This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

SMKI PMA & SSC Guidance (Standards, Procedures and Guidelines)

Document Control

Document Owner	Smart Energy Code Company Ltd
Version	1.2
Date	13 March 2024
Document Status	SMKI PMA and SSC Approved
Date of Next Review	TBD
Classification	White

Change Record

Date	Author	Version	Change Reference
18/02/20	SECCo	0.1	Draft version created for review by SMKI PMA, including replacement of GPG 43, 45 and 46
17/03/20	SECCo	0.2	Draft version created for review by SMKI PMA, including replacement of GPG 13.
17/08/20	SECCo	0.3	Draft version created for review by SSC of the proposed replacement for GPG13 and GPG18
07/09/20	SECCo	0.4	Updated to reflect SSC comments from the SSC meeting on 26 August 2020.
4/12/2020	SECCo	1.0	SMKI PMA and SSC approved for publication.
28/02/2024	SECCo	1.1	Updated in line with MP259 to include guidance on acceptable standards for Transport Layer Security (TLS).
13/03/2024	SECCo	1.2	Updated to include guidance on use of SHA-1 and FIPS 186-5

Table of Contents

1. Introduction

The Smart Energy Code (SEC) contains numerous references to standards, procedures and guidelines in relation to security compliance and to Smart Metering Key Infrastructure (SMKI) and DCC Key Infrastructure (DCCKI) Services and the SMKI and DCCKI Document Sets. These include standards set by the International Organisation for Standardisation (ISO), by the International Electrotechnical Commission (IEC), by the United States National Institute of Standards and Technology (NIST), by the United States Federal Information Processing Standards (FIPS), as well as procedures derived from Request for Comments (RFCs) and NCSC Good Practice Guides (GPGs).

These standards, procedures and guidelines assist the DCC and Users to achieve consistent and reliable performance in the application of security controls and enable a common understanding of how to comply with such standards, procedures and guidelines.

The SMKI PMA has specific duties set out in SEC Section L1.17 that include an obligation to periodically review the effectiveness of the SMKI and DCCKI Document Set. As part of that review, the SMKI PMA identifies any changes or updates to the defined standards, procedures and guidelines and when any are standards, procedures and guidelines are deprecated or discontinued.

Similarly, the Security Sub-Committee (SSC) has delegated authority from the SEC Panel to consider under SEC Section G1.3, the security standards set out in G2 to G9 and the DCC or User have a SEC obligation to comply with any updated or replaced standard, procedure or guideline from such date as is determined by the SSC.

2. Purpose

The purpose of this document is to enable the SMKI PMA and the SSC to notify the DCC and Users of any changes to standards, procedures and guidance through the publication of this document. Where any standard, procedure or guidance is amended to an extent that it no longer applies to smart metering or where a standard, procedure or guideline is deprecated, discontinued or withdrawn by the publishing body, the SMKI PMA and the SSC will consider whether to publish bespoke standards, procedures or guidance to maintain the integrity of the security obligations and the SMKI and DCCKI Services and Document Sets.

3. Transitional Arrangements

The SMKI PMA and the SSC recognise that, when a standard, procedure or guideline is changed, updated or discontinued, industry participants may need some time to implement the new standards, procedures or guidelines unless, exceptionally, there is a ‘material’ and overriding security reason for more immediate action.

The SMKI PMA and the SSC will therefore consider on a case by case basis what, if any, transitional period should apply before the DCC and Users should be required to comply with the new version of a standard, procedure or guideline.

4. Published Information

As part of any review of standards, procedures and guidelines by the SMKI PMA and the SSC, the relevant standard, procedure or guideline will be assessed using the key overleaf.

Categorisation of standards, procedures and guidelines specified in the SEC ensures that the SMKI PMA, the SSC, the DCC and Users stay abreast of pending and actual changes and inform the DCC and Users when standards and guidelines are updated or made obsolete.

Key:	
	Current
	Under review
	Under development
	Related standard/guidance not referenced in SEC, reviewed for future updates
	Archived or withdrawn

In addition, the SMKI PMA and the SSC will publish details of any bespoke standards, procedures and / or guidelines to be implemented to ensure compliance with the SEC.

The DCC and User Independent Assurance Assessors will assess compliance with the standard, procedure or guideline that is specified in the SEC. Where a standard, procedure or guideline has changed or has been replaced by SMKI PMA or the SSC standards, procedures or guidelines, the relevant DCC and User Independent Assurance Assessor will expect to see a gap analysis and any necessary changes made to the Information Security Management System (ISMS), Incident Management Procedures or other relevant documentation affected by the standard, procedure or guideline.

The Excel spreadsheet containing all the standards, procedures and guidelines reviewed by the SMKI PMA can be accessed here, and by those reviewed by the SSC can be accessed here.

5. Background to Standards, Procedures and Guidelines

The original standards, procedures and guidelines that were published in the SEC were defined by BEIS (then DECC) with support from NCSC (then CESG) and were subject to public consultation.

Whilst the majority of standards and procedures are based on either internationally recognised standards such as ISO or IEC, or on widely implemented US standards such as NIST and FIPS, the majority of the guidelines were based on a series of Good Practice Guides (GPGs) developed by NCSC (then CESG).

The GPGs were developed to assist UK government and industries (not restricted to smart metering) to achieve consistent standards in the application of security controls and assist in the protection of Critical National Infrastructure (CNI). The SEC contains references to several NCSC GPGs that are mandated, mainly for compliance by the DCC. The DCC has ensured that the obligation for compliance with the GPGs have, largely, been enshrined into the contracts with its Service Providers.

During 2019, NCSC confirmed that it has discontinued GPGs and has moved to greater use of blogs which can be kept up-to-date more easily and to respond to changing security demands but these are inappropriate to use as mandated SEC obligations since they are subject to frequent change.

The SMKI PMA and the SSC has therefore developed bespoke guidance to ensure that the DCC and Users can continue to abide by relevant and essential guidelines to maintain the integrity of smart metering security and SMKI and DCCKI operations. The guidance has been developed to ensure there is no material change between the discontinued NCSC GPGs and the SMKI PMA and SSC proposed guidance.

6. SMKI PMA Guidance 001 (replaces GPG 45) – Verifying Individual Identity

6.1 Business Requirement

The SMKI PMA recognises that smart metering requires a set of attributes that can be applied to ensure that individuals applying to the DCC for key roles within the SMKI and DCCKI operational areas are appropriately authorised to a consistent standard.

Without such attributes and supporting documentation, it is difficult for the DCC to be absolutely certain of the identity of those applying for key roles e.g. as Senior Responsible Officer (SRO) or Authorised Responsible Officer (ARO).

This SMKI PMA guidance provides guidance on the Identity Proofing and Verification (IPV) of an individual. It describes the strength of evidence required as well as the validation and verification processes and the activity needed to ensure an adequate level of assurance for the legitimacy of an identity.

This guidance provides the DCC and Users with an understanding of the capabilities they will need to be able to demonstrate in order to perform identity proofing and establishes a common framework for the validation and verification of the identity of individuals. The guidance has been developed to ensure there is no material change between the discontinued NCSC GPG 45 and the SMKI PMA and SSC proposed guidance.

