations Manual are available on the Smart DCC website (http://www.smartdcc.co.uk/).

A separate Connection Request form should be completed for each connection required, even if the connections are into the same data centre.

Once completed, the Connection Request Forms can be emailed through to service desk for processing. Alternatively they can be uploaded to a secure area on the DCC's SharePoint. This can be organised via the Service Desk.

2 About DCC Connections

2.1 Why DCC connections are required

2.1.1 SEC Parties

- A DCC Gateway Connection is required by any SEC Party that wishes to connect to live DCC Services for:
  - access to the DCC User Interface Specification as per DCC User Interface Specification (DUIS) and
  - access to the Self-Service Interface (SSI) as per the Self-Service Interface Specification.
- SEC Parties will also need a connection to test with DCC Services (including Sandpit, User Entry Process Testing, Interface Testing and End-to-End Testing) when these testing services are available.
- SEC Parties may need more than one connection for resilience and to support their business continuity and disaster recovery plans.

2.1.2 Registration Data Providers

A DCC Gateway Connection is required by each Registration Data Provider (RDP) to facilitate the initial load of registration data to the DCC, the daily transfer of Registration Data changes to DCC and the DCC status flow back to the RDPs.

2.2 Who can apply for a Connection

Any organisation that is a SEC Party can apply for a DCC Connection (SEC section H15).

RDPs can also apply for their own connection (SEC section E3). However, if as a group, a number of RDPs appoint a shared service provider, then this provider must become a SEC Party in order to operate as the DCC Gateway Party on behalf of the RDPs.

The connection request must be submitted to the DCC by one of the registered nominated contacts for their Party.

The Party (or RDP) that applies for the DCC Gateway Connection is referred to as the **DCC Gateway Party.**

2.3 Sharing of Connections

DCC Connections can be shared for cost and/or operating efficiencies, by multiple SEC Parties or RDPs.

Examples of this may be where:

- A retail business and network operator are in a similar location or use the same data centre and wish to share a single connection
- An organisation holds multiple legal entities (or SEC Parties) that are supported by the same data centres

- A service provider operates DCC Services on behalf of one of more small suppliers
- A Network Operator may wish to share a connection with its RDP
- A group of RDPs appoint an RDP service provider to manage the transfer of RDP data to and from the DCC.

In all of these cases, there will be a DCC Gateway Party who orders, installs and operates the gateway connection on behalf of the other Parties. The Connection will terminate in the DCC Gateway Party's requested data centre and it is the DCC Gateway Party that will be billed for the connection and annual rental charges.

This DCC Gateway Party will then be responsible for the appropriately secured communications from their data centre to the Parties they are operating on behalf of. They are responsible for security and resilience between themselves and the other Parties.

This DCC Gateway Party must be a SEC Party in its own right.

2.4 Number of Connections required

It is up to each SEC Party to determine how many connections it requires and the resilience that is required for its business.

A single connection to the DCC Gateway could, for the most part provide access to both the DUIS and SSI. A single connection can also be used for both testing and live operations.

However, a single circuit would be a single point of failure and if the line were unavailable for a period of time, then no access to the DCC Services would be possible until the line became available again, and this may significantly affect the SEC Party's business operations.

Considerations that affect the number of connections are provided in the following sub-sections:

2.4.1 Resilience

There are three primary choices for connecting to the DCC Gateway which are:

Low Resilience -	One data centre, one connection
Medium Resilience -	One data centre, two connections
High Resilience -	Two data centres, two connections,

2.4.2 Business Continuity and Disaster Recovery

It is likely that each SEC Party/Gateway Party will require a second connection that will operate as a back-up and will automatically come in to operation in a disaster situation. Whether this back-up connection is the same capacity as the primary circuit, or not will depend on how each SEC Party balances the continued access to the DCC against the cost of full resilience.

2.4.3 Split between SSI and Service Requests

Large Service Users may wish to separate their online access to SSI from the DUIS service requests and as such may choose to have two connections, one for each. Both lines could then operate as a back-up for each other.

2.4.4 Separation of Testing and Live Operation

Some Service Users may wish to have a low volume connection for testing followed by a larger connection for live operation, and to keep the two connections separate.

2.5 Contractual Period for Connections

When ordering a connection, the SEC Party must specify the minimum contract period required. This can be either 1 year or 3 years.

Please note that this is the minimum period of connection, and that the contract will automatically be renewed by the DCC if not cancelled.

