**Version AA 1.0**

# Appendix AA

# Threshold Anomaly Detection Procedures

# Table of Contents

**DEFINITIONS**

In this document, except where the context otherwise requires:

- expressions defined in section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that section; and
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below.

| | |
|---|---|
| **Anomaly Detection Thresholds File** | means a CSV file submitted by a User for the purposes of notification of ADT and Warning Thresholds to be applied by the DCC. |
| **Authorised Responsible Officer (ARO)** | means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP, SECCo or a DCC Service Provider in accordance with the SMKI RAPP. |
| **Comma Separated Values (CSV)** | means a tabular set of data records in text format in which the data fields within each data record are delimited using commas, and where data fields are not enclosed with opening and closing double quotation marks. |
| **DCC Service Management System (DSMS)** | means the Service Desk system used to manage Incidents and Service Management Service Requests. |
| **Fast-Track Notification** | means submission from a User to the DCC of an Anomaly Detection Thresholds File that is submitted with the intention of being applied in shorter timescales than standard processing timescales, where such timescales are set out in clause 3 of this document. |
| **File Signing Certificate** | means an IKI Certificate issued to a Party in accordance with the SMKI RAPP and associated with a Private Key that is used for the purposes of Digital Signing of CSV files. |
| **Interface Transaction** | has the meaning ascribed to this term in the Self Service Interface Design Specification. |

| | |
|---|---|
| **Quarantined Communications Action File** | means a CSV file submitted by a User for the purposes of notifying the DCC of the actions to be taken by DCC in respect of quarantined communications. |
| **Quarantined Communications Report File** | means a CSV file issued by the DCC to notify a User that communications have been quarantined. |
| **Senior Responsible Officer (SRO)** | means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, SECCo or a DCC Service Provider in accordance with the SMKI RAPP. |
| **Service Management Service Request (SMSR)** | means the request raised by the User to facilitate management of a Service Desk call. |
| **Warning Threshold** | in respect of a User, a number of communications within a period of time which, if exceeded, will result in the DCC notifying the User. Where both that number and the period of time are set by the User. |

# 1. Introduction

1.1. The Threshold Anomaly Detection Procedures (TADP) document makes provision for such matters as are described in Section G6.1 and G6.4 (b) (i) of the Code, and provides further processes and detail required to facilitate those matters.

# 2. DCC Anomaly Detection Threshold Guidance

2.1. Pursuant to Section G6.4 (b) of the Code, each User shall take into account any guidance issued by the DCC as to the appropriate level for their Anomaly Detection Thresholds (ADTs) giving regard to their Service Request forecast and expected pattern of demand for each Service Request.

2.2. DCC shall:

(a) provide guidance to support Users in setting appropriate ADT and Warning Thresholds;

(b) provide a template for the User to provide its ADT and Warning Thresholds in the format set out in clause 6.3 of this document; and

(c) provide the guidance and template referred to above via the Self Service Interface (SSI).

## 3. Notification of Anomaly Detection Thresholds

**User and DCC Responsibilities: ADT submissions**

3.1. Prior to sending the DCC any Anomaly Detection Thresholds File, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its submission to DCC, where such reference number will be generated by the SSI automatically.

3.2. Each User shall use reasonable steps to organise its business processes in such a manner that obviates the need for it to rely on the use of Fast-Track Notifications.

3.3. Where a User wishes to submit a Fast-Track Notification it shall, prior to doing so, contact the Service Desk and provide a justification for why it is necessary for them to do so.

3.4. A User shall, in each User Role in relation to which it is required (or elects) to set ADTs, provide an Anomaly Detection Thresholds File to the DCC via an email to the Service Desk. The email shall include:

(a) the SMSR reference number in the subject line of the email; and

(b) the Anomaly Detection Thresholds File (of the form set out in clause 6.3 of this document), Digitally Signed by a Private Key associated with a File Signing Certificate and provided to an Authorised Responsible Officer (ARO) in accordance with the SMKI RAPP.

3.5. The User shall update the SMSR corresponding to the Anomaly Detection Thresholds File submission on the SSI. On receipt of an SMSR and accompanying Anomaly Detection Thresholds File, the DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file;

(b) check that the format of the Anomaly Detection Thresholds File is correct; and

(c) for Fast-Track Notifications, assess whether the justification provided is valid.