6.2 Overview of Verifying Individual Identity

The processes outlined in this guidance will enable a legitimate individual to prove their identity in a straightforward manner whilst creating significant barriers to those trying to claim to be somebody they are not by:

- the individual shall be expressly required to declare their identity;
- the individual shall provide specific and defined evidence to prove their identity;
- the evidence shall be confirmed as being Valid and/or Genuine and belonging to the individual;
- checks against the identity will confirm whether it exists in the real world; and
- the breadth and depth of evidence and checking required shall differ depending on the level of assurance needed in that the identity is real and belongs to the individual

Process

The Applicant shall be required to declare the name, date of birth and address that they wish to be known as so that there is no ambiguity about the identity that is going to be used (Claimed Identity).

The Applicant shall be required to provide evidence that the Claimed Identity exists (Identity Evidence Package). This may be provided electronically or physically depending on the level of assurance required and the capabilities of the organisation that is going to proof the Applicant.

The evidence provided shall be checked in order to determine whether it is Genuine and/or Valid (Validation).

The Applicant shall be compared to the provided evidence and/or knowledge about the Claimed Identity to determine whether it relates to them

The Claimed Identity shall be subjected to checks to determine whether it has had an existence in the real world over a period of time (Activity History).

The Claimed Identity shall be checked with various counter-fraud services to ensure that it is not a known fraudulent identity and to help protect individuals who have been victims of identity theft (Counter-Fraud Checks).

At the end of the process there is an Assured Identity that describes the level of confidence that the Applicant is the owner of the Claimed Identity and that identity is genuine.

Evidence to support Verifying Individual Identity Assurance

For smart metering SMKI and DCCKI cryptographic roles set out in the SEC, assurance is required, supported by evidence that the Claimed Identity is an Identity with evidence that supports the real world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken to determine that the identity relates to a real person and that the Applicant is the owner of that identity are such that might be offered in support of criminal proceedings.

There are five (A to E) IPV elements that are used to characterise and score the checks carried out against a claimed identity are described in the following sections.

6.3.1 IPV Element A – Strength of Identity Evidence

The purpose of this element is to record the strength of the Identity Evidence provided by the Applicant in support of the Claimed Identity. The following criteria demonstrates the properties of the Identity Evidence and the corresponding score for this element. The Identity Evidence must, as a minimum, meet all the properties defined to achieve that score.

- The Issuing Source of the Identity Evidence must confirm the applicant's identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2007;
- The issuing process for the Identity Evidence must have ensured that it was delivered into the possession of the person to whom it relates;
- The issued Identity Evidence contains at least one reference number that uniquely identifies itself or the person to whom it relates;
- The Personal Name on the issued Identity Evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases and initials for forenames and surnames are not permitted;
- The issued Identity Evidence contains a photograph/image/Biometric of the person to whom it relates **OR** The ownership of the issued Identity Evidence can be confirmed through Knowledge Based Verification;
- Where the issued Identity Evidence is, or includes, electronic information that information is protected using cryptographic methods and those methods ensure the integrity of the information and enable the authenticity of the claimed Issuing Source to be confirmed;
- Where the issued Identity Evidence is, or includes, a physical object it contains developed security features that requires Proprietary Knowledge and Proprietary Apparatus to be able to reproduce it.

Evidence Examples (IPV Element A)

No single piece of evidence can be considered as proof of identity. However combined with other pieces of evidence they can be used in order to develop a level of assurance as to the identity of an individual.

The following table provides examples of the types of evidence data that may be provided and the Evidence Categories they could be considered to be in.

The Table should not be considered as complete or definitive.

Identity Evidence	Citizen	Money	Living
Passports that comply with ICAO9303 (Machine Readable Travel Documents)	X		
EEA/EU Travel Documents that comply with Council Regulation EC Number 2252 / 2004	X		
Northern Ireland Voters Card	X		X
US Passport Card	X		
Retail bank / Credit Union / Building Society Current Account		X	
Student Loan Account		X	X
Bank Credit Account / Credit Card		X	X
Non-Bank Credit Account (including credit / store / charge cards)		X	
Bank Savings Account		X	
Buy To Let Mortgage Account		X	X
Digital Tachograph Card	X		X
Armed Forces ID Card	X		
Proof of Ager Card issued under the Proof of Age Standards Scheme (containing a unique reference number)			X
Secured Loan Account (including hire purchase)		X	X
Mortgage Account		X	X
EEA / EU Full Driving Licences that comply with European Directive 2016 / 126 / EC	X		X

6.3.2 IPV Element B – Outcome of the Validation of Identity Evidence

The purpose of this element is to record the score obtained from the Identity Evidence Validation process. The following table demonstrates the characteristics of the Validation processes and the corresponding score for this element.

Score Identity Evidence Validation

Score	Identity Evidence Validation
0	Validation of the Identity Evidence was unsuccessful
1	All Personal Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source
2	All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held/published by the Issuing/Authoritative Source **OR**

	The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skill and appropriate equipment and confirmed the integrity of the physical security features **OR** The issued Identity Evidence has been confirmed as Genuine by confirmation of the integrity of the cryptographic security features
3	The issued Identity Evidence has been confirmed as genuine by trained personnel using their skill and appropriate equipment and confirmed the integrity of the physical security features **OR** The issued Identity Evidence has been confirmed as genuine by confirmation of the integrity of the cryptographic security features **AND** All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held / published by the Issuing Source / Authoritative Source**.**
4	The issued Identity Evidence has been confirmed as Genuine by trained personnel using their skills and appropriate equipment including the integrity of any cryptographic security features **AND** All Personal Details and Evidence Details from the Identity Evidence have been confirmed as Valid by comparison with information held / published by the Issuing Source / Authoritative Source

Validation (IPV Element B)

Determining whether Identity Evidence is Genuine

Examination of the security features of a physical document

The proofing organisation capability to Validate identity documents will affect the determined level of identity assurance. The proofing organisation shall have sufficiently trained staff and appropriate equipment to inspect the security features of common forms of physical documents that they accept as Identity Evidence. As a minimum a proofing organisation conducting physical inspection of Identity Evidence shall be able to detect the following common document frauds:

- Counterfeit documents – where a document has been created outside of the normal competent authority processes (e.g. a copy).
- Forged documents – where original documents have been modified to include false details (e.g. changed Personal Details).

Physical document containing cryptographically protected information

For physical documents provided by the Applicant that contains cryptographically protected information the proofing organisation shall have sufficient equipment, systems and training to be able to interrogate the cryptographically protected information, to ensure that it has not been altered since

the Issuing Source produced the Identity Evidence and determine that the cryptographically protected information relates to the physical document to which it is attached.

Electronic evidence containing cryptographically protected information

For electronic Identity Evidence provided by the Applicant that contains cryptographically protected information (e.g. in a PDF document), the proofing organisation shall have sufficient systems and training to interrogate the cryptographically protected information and determine that it relates to the Identity Evidence, and that the Identity Evidence has not been altered since it was produced by the Issuing Source.

Checking if the Identity Evidence is Valid

The proofing organisation should confirm that forms of Identity Evidence that include features such as check digits and specific identifier structures are consistent with their specification. Only an Issuing/Authoritative Source may confirm whether the Identity Evidence is Valid; Identity Evidence cannot be determined to be Valid simply from inspection of the Identity Evidence itself (see Genuine).