However, the DCC will contact the DCC Gateway Party four months before the end of the initial contract period, advising the annual charge that will apply for renewal. The Party then has one month to cancel the connection without incurring further charges.

RDPs are not required to specify the contract period.

2.6 Types of Connection Available

There are two levels of connection available:

Type	Description	Capacity
High Volume Connection	A 100Mb Ethernet connection which could be rated to a lower capacity (in 10Mb increments)	10Mbps – 100Mbps
Low Volume Connection	A superfast broadband connection where this is available at the Party's Data Centre. If it is not available, then a standard broadband connection will be provided.	Superfast: Up to 40Mbps download / 10Mbps upload Standard: Up to 20Mbps download / 2.5Mbps upload

There is no monthly usage allowance on the DCC Gateway Connections. Connections are limited/restricted on a per second basis (i.e. mega bits per second (Mbps)).

The DCC Gateway Low Volume (LV) Connection is typically a business Superfast Broadband link (where available) providing up to a 10Mbps upload (to the DCC) and up to a 40Mbps download (from the DCC).

Where Superfast broadband is not available at a specification location then standard broadband will be investigated although these will be a lower bandwidths. The expected bandwidth will be provided to the Gateway Party following the Site Survey.

The DCC Gateway LV Connection may not be available at all locations in which case the DCC Gateway Party will have to procure a DCC Gateway High Volume (HV) Connection.

The DCC Gateway HV Connection is a 100Mbps Ethernet link (Fibre to the Cabinet). It is possible to procure a DCC Gateway HV Connection (100Mb) but restrict it to a lower capacity for a lower cost (e.g. 10Mb). Increments (and decrements) of 10Mb are possible upto 100Mb. Changes to the configuration installed have a 30 day lead time.

It is not envisaged that a connection higher than 100Mb will be required for the foreseeable future. Larger connections are not currently permitted under SEC.

2.7 Upgrading Connections.

2.7.1 Low Volume

Low volume connections cannot subsequently be upgraded to high volume. However if superfast broadband becomes available, then the connection can be upgraded to use it.

If a Gateway Party needs to move to a high volume connection, then they will need to apply for a new HV connection. They may then choose to cancel the LV connection, although the penalty will equate to the remaining charges under the original order, so they may choose to have both connections for the minimum connection period of the LV connection.

2.7.2 High Volume

When an HV connection is installed, its initial rating is likely to be 10 or 20 Mbps.

If more bandwidth is required, High Volume connections can usually be upgraded (up to a maximum 100Mbps rated at 100Mbps) but this will attract an additional charge.

This will however be able to be achieved within weeks, rather than the initial installation timescales.

2.8 Bandwidth required

It is up to each Gateway Party to determine the bandwidth that it requires. There are a number of factors that need to be considered:

- The number of Parties for whom the connection will be used
- The forecast volumes of the Parties who will be using the connection
- The meter rollout profile of the Parties for whom the Gateway Party is providing a connection, including an allowance for portfolio growth
- The frequency, timing and volume of service requests that Parties intend to submit (based on the forecasts submitted to Finance)
- The complexity of requests such as tariff changes, which will vary significantly in size depending on the complexity of tariffs applied
- Whether testing and live will use the same connection at the same time.

The DCC can assist with the calculation of individual message sizes, and this should be requested via the Service Desk.

Once DCC Connections are operational, the Gateway Party will be able to request a connection performance report that will show the bandwidth utilisation. This will assist Parties with identifying the capacity required and the point at which an upgrade may be desirable.

2.9 Charges for DCC Connections

2.9.1 SEC Parties

Each connection ordered will have an associated installation cost and an annual charge. If a new telephone line has been installed there will also be a charge for this. These charges will be itemised on the Connection quote provided to the DCC Gateway Party and which the authorised person from the DCC Gateway Party will have approved.

The installation charge and the first year's rental will become due on completion of Connection installation. Annual charges will then become due annually (in advance) thereafter.

Where multiple SEC Parties share a DCC Connection, the Connections charges will be collected by DCC from the DCC Gateway Party via the DCC Billing process and will be itemised as 'Explicit Charges'. It is then the responsibility of the DCC Gateway Party to determine how these should be split between users of their connection.

Other costs that may be charged are those that relate to a failed site visit. If the DCC arrives at the data centre to carry out the installation, but is not granted access for any reason, then the rescheduled site visit will be charged.

