Threshold Anomaly Detection Procedures (TADP)

Contents

Formatted: Font: Arial Bold, 16 pt, Font color: Dark Blue

Formatted: Normal

1 Introduction

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

2 DCC Anomaly Detection Threshold Consultation

Pursuant to Section G6.4 (b), each User shall consult with 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.

Each User shall consult with the DCC by accessing and reviewing the information and guidance documentation provided by DCC via the Self Service Interface (SSI). The DCC shall include in such guidance documentation how to determine appropriate values for the ADTs for each relevant type of Service Request and a template for the User to provide their ADTs in the format required, as set out in Section 5.1 of this document.

3 Notification of Anomaly Detection Thresholds

3.1 User and DCC Responsibilities

3.1.1 ADT submissions

Prior to notifying the DCC of any ADT, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its ADT submission, where such reference number will be generated by the SSI automatically.

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

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

~~Users may undertake a Fast-Track Notification under the following scenarios:~~

- ~~where an ADT limit is exceeded, as set out below in Section 4 of this document; or~~
- ~~by prior agreement with the DCC.~~

~~Where a User wishes to submit a Fast-Track Notification, within 24 hours of receipt of an Anomaly Detection Thresholds File by the DCCthe User shall include within the SMSR text a justification as to the reason(s) why this should be considered as a Fast-Track Notification.~~

Pursuant with Section G6.1(a) (i), a User participating in each User Role in relation to which it is required (or elects) to set ADTs shall provide ADTs to the DCC via an email to the DCC Service Desk. The email shall include:

- the SMSR reference number in the subject line of the email; and
- the User's ADTs and their User ID in a ADT Comma Separated Variable (CSV) file (of the form set out in Section 5.1 of this document), Digitally Signed by a Private Key issued to an Authorised Responsible Officer (ARO) for the purpose of signing CSV files.

The User shall update the SMSR corresponding to the ADT submission on the SSI~~ and assign it to the DCC Service Desk~~.

~~Where a User wishes to submit a Fast-Track Notification, the User shall include within the SMSR text a justification as to the reason(s) why this should be considered as a Fast-Track Notification.~~

On receipt of an SMSR and accompanying ADTs, the DCC shall:

a) check the 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 ADT data is correct;

c) check that the ADT values provided are consistent with guidance provided by DCC; and

d) f~~F~~or Fast-Track Notifications, assess whether the justification provided is valid.

The DCC shall validate and process ADT submissions and shall either apply the ADTs or reject the submission, in accordance with the timescales set out immediately below:

- for a notification of ADTs that is not a Fast-Track Notification, within 72 hours of receipt of an Anomaly Detection Thresholds File by the DCC; or
- for a Fast-Track Notification, within 24 hours of receipt of an Anomaly Detection Thresholds File by the DCC.

~~Upon successfully carrying out all of the above checks the DCC shall apply the ADTs and update and close the SMSR.~~

Where successfully applied, the DCC shall update and close the relevant SMSR. Where any of the above checks fail, the DCC shall not apply the ADTs and shall update the SMSR to reflect this and notify the User of the reason for the failure.

Where the check identified in c) above only has failed, the User shall either:

- provide additional confirmation to DCC to apply the ADTs that it has submitted. This confirmation may only be provided by a Senior Responsible Officer (SRO) by updating and reassigning the active SMSR, and in which case the DCC shall apply the ADTs included within the ADT CSV file; or
- resubmit ADTs that are aligned with the guidance.

Formatted: Font: (Default) Calibri

Formatted: Font: 12 pt

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

3.1.2 Population of ADT values

The guidance documentation located on the SSI shall provide details of how the DCC expects ADTs to be specified and any restrictions on how ADT values may be submitted for each Service Request.

4 Threshold Anomaly Detection and Resolution

4.1 User and DCC Responsibilities

4.1.1 User Warning Threshold

Where the number of communications has exceeded the warning threshold for a User's ADT, the DCC shall raise a SMSR and send an email notification to the User's registered contact address on the DCC Service Management System (DSMS).

Following any such notification, a User shall use the View Service Request use case within SSI to obtain details on the warning threshold exceeded using the SMSR reference number provided within the email notification.

Each User shall investigate, and then update and ~~and close~~ assign the SMSR to the DCC Service Desk using the Update Service Request use case within SSI.

4.1.2 User Quarantine Threshold

Where the DCC has quarantined communications, in accordance with G6.1 (a) (ii), the DCC shall raise a SMSR and send an email notification to the affected User's registered contact address on the DSMS to inform the User of the quarantine threshold being exceeded for the User's ADT.