6.3.3 IPV Element C – Outcome of Identity Verification

The purpose of this element is to record the score obtained from the Identity Verification process. The following table demonstrates the outcomes of the Verification processes and the corresponding score for this element.

Score Identity Verification Outcome

Score	Identity Verification Outcome
0	Unable to confirm that the Applicant is the owner of the Claimed Identity
1	The Applicant has been confirmed as having access to the Identity Evidence provided to support the Claimed Identity
2	The Applicant's ownership of the Claimed Identity has been confirmed by a Static Knowledge Based Verification **OR** The Applicant's ownership of the Claimed Identity has been confirmed by a Dynamic Knowledge Based Verification OR The Applicant's ownership of the Claimed Identity has been confirmed by a physical comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity **OR** The Applicant's ownership of the Claimed Identity has been confirmed by a Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity
3	The Applicant's ownership of the Claimed Identity has been confirmed by physical comparison using a photograph / image **OR** Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity AND

	The Applicant's ownership of the Claimed Identity has been confirmed by a Static OR Dynamic Knowledge Based Verification
4	The Applicant's ownership of the Claimed Identity has been confirmed by a physical comparison of the Applicant using a photograph/image to the strongest pieces of Identity Evidence OR By a Biometric comparison of the Applicant to the strongest piece of Identity Evidence provided to support the Claimed Identity **AND** The Applicant's ownership of the Claimed Identity has been confirmed by both a Static **AND** Dynamic Knowledge Based Verification **AND** The Applicant's ownership of the Claimed Identity has been confirmed by an interaction with the Applicant via the declared address

Verification (IPV Element C)

Static Knowledge Based Verification (KBV)

Static KBV requires that the Applicant and the proofing organisation have a pre- existing shared secret, or that the proofing organisation uses an external trusted source with which the Applicant already has a shared secret.

There must be a reasonable expectation that the Applicant is aware that they should not disclose this secret to any person or organisation other than the one with whom they share the secret.

The secret must be random enough to make it unlikely to be guessed by an attacker who is given a number of opportunities to guess it.

A shared secret may only be exchanged via a method where the proofing organisation has confirmed that the delivery method is linked to the Claimed Identity.

External trusted source where the Applicant already has such a relationship can be used as a static KBV. Where an external trusted source is used, the process shall be able to confirm to the proofing organisation that an individual with matching Personal Details has successfully passed the Static KBV process.

Dynamic Knowledge Based Verification

Dynamic KBV needs the proofing organisation to gather information about the Claimed Identity and then requires the Applicant to demonstrate that they have such knowledge about the Claimed Identity that it is likely they are the owner of that identity.

The quality and success of the Dynamic KBV process is dependent on a number of factors:

- The questions should be relevant, sensible and proportionate
- There shall be an expectation that the owner of the Claimed Identity can reasonably be expected to know the answer
- The questions shall be unambiguous as to be easily understood by the Applicant
- The ease by which the Applicant can enter the correct answer
- The availability of the answer from information in the public realm, especially social networking sites and public registers
- The likelihood of friends and family knowing the answer
- The difficulty by which the questions could be correctly answered by guesswork

- The risk of datasets containing the required information being made available to organised crime
- The risk that the theft of a possession such as a wallet or purse could provide the required information to an imposter

Dynamic KBV data

The degree of assurance that can be taken from the KBV process is linked to the quality and availability of the data used to generate the questions.

Wherever it is practical to do so, KBV data should not be used if it is already in the public domain. Information in the public domain means that the KBV data can be accessed by another person either with or without a degree of research or is contained within a public facing information site.

Dynamic KBV principles

There must be a sensible balance between achieving assurance that the Applicant is the owner of the Claimed Identity and presenting an attractive Applicant journey. With this in mind the proofing organisation shall follow a number of basic KBV principles:

- The proofing organisation should try to use KBV data of the highest quality where possible. Fewer questions about KBV data that is highly unlikely to be known by someone other than the owner of the Claimed Identity is preferable to many questions about KBV data that is more likely to be available to others
- KBV questions shall be based on a range of KBV data and not reliant upon one single KBV source
- KBV questions should be carefully constructed as to be clear and obvious to the Applicant what is being asked
- KBV questions should cover facts about the Claimed Identity that fall into different Evidence Categories
- Where the proofing organisation offers the Applicant a selection of suggested answers (i.e. multiple choices) then all the answers must be plausible, and the correct answer should not be easily guessed or determined using publicly available information
- It must be recognised that the process cannot account for every eventuality when using KBV, e.g. it must be accepted that certain KBV data items may be known to close family members.

Physical Comparison

The physical comparison step of verification requires the Applicant to be verified by a visual confirmation that they appear to be the person to whom the Identity Evidence was issued. The two methods by which this may be completed are an in person face-to-face process and a remote process (e.g. using a video/video streaming link). In either case the proofing organisation shall consider a number of basic principles:

- Any person performing the comparison must be able to clearly see both the Applicant and the image to which the Applicant is being compared
- Any person performing the comparison shall have sufficient training in performing identification of persons
- The quality of images must be sufficient to allow the identification of the Applicant as the person depicted by the Identity Evidence

Biometric Comparison

The biometric comparison step of verification requires the Applicant to be verified by a biometric confirmation that they appear to be the person to whom the Identity Evidence was issued. The proofing organisation shall consider a number of basic principles:

- The False Non-Match Rate (FNMR) of the biometric matching system;
- The False Match Rate (FMR) of the biometric matching system;
- The quality of the biometric against which the Applicant is being compared.

In particular, the proofing organisation shall ensure they have a sufficiently low FMR to have confidence that the biometric system is effective at detecting imposters.

6.3.4 IPV Element D – Outcome of Counter-Fraud Checks

The purpose of this element is to record the score obtained from the Counter-Fraud Check process. The following Table demonstrates the outcomes and the corresponding score once any investigation activity has been carried out for this element.

Score Counter-Fraud Checks

Score	Counter-Fraud Checks
0	Applicant is suspected of being, or known to be, fraudulent
1	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity
2	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent
3	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent **AND** No confirmed evidence, using SMKI PMA specified source(s), that the Applicant is fraudulent
4	No confirmed evidence, using a reliable and independent source, that the provided Identifier is being used for fraudulent activity **AND** No confirmed evidence, using a reliable and independent source, that the Applicant is fraudulent **AND** No confirmed evidence, using SMKI PMA specified source(s), that the Applicant is fraudulent

	AND No confirmed evidence, using source(s) private to SMKI PMA, that the Applicant is fraudulent

Counter-fraud Capabilities (IPV Element D)

As part of the counter fraud checks the proofing organisation shall have, through their own internal data sets or via reliable and independent sources, the following counter fraud checking capabilities:

- Whether the Claimed Identity has been subject to identity theft, regardless whether it was successful or not
- Whether the Claimed Identity is known to other organisations
- Whether the Claimed Identity is likely to be targeted by third parties
- Whether the Claimed Identity may be deceased
- Whether the Claimed Identity is known to be a fraudulent identity

6.3.5 IPV Element E – Activity History of the Claimed Identity

The purpose of Activity History is to prove a continuous existence of the Claimed Identity over a period of time backwards from the point of Assessment. Activity History is determined by collating Activity Events across multiple Evidence Categories into a single Activity Event Package.