2.9.2 RDPs

The DCC will provide a low-volume connection to DCC Services for each RDP, free of charge, provided that the connection is used purely for the provision of registration data to the DCC. If the connection is shared with the Network Operator SEC Party data, then the connection will be chargeable.

Failed site visits will also be applicable to RDP connections.

2.9.3 Ballpark Costs

As per the DCC Charging Statement, the indicative charges for DCC Gateway Connections are set out below; these indicative prices based on a sample 'spread' of locations. The exact cost of a selected option will be made available on application (pursuant to Sections H15.8 and H15.9(b) of the SEC):

Service	Indicative connection charge (£, excluding VAT)	Indicative annual charge (£, excluding VAT)
DCC Gateway HV Connection **(Up to 100Mbps (which can be utilised in increments of 10Mbps)**	3,000 – 15,000	4,000 – 32,000
DCC Gateway LV Connection (Up to 40Mbps)	2,000 – 4,000	600 – 1,000

Note: the large variance in costs is due to the potential civil works that may be required in some cases. Gateway Parties will be made aware of the specific costs that relate to them as part of the Connection quotation, before any works commence.

2.10 Cancellation of Connections

Whilst a DCC Gateway Party is entitled to cancel their connection at any point after installation, this will attract a penalty equivalent to the full balance of the costs as per the original order.

Therefore SEC Parties should consider carefully the length of time for which they will need the connection when placing their order(s).

2.11 Authority to Proceed

Once a quotation has been received by the DCC Gateway Party, there is a 30 calendar day window for acceptance of the quote.

The DCC requires that the person who gives authorisation to proceed, actually has the authority to do so. The quote provided should be printed, signed by the authorised individual and then scanned and emailed to Service Desk.

As part of our contact verification process, the DCC will check that the person who accepts the quote has been set up as a nominated contact for DCC Connection authorisation.

To minimise delays, each DCC Gateway Party should ensure that these nominated contacts are set up as soon as possible.

2.12 The Installation Process

DCC Connection installation is a three stage process:

1. installation of circuit by telecom provider (e.g. BT Openreach, Virgin Media)
2. installation of network equipment (by Gamma as the DSP’s appointed agent
3. configuration of the connection and establishing of the sessions (by the DSP).

The first two of these stages will require a physical site visit, but the third stage will be carried out remotely.

2.13 Installation Paperwork

Once the Connection Order has actually been placed, it will be necessary to arrange access to the DCC Gateway Party’s data centre.

Each DCC Gateway Party will have their own paperwork requirements for access to their data centres.

It is important that these are identified before installation or physical site surveys are required, to prevent aborted visits and delays.

Requirements may include:

- Some data centres require documentation to be raised within their own organisation before access can be granted.
- Others require Risk Assessment Method Statements (RAMS) to be provided.

Standard RAMS are available from Gamma and the telecom providers, but custom documents will be chargeable.

2.14 Diverse Routing Requirements

If a Gateway Party is ordering more than one Connection, it may require that these take different or diverse routes to minimise the risk of a single point of failure.

If this is the case, then the Gateway Party should make their requirements clear on the forms for both connections. This should be done by allocating a Gateway Party reference to each form and quoting the related cross-references.

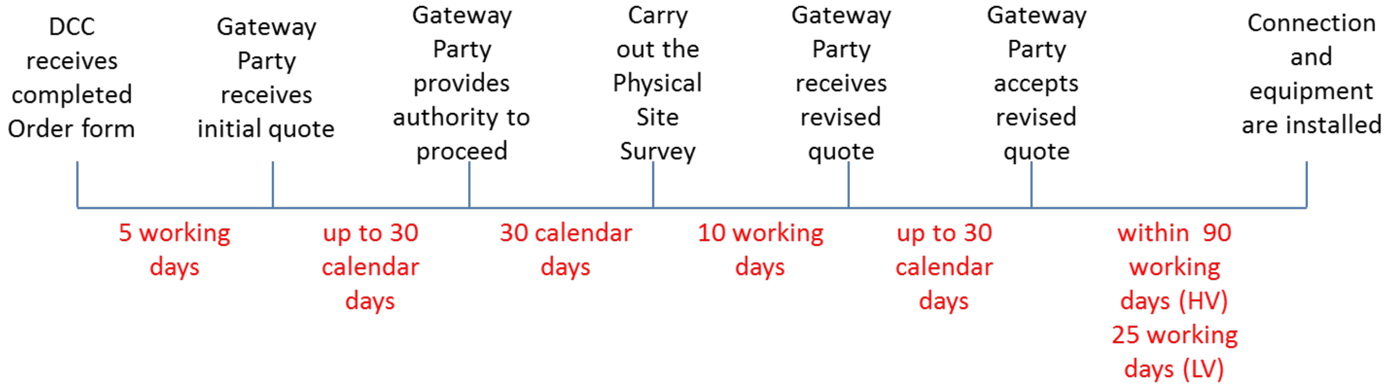
If diverse routing is required, the telecoms provider would route these connections through different exchanges and roads to deliver different connections into the same location.