3.6. Following the checks above the DCC shall verify that the ADT and Warning Threshold values provided are consistent with guidance issued by DCC. Where the DCC considers this not to be the case it shall contact a Senior Responsible Officer (SRO) acting on behalf of the User, by telephone using the contact details held by the DCC. The DCC shall request confirmation from the SRO as to whether the submitted Anomaly Detection Thresholds File should be applied. The SRO shall either:

(a) provide confirmation to the DCC to apply the ADT and Warning Thresholds that it has submitted in which case the DCC shall apply the ADT and Warning Thresholds included within the Anomaly Detection Thresholds File and close the relevant SMSR; or

(b) resubmit Anomaly Detection Thresholds File having had further regard to the guidance.

3.7. The DCC shall validate and process Anomaly Detection Thresholds File submissions and shall either apply the ADT and Warning Thresholds or reject the submission, in accordance with the timescales set out immediately below:

(a) for a notification of an Anomaly Detection Thresholds File that is not a Fast-Track Notification, within 72 hours of receipt of an Anomaly Detection Thresholds File by the DCC; or

(b) for a Fast-Track Notification, within 24 hours of receipt of an Anomaly Detection Thresholds File by the DCC.

3.8. Where the ADT and Warning Thresholds have been successfully applied, the DCC shall update and close the relevant SMSR. Where any of the checks outlined at clause 3.5 fail, the DCC shall not apply the ADT and Warning Thresholds and shall update the SMSR to reflect this and notify the User of the reason for the failure.

## 4. Exceeding Anomaly Detection or Warning Thresholds

**User and DCC Responsibilities: User Warning Threshold**

4.1. Where the number of communications has exceeded the Warning Threshold, the DCC shall raise an Incident and send an email notification to the User's registered contact address on the DSMS.

4.2. Following any such notification, a User shall use the "View Service Management Incident" Interface Transaction within the SSI to obtain details on the Warning Threshold exceeded using the SMSR reference number provided within the email notification.

4.3. Each User shall investigate, and then update and assign the Incident to the Service Desk using the "Update Service Management Incident" Interface Transaction within the SSI.

**User and DCC Responsibilities: User Set Anomaly Detection Threshold**

4.4. Where the DCC has quarantined communications in accordance with the Service Request Processing Document the DCC shall raise an Incident and send an email notification to the affected User's registered contact address on the DSMS to inform the User of the ADT that has been exceeded.

4.5. The DCC shall make all such quarantined communications available to Users to whom they relate to download for a period of 120 hours from the point at which the communication was quarantined. At this point the DCC will immediately initiate the automated email notification process to notify the User that the communication has been quarantined. After this 120 hour time

period has elapsed, the DCC shall archive all quarantined communications relating to the event for audit purposes and permanently delete them after 30 days. During the 30 day archive period, Users can access these archived communications only for the purposes of investigating a Major Security Incident.

4.6. Each User shall use the "View Service Management Incident" Interface Transaction within the SSI to obtain details on the ADT exceeded using the Incident reference number provided within the email notification. The User shall download a configurable report, as set out in clause 6.4 of this document, from the "reporting" Interface Transaction within the SSI, which shall include the list of quarantined communications in a CSV format.

4.7. Each User shall investigate and resolve the ADT exceeded event. Each User shall provide an email to the Service Desk indicating the action to be taken on each of the quarantined communications. The email shall include:

(a) the Incident reference number in the subject line of the email; and

(b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

4.8. Each User shall update the Incident using the "Update Service Management Incident" Interface Transaction within the SSI and assign to the Service Desk for further action. The DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and

(b) check that the format of the data is correct.

4.9. Upon successful validation of all of the above checks the DCC shall perform the actions on the quarantined communications, notify the User, update and close the Incident.

4.10. Where any of the above validation steps fail the DCC shall update the Incident, reassign it to the User and notify the User of the reason for the failure.