To qualify, the Activity Event shall relate to an interaction between the Claimed Identity and a source of Activity Events. This can be in either direction, e.g. the Claimed Identity using the services of the source or the source initiating an interaction with the Claimed Identity including issuing something to the Claimed Identity. Activity Event data must refer to an individual whose Personal Details match those of the Claimed Identity, allowing for any changes in Claimed Identity that have occurred over the time period being assessed for the Activity History.

The degree of assurance that can be taken from the Activity History process is linked to the quality of the data used, how easily it can be fabricated and how well its integrity is protected. The proofing organisation shall take this into account when assessing the Activity History, expanding the data sources and extending the history period where there is insufficient confidence in the Activity Events.

The proofing organisation shall be able to demonstrate with the Activity Events a continuous existence of the Claimed Identity over the period required by the Identity Level.

The following table describes the scoring profile for this element:

Score	Properties of Active History
0	Unable to demonstrate the required Activity History
1	No demonstration of an Identities Activity History was required
2	Claimed Identity demonstrates an Activity History of at least 180 calendar days
3	Claimed Identity demonstrates an Activity History of at least 405 calendar days
4	Claimed Identity demonstrates an Activity History of at least 1080 calendar days

Example Activity Events (IPV Element E)

The following Table provides examples of activity events that could be used to demonstrate a history of activity.

Citizen	Money	Living
Electoral Roll Entry	Repayments on an unsecured Personal Loan Account (excluding payday loans)	Land Registry Entry
	Repayments and transactions on a non-bank credit account (credit card)	National pupil database entry
	Debits and credits on a retail bank / credit union / building society current account	Post on internet / social media site
	Repayments on a student loan account	Repayments on a secured loan account
	Repayments and transactions on a bank credit account (credit card)	Repayments on a mortgage account
	Debits and credits on a savings account	Repayments on a gas account
	Repayments on a Buy to Let mortgage account	Repayments on an electricity account

6.4 Requirements for Acceptable Identity for Smart Metering

The following table set out the minimum criteria for the IPV element required for smart metering.

Category	Requirements
Identity Evidence Profile	The Identity Evidence Package must contain Identity Evidence that as a minimum meets one of following profiles: pieces of Identity Evidence with a score of 3 **OR** 1 piece of Identity Evidence with a score of 3 2 pieces of Identity Evidence with a score of 2 These are referred to as an Identity Evidence Profile of 3:3 and 3:2:2 respectively.
Validation of Identity Evidence	Each piece of Identity Evidence must be Validated with a process that is able to achieve a score that matches the Identity Evidence Profile; i.e. where the profile is 3:3 the Validation processes must be able to also achieve scores of 3:3 respectively, where it is 3:2:2 it must be able to achieve scores of 3:2:2 respectively
Verification	As a minimum the Applicant must be Verified as being the owner of the Claimed Identity by a process that is able to achieve a score of 3 for Verification.
Counter-Fraud Checks	As a minimum the Claimed Identity must be subjected to a Counter-Fraud Check by a process that is able to achieve a score of 3.
Activity History	As a minimum the Activity Event Package must be able to achieve a score of 3 for the Activity History of the Claimed Identity.

6.5 Verifying Individual Identity Definitions

The definitions of identity relevant terms provided here are intended to support a common understanding in the context of this document

Definitions

The following definitions explain the purpose and meanings of the terms used within this document.

Term	Definition
Activity Event	An action, transaction or other point in time occurrence (including issue date) that demonstrates an interaction between the Claimed Identity and another entity. Only Activity Events that are connected to an Identity with Personal Details that match those of the Claimed Identity can be used however, shortenings and aliases are permitted (e.g. Mike for Michael).
Activity Event Package	The Activity Event Package is the collection of Activity Events that is used to evaluate the Activity History of the Claimed Identity. The Activity Event Package must contain Activity Events across multiple Evidence Categories (Citizen – C; Money – M; Living – L)
Applicant	The individual who is stating the claim to an identity.
Assessment	The activity of performing the identity proofing process as defined in this document.
Assured Identity	A Claimed Identity that is linked to an Applicant with a defined level of confidence that it is the Applicant's real identity.
Authoritative Source	An authority that has access to sufficient information from an Issuing Source that they are able to confirm the validity of a piece of Identity Evidence
Biometric	A measure of a human body characteristic that is captured, recorded and/or reproduced in compliance with ICAO 9303 or ISO/IEC 19794.
Citizen Category	A type of evidence category. To be included in the Citizen category at least one of the following criteria shall be met: Be issued by a Public Authority (or national equivalent) Be issued by an organisation through a process determined by a Public Authority (or national equivalent)
Claimed Identity	A declaration by the Applicant of their current Personal Name, date of birth and address.
Evidence Categories	A collective term for the categories of evidence i.e. Citizen (C), Money (M) and Living (L). Evidence shall be assessed against every category and can be considered in multiple categories where it meets the required criteria. Where evidence meets the required criteria for multiple categories it may only be used to fulfil one category requirement at a time per IPV Element (i.e. it doesn't count as fulfilling two categories for a specific IPV Element but can be in different categories for different IPV Elements). This does not mean the evidence must be in the same category for all Applicants, the same type of evidence (e.g. a Bank credit account) may be used in different categories for different Applicants

Evidence Details	A combination of the unique reference number(s) and, where applicable, issue date and expiry date included on a piece of Identity Evidence.
Financial Organisation	An organisation that has been classified as a "financial institution" or "credit institution" by the Money Laundering Regulations 2007.
Genuine Identifier	To be what something is said to be; i.e. authentic not counterfeit. A thing that is used to repeatedly recognise an individual. The Identifier isn't required to demonstrate the Identity of the individual only that it can be used to recognise the same individual.
Identity	A collection of attributes that uniquely define a person or organisation. The fact of being whom or what a person or thing is.
Identity Assurance	A process that determines that level of confidence that the Applicant's Claimed Identity is their real identity
Identity Evidence	Information and/or documentation that is provided by the Applicant to support the Claimed Identity. Identity Evidence must, as a minimum, contain the Personal Details **OR** the Personal Name and photo/image of the person to whom it was issued. Identity Evidence must be current, i.e. it must not have an expiry date that is before the time of Assessment. Examples of Identity Evidence are given in Annex A.
Identity Evidence Package	The Identity Evidence Package is the collection of Identity Evidence provided to support the Claimed Identity. The Identity Evidence Package must contain at least one piece of Identity Evidence that demonstrates address and one that demonstrates date of birth. The Identity Evidence Package must only contain one piece of Identity Evidence in any Evidence Category.
Identity Evidence Profile	The Identity Evidence Profile sets out the minimum criteria for the strength of Identity Evidence in the Identity Evidence Package.
Issuing Source	An authority that is responsible for the generation of data and/or documents that can be used as Identity Evidence.
Knowledge Based Verification (KBV)	**Static** Where a secret has been previously exchanged between two parties. One party uses the secret to verify that they are the other party with whom the secret was originally exchanged. Also referred to as a shared secret. **Dynamic** A process where the Applicant is required to provide answers to questions relating to the Claimed Identity.
Living Category	A type of evidence category. To be included in the Living category at least one of the following criteria shall be met: Be issued by • an organisation that provides employment to the Applicant • an organisation that provides education services to the Applicant