This protects against cable failure and also the failure of a local exchange.

However, diverse routing may not always be available and even if it is, the cost of the civil works to build diverse routes may be prohibitive.

3 Overview of Connection Ordering Process

3.1 Timeline


DCC receives completed Order form
Gateway Party receives initial quote
Gateway Party provides authority to proceed
Carry out the Physical Site Survey
Gateway Party receives revised quote
Gateway Party accepts revised quote
Connection and equipment are installed
5 working days
up to 30 calendar days
30 calendar days
10 working days
up to 30 calendar days
within 90 working days (HV)
25 working days (LV)

3.2 Initial Order

In order to initiate the process the DCC Gateway Party will need to download the Connection Request Form from http://www.smartdcc.co.uk/documents-and-publications/resources/.

Guidance notes are included with the form to help with correct population of the form.

A separate form should be completed for each separate Connection required.

When the DCC receives the form it will check it for completeness. If it is OK, the DCC will inform the Party that the request has been accepted. If there is anything wrong or unclear on the form the DCC will contact the Party for clarification or correction.

Once the form has been accepted, the DCC will arrange an Electronic Site Review, which is a desk based assessment of the Party's requirements.

3.3 Initial Quote

Within 5 working days of having accepted the form the DCC will send the Party a Quotation with an estimate of the cost and delivery date for the link.

If the type of connection requested requires a physical site survey, this will be shown on the quote and the cost quoted will be indicative, to be confirmed after the site survey has taken place.

3.4 Authority to Proceed

Once the DCC Gateway Party has received the quotation, the Party has 30 calendar days, as specified in the SEC, to confirm whether it wishes to proceed.

This authorisation commits the DCC Gateway Party to the full cost of the connection as included in the quote.

If the DCC does not receive an explicit authority to proceed (signed by an authorised person) within 30 days the DCC will assume that the Party does not wish to proceed.

If the Party then decides to proceed at a later date they will have to start the connection ordering process from the beginning.

3.5 Notification of Access Procedures

As part of the authority to proceed, the Gateway Party must advise the DCC if the requested location is governed by any specific access protocols and identify what actions are required prior to any visit taking place.

It is important to identify all the documentary evidence that the DCC Gateway Party's organisation needs (including those where the Party does not own the data centre) before the Party will allow a DCC subcontractor to work on their premises. The DCC understands that different organisations have different requirements, so each Gateway Party should provide all the relevant information they require on the site-visit Pre Requisite form.

If there is any uncertainty, the Party should seek clarification via Service Desk.

If there is a need for a Risk and Method Statement (RAMS) document to be provided this should be advised in advance as there may be a charge for providing this.

Access to the site is required for both the site survey and installation. Any declined access, without prior warning of 5 working days, will result in another visit which would be chargeable.

3.6 Physical Site Survey

If a physical site survey is required, the telecom provider will visit the requested location and ensure that it is possible to install the circuit as requested and that the standard equipment can be installed.

The Gateway Pary needs to advise the DCC of any documentation or access procedures that need to be followed. If this is not done, and the telecom provider representative is turned away, the second visit will be chargeable.

Following completion of the Site Survey, an updated quote will be produced either confirming that the original quote is still valid, or providing updated quote details. This must be accepted by the Gateway Party before installation can commence.

3.7 Connection Installation

The telecom provider will install the physical line and equipment to terminate the connection into the requested data centre.

For HV installations the equipment typically installed requires 4U of rack space. For the LV option rack space capacity of 1U is required.

Once the line has been installed and basic testing carried out, Gamma will install the appropriate routing equipment.

If no issues are identified, the circuit installation will be flagged as complete and the Gateway Party will be billed for the circuit.