**User and DCC Responsibilities: DCC Set Anomaly Detection Threshold**

4.11. Pursuant to Section G6.6 of the Code the DCC shall set ADTs. Where a DCC set ADT has been exceeded, the DCC shall:

(a) quarantine the communication(s) that have exceeded the ADT;

(b) raise an Incident in accordance with the Incident Management Policy; and

(c) determine the reasons for the Incident and take appropriate remedial action.

4.12. DCC shall contact the User(s) impacted by the event by raising an Incident to notify them that their communication(s) have been quarantined. At an appropriate point during the investigation, DCC shall advise Users of the action that should be taken in respect of quarantined communications, which will be one of the following:

(a) that quarantined communications must be deleted;

(b) that the User may decide whether quarantined communications should be processed or deleted; or

(c) that no action should be taken by the User in respect of quarantined communications, which will result in the quarantined communications being archived for 30 days and subsequently deleted by the DCC.

4.13. Upon being advised of the action to be taken, Users shall submit an email and Quarantined Communications Action File which specifies actions in respect of each quarantined communication and shall, where relevant, correspond with the actions as advised by the DCC. Such email shall be submitted to the Service Desk and shall include:

(a) the DSMS Incident reference number notified in the subject line of the email; and

(b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

4.14. The DCC shall make all such quarantined communications available to Users to whom they relate to download for a period of 120 hours from the point at which the communication was quarantined. At this point the DCC will immediately initiate the automated email notification process to notify the User that the communication has been quarantined. After this 120 hour time period has elapsed, the DCC shall archive all quarantined communications relating to the event and permanently delete them after 30 days. During the 30 day archive period, Users can access these archived communications only for the purposes of investigating a Major Security Incident.

4.15. The User shall download a configurable report, as set out in clause 6.4 of this document, from the "reporting" Interface Transaction within the SSI which shall include the quarantined communications(s) in a CSV format. Each User shall update the Incident using the "Update Service Management Incident" Interface Transaction within the SSI and assign the Incident to DCC for further action. The DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and

(b) check that the format of the data is correct.

4.16. Within 24 hours of receipt of a Quarantined Communications Action File, the DCC shall validate that Quarantined Communications Action File and shall either:

(a) where the checks are successful, perform the actions on the quarantined communications and notify the User of successful completion of the notified actions once completed, via the SSI; or

(b) where the checks are unsuccessful, update and reassign the Incident and notify the User of the reason for the failure.

## 5. Exceptions Process

5.1. There are no exceptions to the process.

## 6. Communication Formats

6.1. All data sent by email for use in the DCC Systems for the purposes of these Threshold Anomaly Detection Procedures shall be in the form of a Digitally Signed CSV file. The field separator shall be a comma "," and the record separator shall be a line feed character 0x0A. In the file descriptions set out in clause 6.3 to 6.5 of this document, the character "▲" indicates the record separator. Users may include, within such CSV files, consecutive comma separators to the left of a record separator to specify that a field has a null value. DCC shall interpret consecutive commas within a record to identify a null value.

6.2. Each User submitting a CSV file that is to be Digitally Signed using the Private Key associated with a File Signing Certificate shall, prior to Digitally Signing that file, ensure that:

(a) the CSV file is formatted to ensure that each record has a separator which is a 0x0A character and that any 0x0D character is removed from the file; and

(b) the last record in the CSV file is terminated with a 0x0A character.

**Anomaly Detection Thresholds File**

6.3. Each Anomaly Detection Thresholds File shall be generated in accordance with the procedure set out immediately below.

(a) an "initial" CSV file shall be created, which shall contain the following records:

(i) UserID ▲

(ii) Service_Reference_Variant, Warning_Threshold,Quarantine_Threshold, Time_Period_Applicable, (repeated for each applicable Service Reference Variant to be used) ▲

(b) a File Signing Certificate_ID shall be appended as a record to the end of the "initial" CSV file, comprising:

(i) all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and

(ii) the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character;

(c) a Digital Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in clause 6 of this document; and

(d) where the fields are defined as follows:

(i) The UserID is the EUI-64 identifier obtained as part of the ID Allocation Procedure.

(ii) The Service Reference Variant is the number set out in the DCC User Interface Specification (DUIS) for the Service Request.

(iii) The warning threshold field shall be populated with an integer value that is greater than or equal to zero.

(iv) The quarantine threshold field shall be populated with an integer value that is greater than or equal to zero.