	• an organisation that provides training services to the Applicant • an organisation that provides certified assessment of the Applicant • an organisation that provides licensing of the Applicant • an organisation that provides an essential utility to the Applicant • an organisation that provides living support to the Applicant • an organisation that operates a community or social group/network to which the Applicant belongs • an organisation that operates a loyalty programme to which the Applicant belongs • an organisation that operates a subscription service to which the Applicant subscribes • an organisation that provides health services to the Applicant • an organisation that provides goods or services to the address of the Applicant
Money Category	A type of evidence category. To be included in the Money category at least one of the following criteria shall be met: Be issued by a Financial Organisation regulated by a Public Authority (or national equivalent) Be issued by a Financial Organisation regulated by a body mandated by national legislation
Personal Details	A combination of Personal Name and **at least one of** date of birth or address. (Not to be confused with Personal Data as defined by the Data Protection Act.)
Personal Name	A proper name used to identify a real person, as a minimum this contains forename and surname (also known as given name and family name); it may include titles, other/middle names and suffixes
Proprietary Apparatus	Any apparatus that is, or has been, specially designed or adapted for the making of false documents, and any article or material that is, or has been, specially designed or adapted to be used in the making of such documents.
Proprietary Knowledge	Knowledge about the format, layout and material that is required for the making of a false document.
Public Authority	An organisation that has been classified as such by the Freedom of Information Act 2000
Valid	To know that something stated is true.
Validation	A process performed to determine whether a piece of Identity Evidence is Genuine and/or Valid.
Verification	A process performed to determine whether the Applicant is the owner of the Claimed Identity.

7. SMKI PMA Guidance 002 (replaces GPG 46) – Verifying Organisation Identity)

7.1 Business Requirement

The SMKI PMA recognises that individuals that are subject to identity proofing will rely on the sponsorship and authorisation of a qualifying organisation. This guidance is designed to demonstrate how identifying the individual in combination with checking that they are a responsible person acting on behalf of the organisation, can provide an adequate level of assurance with regard to the existence of an organisation and that the individual claiming to be acting on behalf of the organisation is someone who is authorised to act on behalf of the organisation

This SMKI PMA guidance assists the DCC and Users to understand what is required for the proofing of an organisation and verification that an individual is a real person and that they are responsible and accountable for the action of that organisation. The guidance has been developed to ensure there is no material change between the discontinued NCSC GPG 46 and the SMKI PMA and SSC proposed guidance.

7.2 Overview of Verifying Organisation Identity

The arrangements outlined in this guidance will establish the requirements for identifying an organisation and at least one individual who is accountable and responsible for actions of that organisation in the context of smart metering SMKI and DCCKI services and operations.

In addition, this guidance will characterise the elements of the validation and verification processes that should be carried out. The guidance will:

- establish the requirements for identifying an organisation and at least one individual who is accountable for that organisation in the context of access to and use of HMG online services.
- provide an understanding of the capabilities needed by the proofing process to demonstrate that an individual is accountable for an organisation in the context of access to and use of smart metering SMKI and DCCKI services and operations.
- provide information to independent assessment organisations to facilitate independent assessment and accreditation of organisation proofing services as appropriate.

7.3 Process to support Verifying Organisation Identity

The process should enable a legitimate individual to demonstrate that they are a Responsible Officer of an Organisation in a straightforward manner whilst creating significant barriers to those who are not.

The individual shall be required to demonstrate their identity and shall be required to declare that they are a Responsible Officer of an Organisation. Checks shall be carried out in a manner that is sufficient to both hold an individual accountable for their actions and hold an Organisation accountable for the actions performed by the individual acting in their capacity as a Responsible Officer of that Organisation.

Within the UK, an organisation is created from self-asserted data by the organisation's owner, with little or no identity proofing of the owner. However all organisations will have one or more people that are held accountable for the actions of that organisation (known as Responsible Officers).

Whilst some UK organisations are not registered in any statutory and publicly available register, most smart metering organisations tend to be registered (e.g. limited companies, or Limited Liability Partnerships (LLP)). These organisations are at risk of being targeted by a person fraudulently

claiming to be an authorised representative of the organisation to either disrupt the organisation's businesses or to commit fraud.

A limited company or a LLP in the UK must be registered with Companies House. When registering with Companies House they must provide a correspondence address by which they can be contacted (the registered address) and provide the details of all Responsible Officers (as a minimum there must be at least one if a company (Director) or two if a partnership (Partners)). The Registrar will confirm the registered address via the address registered for that organisation.

Whilst an organisation has a legal standing in its own right, all organisations operate through an individual (or several individuals) that have authority to make decisions and act on behalf the organisation. For an organisation to have an Identity it must have at least one individual who can act for and on its behalf. Therefore and importantly it is not just the assurance of the existence of the organisation itself that is being sought but also that there is an individual (Responsible Officer) who has the authority to act for and on behalf of that organisation when interacting with smart metering SMKI and DCCKI services and operations.

The Verification Process

The following provides an overview of the proofing process:

- The identity of the applicant shall be proven in accordance with SMKI PMA Good Practice Guide 001 (Identity Proofing and Verification of an Individual).
- The applicant shall declare the organisation for which they are a responsible officer. Where details of an organisation are held on a register, the applicant shall provide the registered details which must, as a minimum, contain the organisation details, the registered address and, where applicable, the organisation identifier.
- Checks shall be performed to determine that the applicant is a responsible officer of the organisation.
- At the end of the process a relationship has been established between the applicant and an organisation that describes the level of confidence that the applicant is a responsible officer of that organisation and, by inference, that the organisation is a legal entity.

The Verification Level

The level of identity proofing required provides an adequate level of confidence in that claimed identity where the Applicant has declared that they are a Responsible Officer for the Organisation and gives sufficient confidence for it to be offered in support of criminal proceedings.

Organisation Proofing and Verification (OPV) Elements

OPV elements are used to characterise and score the checks carried out against a claimed organisation identity. There are three OPV elements that are described in the following sections.

7.3.1 OPV Element A - Outcome of IPV of the Applicant's Identity

The purpose of this element is to record the assurance gained of the Applicant's identity. This is important as before the Applicant can be confirmed as being a Responsible Officer of an organisation there must be some certainty as to who they are.

Mandatory Requirement

To demonstrate satisfactory assurance of the identity required, the Applicant must have been proofed to the level compliant with that described in SMKI PMA Guidance 001 (Identity Proofing and Verification of an Individual).

7.3.2 OPV Element B - Outcome of Verification of the Responsible Officer

The purpose of this element is to record the assurance gained of the Applicant being a Responsible Officer of the organisation.

Mandatory requirement

To demonstrate satisfactory assurance of the Responsible Officer:

- The Personal Details of the Applicant must have been confirmed as matching those of a Responsible Officer for the Organisation held in a Register (e.g. listed at Companies House).

OR

- The Applicant has been confirmed by the Organisation as being a Responsible Officer.

7.3.3 OPV Element C - Outcome of Counter-Fraud Checks

The purpose of this element is to record the outcome from the Counter-Fraud Check process.

Mandatory Requirement

To demonstrate satisfactory assurance of the Counter-Fraud aspects:

- There must be no confirmed evidence, using a reliable and independent source, that the Organisation is not a legal Organisation.