3.7.1 Connection Configuration

The DSP will then configure the router and set up test connectivity.

The Gateway Party is responsible for deciding which sessions are required and arranging set up of these in conjunction with the DSP. Session setup is a combination of the Gateway party providing the DSP with the appropriate IP addresses so that the firewalls can be opened and the Gateway Party following DCCKI doucmention to setup sessions to the appropriate DCC Services,

4 Detailed Connection Options

The following table shows the connection options available together with the levels of Availability that would be available for connection to the DCC Gateway.

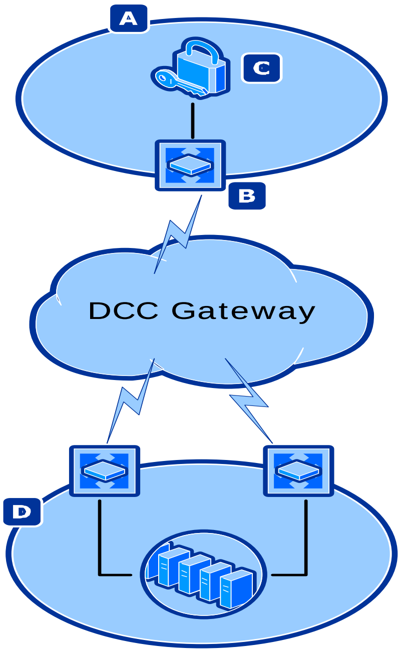
Connection Type	Resilience of access to DCC	Cost	Complexity
One site, one connection, one tunnel	Low	Low	Low
One site, two connections, two tunnels	Medium	High	Medium
Two sites, two connections, two tunnels	High	High	High

4.1 Low Resilience - One data centre, one connection

This is a suitable means of connection for small DCC Service Users and has the lowest installation and running costs.

As there is only a single connection, which could be either High Volume or Low Volume, the service availability is reduced (i.e. the DCC does not guarantee any availability target should the link fail).

This is acknowledged by the user when requesting this circuit type but has the advantage of the DCC Dateway Party paying only low charges for connection to the DCC.



In this example, a single connection to the DCC Gateway is made from the DCC Gateway Party location [A] to DCC MPLS network and onwards to the DCC data centres [D].

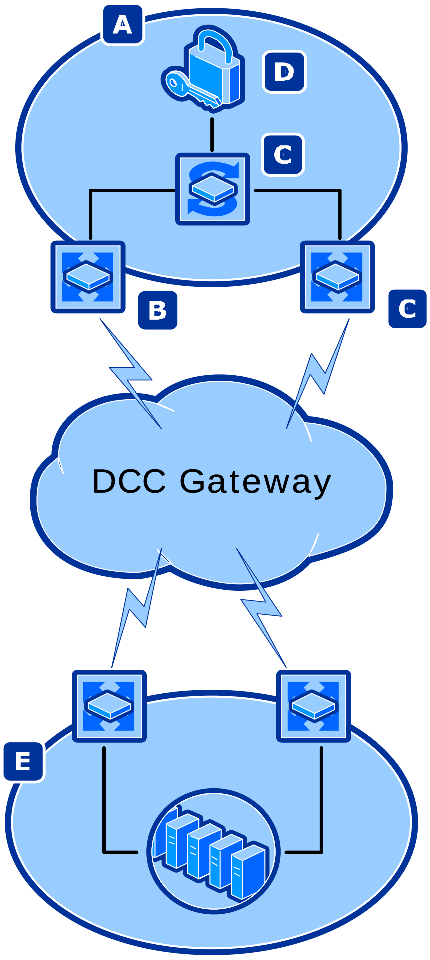
The DCC will install a router [B] at the user site which will link to the user's Policy Enforcement (PEP) [C] which is mandatory for the connection. (See the Code of Connection documentation)

IP addressing for the DCC router and user PEP will be supplied by the DCC.

4.2 Medium Resilience - One data centre, two circuits

Where the DCC Gateway Party has a high resilience data centre they may wish to order two diversely routed links into the single location.

When designing the service the Gamma will check each path from the site to the network core and ensure that there are no common connection points.



In this example the DCC Gateway Party data centre [A] is linked using diversely routed links and dual routers [B,C] to the DCC MPLS network and onwards to the DCC data centres [E].

The DCC supplied routers for each link must be connected via a user supplied layer 2 switched network [C]. This network must also link to the user security gateway [D], routed links are not supported by the standard service.

