ΑΠΟΦΑΣΗ (ΕΕ) 2021/1758 ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΕΝΤΡΙΚΗΣ ΤΡΑΠΕΖΑΣ

της 21ης Σεπτεμβρίου 2021

που τροποποιεί την απόφαση ΕΚΤ/2007/7 σχετικά με τους όρους και τις προϋποθέσεις του TARGET2-ΕΚΤ (ΕΚΤ/2021/43)

Η ΕΚΤΕΛΕΣΤΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΕΝΤΡΙΚΗΣ ΤΡΑΠΕΖΑΣ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 127 παράγραφος 2, πρώτη και τέταρτη περίπτωση,

Έχοντας υπόψη το καταστατικό του Ευρωπαϊκού Συστήματος Κεντρικών Τραπεζών και της Ευρωπαϊκής Κεντρικής Τράπεζας, και ιδίως τα άρθρα 11.6, 17, 22 και 23,

Εκτιμώντας τα ακόλουθα:

(1) Στις 20 Ιουλίου 2021 το διοικητικό συμβούλιο τροποποίησε ([1]) την κατευθυντήρια γραμμή ΕΚΤ/2012/27 της Ευρωπαϊκής Κεντρικής Τράπεζας ([2]), προκειμένου: α) να διευκρινίσει ότι οι κάτοχοι ΕΛΜ του TIPS και οι κάτοχοι ΕΛΜ του T2S θα συνδέονται με το TARGET2 μέσω του Ενιαίου Διαύλου Υποδομών Αγοράς του Ευρωσυστήματος από τον Νοέμβριο του 2021 και τον Ιούνιο του 2022, αντίστοιχα· β) να αποσαφηνίσει και να επεκτείνει τους κανόνες τήρησης των απαιτήσεων ασφαλείας τερματικών σημείων του TARGET2, ώστε να διασφαλιστεί ότι το TARGET2 συνεχίζει να εξελίσσεται προς την κατεύθυνση της αντιμετώπισης απειλών κατά της ασφάλειας στον κυβερνοχώρο· γ) να επιβάλει στους κατόχους λογαριασμών ΜΠ, στους οικείους έμμεσους συμμετέχοντες και τους κατόχους προσβάσιμου BIC που έχουν προσχωρήσει στο σύστημα SCT Inst υπογράφοντας τη σύμβαση προσχώρησης στο σύστημα άμεσης μεταφοράς πίστωσης SEPA την απαίτηση να είναι και να παραμένουν διαρκώς προσβάσιμοι στην πλατφόρμα TIPS μέσω ΕΛΜ του TIPS, ώστε να διασφαλίζεται η δυνατότητα πραγματοποίησης άμεσων πληρωμών σε ολόκληρη την Ένωση· δ) να θεσπίσει διαφάνεια των όρων μεταφοράς υπολοίπων από λογαριασμούς συμμετεχόντων στο TARGET2 στους αντίστοιχους διάδοχους λογαριασμούς τους στο μελλοντικό σύστημα TARGET χάριν ασφάλειας δικαίου· και ε) να αποσαφηνίσει και να επικαιροποιήσει ορισμένες άλλες πτυχές της κατευθυντήριας γραμμής ΕΚΤ/2012/2.

(2) Με τη θέση σε εφαρμογή του έργου «T2-T2S Consolidation Project» θα καταστεί εξάλλου αναγκαίο να διασφαλιστεί η διαφάνεια των όρων μεταφοράς υπολοίπων από λογαριασμούς συμμετεχόντων στο TARGET2-ECB στους αντίστοιχους διάδοχους λογαριασμούς τους χάριν ασφάλειας δικαίου.

(3) Οι τροποποιήσεις της κατευθυντήριας γραμμής ΕΚΤ/2012/27 που επηρεάζουν τους όρους και τις προϋποθέσεις του TARGET2-ΕΚΤ θα πρέπει να αποτυπωθούν στην απόφαση ΕΚΤ/2007/7 της Ευρωπαϊκής Κεντρικής Τράπεζας ([3]).

(4) Για τους λόγους αυτούς η απόφαση ΕΚΤ/2007/7 θα πρέπει να τροποποιηθεί,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Τροποποιήσεις

Τα παραρτήματα I, II και III της απόφασης ΕΚΤ/2007/7 τροποποιούνται σύμφωνα με τα παραρτήματα της παρούσας απόφασης.

([1]) Κατευθυντήρια γραμμή (ΕΕ) 2021/1759 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 20ής Ιουλίου 2021, που τροποποιεί την κατευθυντήρια γραμμή ΕΚΤ/2012/27 σχετικά με το Διευρωπαϊκό Αυτοματοποιημένο Σύστημα Ταχείας Μεταφοράς Κεφαλαίων και Διακανονισμού σε Συνεχή Χρόνο (TARGET2) (ΕΚΤ/2021/30) (βλέπε σελίδα 45 της παρούσας Επίσημης Εφημερίδας).

([2]) Κατευθυντήρια γραμμή ΕΚΤ/2012/27 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 5ης Δεκεμβρίου 2012, σχετικά με το Διευρωπαϊκό Αυτοματοποιημένο Σύστημα Ταχείας Μεταφοράς Κεφαλαίων και Διακανονισμού σε Συνεχή Χρόνο (TARGET2) (ΕΕ L 30 της 30.1.2013, σ. 1).