AND

- No confirmed evidence, using SMKI PMA specified source(s), that the Organisation is not a legal Organisation.

7.3.4 Outcome of Organisation Identity Checks

The Organisation Identity will only be met when all three of the mandatory requirements set out in OPV A, B and C have been met as a minimum.

7.4 Organisation Proofing Definitions

The definitions of relevant terms relating to Organisation Proofing provided here are intended to support a common understanding in the context of this document

Definitions

The following definitions explain the purpose and meanings of the terms used within this document.

Term	Definition
Applicant	An individual who is purporting to be a responsible officer of an Organisation
IPV	Identity Proofing and Verification
Organisation	A legal body with an existence that is separate in law from its members
Organisation Details	The legal name and address of an organisation

Organisation Identifier	An identifier associated with an organisation that is unique within a register
OPV	Organisation Proofing and Verification
Personal Details	A combination of personal name, date of birth and address. (Not to be confused with Personal Data as defined by the Data Protection Act.)
Personal Name	A proper name used to identify a real person, as a minimum this contains forename and surname (also known as given name and family name); it may include titles, other/middle names and suffixes.
Register	An official public record containing details about an organisation that the organisation is legally required to keep up to date and accurate
Registered Address	The postal address and email address (where applicable) of an organisation as recorded in a register
Registration Details	Information about an organisation that is held in a Register
Responsible Officer	A person who is legally accountable for the actions of an organisation

7 SMKI PMA & SSC Guidance 003 (replaces GPG 13) – Protective Monitoring

8.1 Business requirement

The SEC requires the DCC and its Service Providers to monitor the activity on the DCC Systems in accordance with Protective Monitoring Guidance provided by the SMKI PMA and SSC. The Guidance also aims to ensure that all system activity is recorded in audit logs and that Time Stamping is recorded in a standard format which is compliant with appropriate British and International Standards and SMKI PMA and SSC Guidance.

The SMKI PMA and the SSC recognise that smart metering systems operated by the DCC and its Service Providers require a set of business processes, with essential support technology, to ensure security measures that protect the confidentiality, integrity and availability of those systems and that also ensure the accountability of the participants.

The business requirement is to implement Protective Monitoring solutions to be developed, deployed and managed in accordance with the requisite industry best security standards as set out in the Smart Energy Code (SEC) and underpinned by an industry best practice information security framework based on ISO27001 and an industry best practice risk management framework based on ISO27005 as set out in the SEC.

The purpose of this Guidance is to provide information security controls for smart metering systems (e.g. inspecting firewall logs, investigating operating system security alerts and monitoring an IDS/IPS). It includes putting into place mechanisms for configuration of event logs, and automated collection and analysis of such logs to provide an audit trail of security relevant events of interest.

This Guidance sets out what is meant by Protective Monitoring and provides guiding principles on a Protective Monitoring Strategy to inform the implementation and Protective Monitoring controls that are required to be implemented by the DCC and its Service Providers in relation to DCC Total Systems such that there can be confidence in the security of the DCC Total System.

This guidance has been developed and agreed by the SMKI PMA and the SSC. The guidance has been developed to ensure there is no material change between the discontinued NCSC GPG 13 and the SMKI PMA and SSC proposed guidance.

8.2 Overview of Protective Monitoring Benefits

To take from NIST and adapt accordingly: The benefits of Protective Monitoring can be defined as maintaining continuous and ongoing awareness of information security, vulnerabilities, and threats to support organisational risk management decisions[1].

This Protective Monitoring Guidance is aligned to:

- ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls
- National Information Systems (NIS) Directive's Cyber Assessment Framework (CAF) (with particular focus on Objective C - Detecting Cyber Security Events).
- ISO/IEC 27005:2011- Information technology - Security techniques - Information security risk management

[1] The terms "continuous" and "ongoing" in this context mean that security controls and organisational risks are assessed and analysed at a frequency sufficient to support risk-based security decisions to adequately protect organisation information. Data collection, no matter how frequent, is performed at discrete intervals.

This Guidance does not preclude the DCC or its Service Providers from using additional industry standard tools and techniques to complement the above as part of their Protective Monitoring strategy. For example, this may include using frameworks such as MITRE ATT&CK for threat analysis to feed into their risk assessment and their Protective Monitoring activities.

8.3 Protective Monitoring Guiding Principles

When considering Protective Monitoring, the DCC and its Service Providers must take into account the following guiding principles:

1. Adopt an organisation-wide Protective Monitoring strategy that defines a consistent approach and common goals;
2. Identify the value and benefits that Protective Monitoring brings to the DCC and its Service Providers;
3. Implement adequate infrastructure to support Protective Monitoring requirements within the DCC and its Service Providers;
4. Ensure adequate resourcing for Protective Monitoring roles and ensuring personnel in such roles have adequate skills and ongoing training;
5. Document and operate the business processes necessary to undertake Protective Monitoring responsibilities;
6. Regularly review the performance for Protective Monitoring business processes and embed these within a culture of continuous improvement (performance evaluation).
7. Maintain an understanding and keep informed of threats and threat activities (threat intelligence);
8. Implement pro-active event monitoring within networks and information systems to protect against malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable);
9. Implement operational monitoring teams with roles and responsibilities that cover both security and performance related monitoring to ensure greater business benefit and multi-purpose use of the same datasets;
10. Seamlessly integrate Protective Monitoring into the Incident Management function;
11. Ensure asset management processes to ensure knowledge of assets is sufficiently detailed and accurate to efficiently trace observed events to their sources;
12. Collect, correlate, and analyse security-related information;
13. Provide actionable communication of security status across the DCC and its Service Providers;
14. Engage in continuous active management of risk;
15. Continuously monitor the security status of the networks and systems supporting the essential functions in order to detect potential security problems; and
16. Track the ongoing effectiveness of protective security measures.

Note: It is important for the Protective Monitoring Strategy to consider and ensure adequate provisions are in place to ensure the information gathered for Protective Monitoring purposes is used for correct and lawful purposes and not abused. Information obtained as part of Protective Monitoring activities may be subject to legal requirements that need to be observed especially where, information in its raw form, includes personal data.

8.4 Protective Monitoring Strategy

This Guidance requires that a Protective Monitoring Strategy is developed and maintained by the DCC where the strategy is based on business needs and an assessment of risk and covers all parts of the DCC Total System. This Protective Monitoring Strategy should form an integral part of the DCC's ISMS.