The links will operate as an active/standby pair and cannot be used for load sharing. (if you buy two links, both of them will not be active at the same time, one will be a backup for the other).

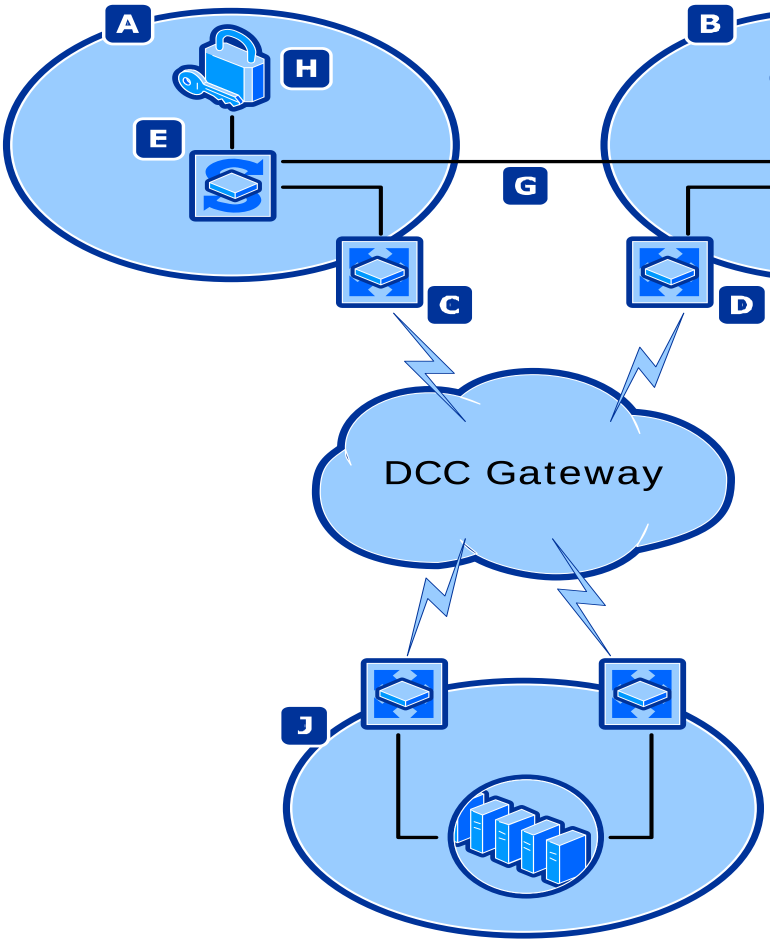
It is not a requirement for each link to be identically sized and either link can be high or low volume. Should the DCC Gateway Party decide to implement differently sized links they accept the risk that their service may be degraded when running on the smaller link in the event of a DR situation.

The two DCC routers will present a virtual shared IP which will be the gateway for the DCC Gateway Party security device. Should a DCC link, or router, fail the virtual IP will automatically switch to the standby router and traffic will continue to pass over the network. IP addressing for the DCC routers and the DCC Gateway Party's PEP will be provided by the DCC.

4.3 High Resilience - Two sites, two circuits

This service offers the most resilience and uses geographical separation of the customer sites to increase the resilience of the service.

This example shows the connectivity between DCC Gateway Party sites [A,B] and the DCC Data Service [J].



A link and router [C,D] will be installed by the DCC into the two sites. These will link to a DCC Gateway Party provided layer-2 switch at each site [E,F] and connect to the Party PEP [H,I].

To enable this to operate, the user must provide a layer-2 link [G] between the data centres for the connection of the routers and security gateways.

The links will operate as an active/standby pair and cannot be used for load sharing

It is not a requirement for each link to be identically sized and either link can be high or low volume. Should the DCC Gateway Party decide to implement differently sized links they accept the risk that their service may be degraded when running on the smaller link.

The two DCC routers will present a virtual shared IP which will be the gateway for the PEP.

Should a DCC link, or router, fail the virtual IP will automatically switch to the standby router and traffic will continue to pass over the network. IP addressing for the DCC routers and the PEP will be provided by the DCC.

Other options are available (such as two circuits into one site and a single circuit into another), but discussions with DCC Gateway Parties will be needed to establish failover and DR options. If there is a need to discuss requirements further then please contact the DCC who can organise a call with the necessary parties to review requirements and provide appropriate guidance.