(v) The Time Period Applicable is populated with a number that represents the measurement interval for the threshold in minutes, which shall be an integer value that is greater than or equal to one and less than or equal to 43200.

**Quarantined Communications Report File**

6.4. Each Quarantined Communications Report File shall contain the following fields:

(a) Event_Reference, Service_Reference_Variant, Critical_Indicator, Date/time, Originator_ID, Target_ID, Counter, (repeated for each quarantined communication uploaded by the User) ▲; and

(b) where the fields are defined as follows:

(i) The Event Reference is generated by the DCC for a particular instance of an ADT or Warning Threshold being exceeded.

(ii) The Service Reference Variant is the number set out in DUIS for the Service Request.

(iii) The Critical Indicator indicates whether the Service Request is Critical or Non-Critical, which shall be set to 'C' or 'NC'.

(iv) The Date/time field is the date and time when the communication was placed in quarantine, which will be of the format *DD/MM/YYYY hh:mm:ss*.

(v) Originator ID, Target ID and Counter fields are equivalent to the "RequestID", as set out in DUIS, for each quarantined communication.

**Quarantined Communications Action File**

6.5. Each Quarantined Communications Action File shall be generated in accordance with the procedure set out immediately below.

(a) an "initial" CSV file shall be created, which shall contain the following records:

(i) UserID ▲

(ii) Event_Reference, Service_Reference_Variant, Critical_Indicator, Date/time, Originator_ID, Target_ID, Counter, Action (repeated for each quarantined communication uploaded by the User) ▲

(b) a File Signing Certificate_ID shall be appended as a record to the end of the "initial" CSV file, comprising:

(i) all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma;

(ii) the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and

(c) a Digital Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in clause 6 of this document; and

(d) where the fields are defined as follows:

(i) The UserID is the EUI-64 obtained as part of the ID Allocation Procedure.

(ii) The Event Reference is generated by the DCC for a particular instance of an ADT or Warning Threshold being exceeded.

(iii) The Service Reference Variant is the number set out in DUIS for the Service Request.

(iv) The Critical Indicator indicates whether the Service Request is Critical or Non-Critical, which shall be set to 'C' or 'NC'.

(v) The Date/time field is the date and time when the communication was placed in quarantine, which will be of the format DD/MM/YYYY hh:mm:ss.

(vi) Originator ID, Target ID and Counter fields are equivalent to the "RequestID", as set out in DUIS, for each quarantined communication.

(vii) The Action field shall be created and populated by the User for each quarantined communication with the required action, which shall have a value of "Delete" or "Release".

## 7. File Signing the "input" CSV File

7.1. An "input" CSV file will be finalised for communication by applying a Digital Signature to the end of the file.

7.2. The Private Key corresponding with the File Signing Certificate used for Digitally Signing the "input" CSV file shall be stored on a cryptographic token, supplied by the DCC in accordance with the SMKI RAPP.

7.3. Each User wishing to use the Private Key corresponding with a File Signing Certificate to apply a Digital Signature to an "input" CSV file and to append such Digital Signature record to the end of the "input" CSV file shall:

(a) Digitally Sign the content in the "input" CSV file, using a Private Key corresponding with the File Signing Certificate in accordance with the FIPS 186-4 Digital Signature Standard and using the parameters for signing as set out in clause 7.4; and

(b) convert the Digital Signature to Base64 format and append the Base64 encoded Digital Signature, as a record, to the end of the "input" file, followed by a 0x0A character, to create the "finalised" CSV file.

7.4. The parameters used for signing will be:

(a) Hashing algorithm: SHA-256, as specified in FIPS 180-4;

(b) Signing Method: The RSASSA – PKCS - v1.5 Digital Signature Algorithm specified in Section 5.5 of FIPS 186-4; and

(c) Key Length: 2048.

7.5. The DCC shall provide a software utility for the purposes of Digitally Signing files, which a User may choose to utilise in order to meet its obligations:

(a) to format such files so that the correct field separators and record separators are used;

(b) in respect of obligations to append a File Signing Certificate_ID to CSV files where required; and

(c) to Digitally Sign the "finalised" CSV file as set out in clause 7.3.