"*An effective monitoring strategy is required so that actual or attempted security breaches are discovered and there are appropriate processes in place to respond. Good monitoring is more than simply the collection of logs. It is also the use of appropriate tools and skilled analysis to identify indicators of compromise in a timely manner so that corrective action can be taken.*" – **NISD CAF Objective C.1 (developed by NCSC)**

As well as the guiding principles in Section 8.3 of this guide, the Protective Monitoring Strategy (and any supporting documentation) should also consider:

1. How the Protective Monitoring Strategy fits in to the overall DCC information security strategy;
2. The objectives of the Protective Monitoring Strategy and how it meets the overarching security requirements of the DCC;
3. The approach to Protective Monitoring and the desired outcomes;
4. How the effectiveness of the Protective Monitoring Strategy shall be monitored, measured, analysed and evaluated and the frequency of such activities;
5. The relationship between the Protective Monitoring controls and:
    a. Asset identification;
    b. The risk assessment; and
    c. Supporting threat assessments and intelligence.
6. High level requirements of what needs to be logged and monitored, in terms of:
    a. Usage scenarios of the aspect of the DCC Total System under consideration - what participants are allowed to do and which actions need to be accounted for;
    b. Exceptions and how they will be detected - what participants are not allowed to do or what would constitute suspicious activity;
    c. The complexity in terms of the different types of connectivity to support these interactions (e.g. air-gapped systems, electronic exchanges, remote access, wireless, Internet services, etc.).
    d. What information will be collected to support the accounting, logging and monitoring of these activities;
    e. How the information gathered will be used (including both a list of permitted purposes and a list of prohibited purposes);
    f. How often the information will be gathered and how often they will be reviewed and validated;
    g. Deciding on centralised or decentralised approach to logging and monitoring;
    h. Who will access it and their associated responsibilities;
    i. How the information will be protected;

j. How the information will be securely stored (including consideration of how logs are protected incl. System Administrators/Privileged Personnel);

k. How long information is retained for;

l. How information is securely disposed of;

m. How notification of monitoring is achieved and how participant consent is obtained, or otherwise; and

n. Identification of the types of events to be logged and monitored.

9 SSC Guidance 004 (replaces GPG 18) – Forensic Readiness

9.1 Business requirement

The SEC Section G2.27 (b) requires the DCC to apply Forensic Readiness Guidance provided by the SSC to system activity on DCC Systems.

Forensic Readiness is the achievement of an appropriate level of capability by an organisation for it to collect, preserve, protect and analyse Digital Evidence so that this evidence can be effectively used in any legal matters, in security investigations, in disciplinary matters, in an employment tribunal or in a court of law.

In the context of Smart Metering, Digital Evidence is any information that can be obtained from the DCC Systems and used during the course of any civil or criminal legal procedure. This extends to internal disciplinary hearings, employment tribunals, arbitration panels and all courts of law.

The DCC and its Service Providers are therefore required to develop a Forensic Readiness capability that it is matched to the business need which is enshrined in a Forensic Readiness Policy that lays down a consistent approach, detailed planning against typical (and actual) case scenarios that an organisation faces, identification of (internal or external) resources that can be deployed as part of those plans, identification of where and how the associated Digital Evidence can be gathered that will support case investigation and a process of continuous improvement that learns from experience. The guidance has been developed to ensure there is no material change between the discontinued NCSC GPG 18 and the SMKI PMA and SSC proposed guidance.

Overview of Forensic Readiness Benefits

The benefits of an effective Forensic Readiness capability are to ensure that Digital Evidence that is in computers and storage media can be collected to a standard required by the law and to:

a) support corporate governance and provide an electronic audit trail;

b) support root cause analysis of incidents or claims;

c) support information risk management and the protection of personal information;

d) detect and deter nefarious activities (by insiders or outsiders);

e) detect and deter abuse of protectively marked information;

f) be an important control in assisting:

  i) countermeasures against terrorists and criminals;

  ii) in-depth system investigations to remedy system and business performance issues;

  iii) investigation of malicious software incidents;

  iv) tracing of attackers;

  v) demonstration that staff privacy is being respected;

  vi) disclosure requests to be efficiently dealt with;

9.2 Forensic Readiness Guiding Principles

Forensic Readiness is a proactive process for effective planning to be ready for any civil or criminal legal procedure. This extends to internal disciplinary hearings, employment tribunals, arbitration plans and all courts of law. The approach has much in common with business continuity and contingency

planning and provides a measure of deterrence to potential attackers by provision of an effective investigation capability.

Forensic Readiness should adopt the following guiding principles:

1. Develop, implement and maintain a Forensic Readiness Policy that demonstrates the DCC's commitment and senior management ownership;
2. Ensure an effective records management system to enable documentary evidence to be furnished that may be relied to support any form of legal proceedings;
3. Maintain compliance with BS 10008:2008 - Legal Admissibility and Evidential Weight of Information Stored Electronically on electronic record systems when records exist only in electronic format;
4. Ensure an effective records retrieval process that can support necessary legislation e.g. GDPR, Data Protection Act, including the processing of Subject Access Requests and appropriate management of personal information;
5. Implement an adequate infrastructure that is closely integrated with information security incident management business processes, including management reporting and escalation;
6. Ensure documented processes and rules of engagement for the conduct of investigations and evidence handling that aligns with business records management and access to information requirements;
7. Ensure there are defined roles and responsibilities with clearly defined relationships between the information security management, contingency planning, legal, commercial/contract, human resource etc. functions;
8. Undertake scenario based Forensic Readiness Planning activities to prepare for and to learn from experience gained;
9. Include Forensic Readiness in the overall cycle of management review and continuous improvement;
10. Obtain independent assurance of compliance as part of wider DCC assurance regimes;
11. Track the ongoing effectiveness of Forensic Readiness measures.

9.4 Forensic Readiness Policy

Forensic Readiness Policy is a formal commitment given by the DCC that it and its Service Providers will adopt and implement the principles of Forensic Readiness adapted to the context of Smart Metering and the DCC Systems.

This Guidance requires that a Forensic Readiness Policy is developed and maintained by the DCC where that policy is based on business needs and covers all parts of the DCC Total System. This Forensic Readiness Policy should form an integral part of the DCC's ISMS.

As well as the guiding principles in Section 9.3 of this guide, the Forensic Readiness Policy (and any supporting documentation) should also consider:

1. How the Forensic Readiness Policy fits in to the overall DCC information security strategy and dependencies on e.g. security incident management, Protective Monitoring, business continuity and external Service Provider contractual arrangements;
2. How the Forensic Readiness Policy fits into the DCC's leadership management framework, corporate governance and accountability;

3. The objectives of the Forensic Readiness Policy and how it meets the overarching legal obligations of the DCC to be ready for any civil or criminal legal procedure as well as internal disciplinary hearings, employment tribunals, arbitration plans and all courts of law;
4. How Forensic Readiness fits into the DCC Information Classification Policy;
5. The procedures for handling sensitive information during investigations including how it is extracted from systems that process protectively marked data, or data with special handling caveats.
6. The arrangements and security clearance requirements for those involved in investigations and data handling requirements;
7. How capability, knowledge and awareness of Forensic Readiness will be established and maintained across the organisation(s);
8. How organisational approaches to records management, data protection and access to information will be arranged and managed;
9. How relevant standards will be adhered to e.g. BS 10008:2008 - Legal Admissibility and Evidential Weight of Information Stored Electronically; GDPR; Data Protection Act; and how records will be produced as evidence in legal proceedings if required;
10. How the effectiveness of the Forensic Readiness Policy shall be monitored, measured, analysed and evaluated and the frequency of such activities;

10. SMKI PMA & SSC Guidance 005 (supports MP259 - Acceptable Standards for TLS

10.1 Business Requirements

The Transport Layer Security (TLS) protocol is designed to prevent eavesdropping, tampering and message forgery of communication between two parties. Prior to MP259, which was implemented into the SEC in February 2024, TLS v1.2 was mandated throughout the SEC and multiple SEC Appendices as a required method of encrypting communications. However, at that time, there were later versions of TLS available and older versions can be expected to be deprecated over time and new versions to become available.