5 Equipment to be Installed

The space requirements for the equipment that will be installed are expressed in rack unit of height (U). 1 rack unit of height (1U) equals 1.75-inches (44.45mm) of rack height.

The space requirements and equipment that will be installed at the DCC Gateway Party end of the connection will be:

5.1 Low Volume Connection

The requirement for an LV connection is for 1 rack unit (1U) per site.

The Gamma equipment installed will currently be a Cisco 3750G.

5.2 High Volume Connection

For HV the space required is 4 rack units (4U) per site:

- 1U switch,
- 1U fibre tray,
- 1U BT NTE,
- 1U BT remote access router. This will be a Cisco 3750G

Please note that model and versions may change.

5.2.1 Equipment Location

The equipment deployed should be located in an area where adequate power is available.

Placing equipment under an air conditioning unit would not be advisable as water could damage the equipment. Placing the equipment in a location that has access control would be preferable as security of the equipment is important.

It is the responsibility of the Gateway Paty to ensure that the environment within which the equipment will be located, is suitable from both space and temperature points of view.

AC power sockets are required for the equipment.

5.2.2 SEC Obligations

CoCo1.12 - The DCC Gateway Party shall ensure that the DCC Gateway Equipment is protected from unauthorised physical access. An access log of who has had physical access to the DCC Gateway Equipment shall be maintained at all times.

SEC H15.24 Each DCC Gateway Party shall ensure that no damage is deliberately or negligently caused to the DCC Gateway Equipment installed at its premises (save that such a Party may take emergency action in accordance with Good Industry Practice to protect the health and safety of persons or to prevent imminent damage to property).

6 Connection Configuration

Once a DCC Connection has been purchased and installed, then the connection must be configured to support the appropriate SEC Parties, User Roles and Services that each one will support.

This is done, by setting up a number of Transport Layer Security (TLS) tunnels, (referred to in this document as ‘sessions’).

These sessions will need to be requested and configured across the DCC Gateway Connection. There is no additional charge for the setup of these tunnels.

The sessions will be secure connections between the appropriate Policy Enforcement Points (PEPs) at each end (see the relevant DCC User Interface Specification (http://www.smartdcc.co.uk/DUGIDSv0.8_Clean.pdf) and SSI Interface Specification(http://www.smartdcc.co.uk/SSI_design_spec_v1.1.pdf).

The Smart Energy Code (SEC) determines that it is the Service User responsibility (and hence the responsibility of the DCC Gateway Party) to ensure that data to the live DCC User Gateway (i.e. Service Requests for meters) are prioritised over other traffic.

The sessions setup across the DCC Gateway Connection allow ‘bursting’ (i.e. can maximise the whole session) and they are not setup with any priority of service (i.e. the DCC Gateway Parties have to ensure that other traffic does not affect the Service Requests.

The sessions setup across the various DCC Connections allow for a maximum of two links with regard to auto-failover. i.e. if the primary connection fails then the link will automatically failover to the secondary connection, but if this also fails it will not automatically failover to a third connection.

The DCC Gateway Connections act in a Active – Passive mode and load balancing is not possible across two sessions.

The DCC Gateway has been designed so that when failover on a primary link fails, connectivity automatically routes to the secondary link, without any reconfiguration.

Likewise the IP addresses will remain the same. However should the secondary connection be to a different location to the primary, it is the responsibility of the Gateway Party to have a suitable connection between their two locations.

6.1 Complexity

Due to the possibility of there being any number of sessions across the DCC Gateway Connection, it is possible for some of the primary sessions (e.g. the live link for DUIS) to go down one DCC Gateway Connection and failover to a second DCC Gateway Connection and for other primary sessions (e.g. test connections) to go down the second DCC Gateway Connection and failover (if appropriate) to the first DCC Gateway Connection.

7 Disaster Recovery

The DCC Gateway has been designed so that when a Gateway Party's primary link fails, connectivity automatically routes to the secondary link, without any reconfiguration. Likewise the IP addresses will remain the same.

However should the secondary connection be to a different location to the primary, it is the responsibility of the Gateway Party to have a suitable connection between their two locations.

8 Glossary of Terms

Term / Acronym	Description
DR	Disaster Recovery
DUIS	DCC User Interface Specification
HV	High Volume
LV	Low Volume
PEP	Policy Enforcement Point
RDP	Registration Data Provider
SEC	Smart Energy Code
SSI	Self-Service Interface
TLS	Transport Layer Security