The DCC shall make all such quarantined communications available to Users to download for a period of 120~~96~~ hours after the quarantine threshold exceeded email notification. After this 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 period of archive, Users cannot access these ~~quarantined~~ archived communications via the SSI. Where required for the purposes of investigating a Major Security Incident, DCC shall not unreasonably withhold access to archived communications, in accordance with the Incident Management Policy.

Each User shall use the View Service Request use case within SSI to obtain details on the ADT quarantine threshold exceeded using the SMSR reference number provided within the email notification. The User shall download a configurable report, as set out in Section 5.2 of this document, from the Reporting use case within SSI, which shall include the list of quarantined communications in a CSV format.

Each User shall investigate and resolve the ADT quarantine threshold exceeded event. In accordance with G6.1 (c), each User shall provide an email to the DCC Service Desk indicating the action to be taken on each of the quarantined communications. The email shall include:

- the SMSR reference number in the subject line of the email; and

- 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 Section 5.3 of this document.

Each User shall update the SMSR using the Update Service Request use case within SSI and assign to the DCC Service Desk for further action. ~~In the case of the action for Service Requests to be released from quarantine, the User update shall include justification for the release.~~

The DCC shall:

a) check the 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.

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 SMSR.

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

4.1.3 DCC Set Quarantine Threshold

Pursuant with Section G6.6, the DCC shall set ADTs and, where a DCC set ADT has been exceeded, the DCC shall:

- quarantine the communication(s) that have exceeded the ADT; and
- investigate the reasons and take appropriate remedial action in accordance with the Incident Management Policy.

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 actions that should be taken in respect of quarantined communications, which will be one of the following:

- that quarantined communications must be deleted;
- that the User may decide whether quarantined communications should be processed or deleted; or
- that no action should be taken by the User in respect of quarantined communications, which will result in the quarantined communications being archived and subsequently deleted by the DCC.

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

- the DSMS Incident reference number notified in the subject line of the email; and
- 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 Section 5.3 of this document.

The DCC shall make all such quarantined communications available to Users to download for a period of ~~96~~ 120 hours after the quarantine threshold exceeded email notification. After this time period has elapsed, the DCC shall archive all quarantined communications relating to the event and permanently delete them after 30 days. During the period of archive, Users cannot access these archived communications via the SSI.

The User shall download a configurable report, as set out in Section 5.2 of this document, from the Reporting use case within SSI which shall include the quarantined communications(s) in a CSV format. Each User shall update the DSMS Incident using the Update Service Management Incident use case within SSI and assign in DSMS Incident to DCC for further action.

The DCC shall:

a) check the 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.

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, ~~If the checks are successful, the DCC shall~~ 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 DSMS Incident and notify the User of the reason for the failure.

~~Where any of the above steps fail the DCC shall update and reassign the DSMS Incident and notify the User of the reason for the failure.~~

Formatted: Font: Arial

Formatted: Font: (Default) Arial, 12 pt

Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 1 cm, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Font: Arial

Formatted: Font: (Default) Arial, 12

Formatted: Font: Arial

Formatted: Font: Arial

Formatted: Font: Arial

Formatted: Font: 12 pt

5 Communication Formats

All data sent by email for use in the DCC Systems for the purposes of this procedure 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 sections 5.1 to 5.3 to of this document, the character "▲" indicates the record separator.

As some spreadsheets output a carriage return line feed 0x0D0A as the record separator, the DCC shall ensure that the software utility that signs the CSV file must first normalise the file to remove any carriage return characters and to ensure that the last record in the file is terminated with a line feed character. Details of the function of the software utility are contained within section 6 of this document.

5.1 Anomaly Detection Thresholds File

Each ADT CSV file shall contain the following fields:

- UserID ▲~~,~~
- Service_Reference_Variant, ,Warning_Threshold,Quarantine_Threshold,Time_Period_Applicable, (repeated for each applicable Service Reference Variant to be used) ▲
- ~~CSV~~ File Signing Certificate_ID ▲~~,~~
- Digital_Signature ▲

Where:

- The UserID is the EUI-64 identifier obtained as part of the SEC Panel ID Allocation Procedure.
- The Service Reference Variant is the number set out in DUIS for the Service Request.
- The Warning Threshold field shall be populated with an ~~absolute number~~integer value that is greater than or equal to zero.
- The Quarantine Threshold field shall be populated with an integer value that is greater than or equal to zero~~absolute number~~.
- 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.