The DCC and Users should be able to use the latest or most appropriate version of TLS and MP259 removed the version numbers from the SEC and allows the SMKI PMA and SSC Guidance to be updated as appropriate to provide guidance on the current available and acceptable versions of TLS to be used. This effectively futureproofs the SEC by removing the need for repeated SEC Modifications and enables guidance to be nimble and responsive to change in standards.

10.2 SMKI PMA & SSC Guidance on TLS Versions

The SSC takes advice from NCSC. The NCSC advice is that the TLS version to be used must be in accordance with the current version of the relevant NCSC Guidance for the protocol[2]. TLS then must include client authentication; and, if being used in connection with the Triage System Interface, must be compliant with the requirements of the Triage extensions to the NCSC CPA Scheme Build Standard as defined in “CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC SCs and CPA Build Standard Extensions”.

At present, the DCC and Users should NOT use TLS v1.0 or TLS v1.1 since both of these standards have been deprecated. It is acceptable to use TLS v1.2 or TLS v1.3 and, in general it is advisable to use the latest version.

[2]See NCSC Guidance web pages ‘Using TLS to protect data’: https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data

11. SMKI PMA & SSC Guidance 006 (SHA-1)

11.1 Business Requirements

In cryptography, **SHA-1** (**Secure Hash Algorithm 1**) is a hash function which takes an input and produces a 160-bit (20-byte) hash value, typically rendered as 40 hexadecimal digits. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard. The algorithm has been cryptographically broken but is still widely used.

SHA-1 is no longer considered secure and, in 2011, NIST formally deprecated use of SHA-1 and disallowed its use for digital signatures in 2013, and declared that it should be phased out by 2030. It recommended removing SHA-1 from products as soon as possible and instead use SHA-2 or SHA-3. Replacing SHA-1 is urgent where it is used for digital signatures.

The SEC in general specifies the use of SHA-256 which is available with both SHA-2 and SHA-3 and is appropriately secure when used as the hash value associated with digital signatures.

However, the SEC Appendix AL (SMETS1 Transition and Migration Approach Document) and Appendix AM (SMETS1 Supporting Documents) specifies the use of SHA-1 for the purpose of generating a key identifier in SMETS1, where SHA-1 is used as a hash function over the public key. The SEC does NOT require SHA-1 as part of digital signature generation or code signing, which is where its use is deprecated.

GBCS also has two references which specify the use of SHA-1 in connection with the "*GBCS Certificate requirements mean that subjectKeyIdentifier attributes will all be 8 byte SHA-1 Hashes."*

11.2 SMKI PMA Guidance on use of SHA-1

In these limited situations, the increased collision risk of SHA-1 against a stronger hash function (e.g. SHA-256) does not apply as the hash output is truncated to 8 octets. There is also a limited set of public keys in use in the PKI estate (compared to e.g. messages that need a digital signature), limiting the likelihood of a collision. Therefore, there is no increased security risk by continuing to use SHA-1 for generating a key identifier going forward in the situations described in SEC Appendices AL and AM and in GBCS.

This is supported in the Security Considerations section of [RFC7093]*: "While hash algorithms provide preimage resistance, second-preimage resistance, and collision resistance, none of these properties are needed for key identifiers".* Therefore, there is no cryptographic reason to deprecate the use of SHA-1 for generating key identifiers at this stage.

There is a misconception that Devices must support SHA-1, possibly due to it being mentioned twice in GBCS in conjunction with key identifiers. However, a Device only uses the value of the key identifier as part of certification path validation and never needs to perform the SHA-1 operation on a public key to generate a key identifier.

The SMKI PMA recommendation is to follow the NIST guidance and use SHA-2 and SHA-3 wherever possible and definitely when associated with digital signatures. However, SHA-1 can continue to be used for generating key identifiers in the circumstances defined in the SEC and GBCS until advised otherwise. This requires no changes to the SEC.

In due course, it will become necessary to move away from the use of SHA-1 for key identifier generation, and the SMKI PMA will recommend that key identifier generation transitions to using a stronger hash that conforms to current lifetime recommendations, e.g. SHA2-256 or SHA3-256. The SMKI PMA will raise a SEC Modification well in advance of this being required to allow visibility and adequate time for planning and for implementing changes.

12. SMKI PMA & SSC Guidance 007 (FIPS 186-4 and FIPS 186-5)

12.1 Business Requirements

The NCSC recommends that digital signature algorithms for Critical National Infrastructure (CNI) adopt the standards set by the US National Institute for Science and Technology (NIST) and use the Federal Information Processing Standard 186 (FIPS 186).

This standard specifies a suite of algorithms that can be used to generate a digital signature which is used to detect unauthorised modifications to data and to authenticate the identity of the signatory. The recipient can also use the digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This proves non-repudiation since the signatory cannot repudiate the signature at a later time.

Smart metering and the SEC specify the **Signature Method ECDSA** (Elliptic Curve Digital Signature Algorithm) with a structure defined as per RFC 5480 (as updated by RFC 8813) and based on using the P-256 elliptic curve in conjunction with the SHA-256 secure hash algorithm.

The SEC specifies the use of FIPS 186-4 which was the relevant standard from 2013. However, this was superseded by FIPS 186-5 in February 2023 with a one-year transition period and FIPS 186-4 was withdrawn on 3 February 2024.

The significant changes in FIPS 186-5 pertaining to ECDSA are:

1. ANSI X9.62 is no longer used as a reference and the methods from ANSI X9.62 are now included; and
2. a method for deterministic ECDSA is now included.

The second change has significance for the SEC.

12.2 SMKI PMA Guidance on use of FIPS 186-5 and FIPS 186-4

The SSC and SMKI PMA take advice from NCSC. The NCSC advice in respect of FIPS 186-5 is that best practice for CNI cryptography is to follow NIST guidance and to be FIPS compliant, the latest NIST standards should be followed.

The only change in FIPS 186-5 that is significant for the SEC is the introduction of a method for deterministic ECDSA.

Deterministic ECDSA is a method that is particularly suited to devices that do not have a good source of quality random numbers. This may apply to smart metering devices. For this reason, and because earlier versions of FIPS 186 did not specify a deterministic ECDSA method, the SEC specifies its own deterministic ECDSA method and requires its use. However, the method specified in the SEC is different to the method specified in FIPS 186-5.

If strict compliance with FIPS 186-5 were required, this would incur significant changes to smart metering devices.

NCSC recognise that the risks of staying with the SEC-specified deterministic ECDSA method needs to be weighed against the risks (and costs) of updating the End-to-End Smart Metering System to use the deterministic ECDSA method specified in FIPS 186-5. Updating the End-to-End Smart Metering System to adopt changes to the creation of digital signatures is a significant specification change that must be carefully planned over a period that allows for updates to Device and Systems design.

The risk from continuing with the SEC-specified deterministic ECDSA method is considered to be low. The SEC-specified method uses an approved secure hash algorithm (SHA-256) and a method based on that used in other approved signature schemes, for example, EdDSA.

The summary is that NCSC advise that system owners follow NIST standards, but at the same time to be pragmatic and consider the risk to the system as a whole.

The SMKI PMA recommendation is to follow the NCSC advice and adopt the latest NIST standards where possible and practicable. However, the SEC-specified deterministic ECDSA method can continue to be used.