5.2 Quarantined Communications Report File

Each Quarantined Communications Report File shall contain the following fields:

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

Formatted: Indent: Left: 0 cm, Hanging: 1 cm

Where:

- The Event Reference is generated by the DCC for a particular instance of an ADT quarantine threshold being exceeded~~, as notified in the SSI Incident record~~.
- The Service Reference Variant is the number set out in DUIS for the Service Request.
- The Critical Indicator indicates whether the Service Request is Critical or Non-Critical, which shall be set to *C* or *NC*.

Formatted: Font: Italic

Formatted: Font: Italic

- 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*.
- Originator ID, Target ID and Counter fields are equivalent to the “RequestID”, as set out in DUIS, for each quarantined communication.

5.3 Quarantined Communications Action File

Each Quarantined Communications Action File shall contain the following fields:

- UserID
- Event_Reference,Service_Reference_Variant,Critical_Indicator,Date/time, Originator_ID,Target_ID,Counter,Action, (repeated for each quarantined communication uploaded by the User)
- CSV File Signing Certificate_ID
- Digital_Signature

Where:

- The UserID is the EUI-64 obtained as part of the SEC Panel ID Allocation Procedure.
- The Event Reference is generated by the DCC for a particular instance of an ADT quarantine threshold being exceeded.

Formatted: Font: (Default) Arial, 12

Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 1 cm, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Font: 12 pt

- The Service Reference Variant is the number set out in DUIS for the Service Request.
- The Critical Indicator indicates whether the Service Request is Critical or Non-Critical, which shall be set to '*C*' or '*NC*'.
- 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*.
- Originator ID, Target ID and Counter fields are equivalent to the "RequestID", as set out in DUIS, for each quarantined communication.
- 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 ~~flagged as either~~ 'Delete' or 'Release'.

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: (Default) Arial, 12

Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 1 cm, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Font: (Default) Arial, 12

Formatted: Font: (Default) Arial, 12

Formatted: Font: (Default) Arial, 12

Formatted: Font: (Default) Arial, 12

Formatted: Font: (Default) Arial, 12

Formatted: Font: (Default) Arial, 12

Formatted: Font: 12 pt

6 File Signing

The Private Key corresponding with the File Signing Certificate shall be stored on a cryptographic token, supplied by the DCC in accordance with the SMKI RAPP.

In all submissions of ADTs from a User to the DCC, the User shall append the ID of the File Signing Certificate to the CSV file before applying the Digital Signature.

The User shall then Digitally Sign the CSV file using a Private Key corresponding with the File Signing Certificate in accordance with the FIPS 186-4 Digital Signature Standard using SHA-256 hashing algorithm. The SHA-256 hashing algorithm shall be applied to the entire data file, including the header and the File Signing Certificate_ID. The derived hash shall be encrypted using an RSA 2048 Digital Signing Algorithm using the Private Key corresponding with the File Signing Certificate, as stored on the File Signing Token. This will result in a digital signature of 2048 bits in Octet form, which shall be converted to Base64 before appending it to the CSV file.

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 as set out immediately above. The DCC shall ensure that the software utility enables Users to:

- normalise the CSV file that the User wishes to Digitally Sign;
- attach the File Signing Certificate identifier and a linefeed character;
- apply the SHA-256 hashing algorithm;
- encrypt the derived hash as set out in this section; and
- append the Digital Signature to the file.

Formatted: Font: (Default) Arial

Formatted: List Paragraph, Indent: Left: 0 cm, Hanging: 1 cm, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: 12 pt

Appendix A Definitions

Anomaly Detection Thresholds File

means a CSV file submitted by a User for the purposes of notification of ADTs to be applied by the DCC

Comma Separated Variable (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

means the DCC Service Desk system used to manage Incidents and Service Management ~~System~~ Service Requests.

Fast-Track Notification

means notification from a User to the DCC of ADTs that are submitted with the intention of being applied in shorter timescales than standard processing timescales, where such timescales are set out in section 3.1.1 of the TADP

File Signing Certificate

means an IKI Certificate issued to a~~n~~ ~~Authorised Responsible Officer~~ Party and associated with a Private Key that is used for the purposes of Digital Signing of CSV files

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

Formatted: Font color: Text 1

Formatted: Left, Space Before: 0 pt, After: 0 pt

Formatted: Space Before: 0 pt, After: 0 pt

Formatted Table

Formatted: Font: 12 pt

Formatted: Justified, Tab stops: 2.12 cm, Left

Service Management ~~System~~ Service Request	means the request raised by the User to facilitate management of a DCC Service Desk call~~.~~

Formatted: Font color: Text 1

Formatted: Left, Space Before: 0 pt, After: 0 pt

Formatted: Space Before: 0 pt, After: 0 pt

Formatted Table