([3]) Απόφαση ΕΚΤ/2007/7 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 24ης Ιουλίου 2007, σχετικά με τους όρους και τις προϋποθέσεις του TARGET2-ΕΚΤ (ΕΕ L 237 της 8.9.2007, σ. 71).

Άρθρο 2

Τελικές διατάξεις

Η παρούσα απόφαση αρχίζει να ισχύει την πέμπτη ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Εφαρμόζεται από την 21η Νοεμβρίου 2021, με εξαίρεση την παράγραφο 1 στοιχείο γ) και τις παραγράφους 7 και 9 του παραρτήματος ΙΙ, οι οποίες εφαρμόζονται από την 13η Ιουνίου 2022.

Φρανκφούρτη, 21 Σεπτεμβρίου 2021.

Η Πρόεδρος της ΕΚΤ
Christine LAGARDE

ΠΑΡΑΡΤΗΜΑ Ι

Το παράρτημα Ι της απόφασης ΕΚΤ/2007/7 τροποποιείται ως εξής:

1) το άρθρο 1 τροποποιείται ως εξής:

α) ο ορισμός «instant payment order» αντικαθίσταται από το ακόλουθο κείμενο:

«— “instant payment order” means, in line with the European Payments Council’s SEPA Instant Credit Transfer (SCT Inst) scheme, a payment instruction which can be executed 24 hours a day any calendar day of the year, with immediate or close to immediate processing and notification to the payer and includes (a) the TIPS DCA to TIPS DCA instant payment orders, (b) TIPS DCA to TIPS AS technical account instant payment orders, (c) TIPS AS technical account to TIPS DCA instant payment orders and (d) TIPS AS technical account to TIPS AS technical account instant payment orders,»·

β) παρεμβάλλονται οι ακόλουθοι ορισμοί:

«— “European Payments Council’s SEPA Instant Credit Transfer (SCT Inst) scheme” or “SCT Inst scheme” means an automated, open standards scheme providing a set of interbank rules to be complied with by SCT Inst participants, allowing payment services providers in SEPA to offer an automated, SEPA-wide euro instant credit transfer product,

— “TIPS ancillary system technical account (TIPS AS technical account)” means an account held by an ancillary system or a CB on an ancillary system’s behalf in the CB’s TARGET2 component system for use by the ancillary system for the purpose of settling instant payments in its own books,

— “TIPS DCA to TIPS AS technical account liquidity transfer order” means the instruction to transfer a specified amount of funds from a TIPS DCA to a TIPS AS technical account to fund the TIPS DCA holder’s position (or the position of another participant of the ancillary system) in the books of the ancillary system,

— “TIPS AS technical account to TIPS DCA liquidity transfer order” means the instruction to transfer a specified amount of funds from a TIPS AS technical account to a TIPS DCA to defund the TIPS DCA holder’s position (or the position of another participant of the ancillary system) in the books of the ancillary system,

— “reachable party” means an entity which: (a) holds a BIC; (b) is designated as a reachable party by a TIPS DCA holder or by an ancillary system; (c) is a correspondent, customer or branch of a TIPS DCA holder or a participant of an ancillary system, or a correspondent, customer, or branch of a participant of an ancillary system; and (d) is addressable through the TIPS Platform and is able to submit instant payment orders and receive instant payment orders either via the TIPS DCA holder or the ancillary system or, if so authorised by the TIPS DCA holder or by the ancillary system, directly.»·

γ) ο ορισμός «TIPS network service provider» διαγράφεται·

2) στην πρώτη παράγραφο του άρθρου 2 προστίθεται το ακόλουθο κείμενο:

«Appendix VII: Requirements regarding information security management and business continuity management»·

3) το άρθρο 3 τροποποιείται ως εξής:

α) στην παράγραφο 2 το σημείο (fc) αντικαθίσταται από το ακόλουθο κείμενο:

«(fc) TIPS DCA to PM liquidity transfer orders and PM to TIPS DCA liquidity transfer orders;»·

β) στην παράγραφο 2 παρεμβάλλεται το ακόλουθο στοιχείο fd):

«(fd) TIPS DCA to TIPS AS technical account liquidity transfer orders and TIPS AS technical account to TIPS DCA liquidity transfer orders; and»

γ) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts, T2S DCAs and TIPS DCAs. TARGET2 is established and functions on the basis of the SSP through which payment orders are submitted and processed and through which payments are ultimately received in the same technical manner. As far as the technical operation of the T2S DCAs is concerned, TARGET2 is technically established and functions on the basis of the T2S Platform. As far as the technical operation of the TIPS DCAs and TIPS AS technical accounts is concerned, TARGET2 is technically established and functions on the basis of the TIPS Platform.»·

4) το άρθρο 5 αντικαθίσταται από το ακόλουθο κείμενο:

«*Article 5*

Direct participants

PM account holders in TARGET2-ECB are direct participants and shall comply with the requirements set out in Article 8(1) and (2). They shall have at least one PM account with the ECB. PM account holders that have adhered to the SCT Inst scheme by signing the SEPA Instant Credit Transfer Adherence Agreement shall be and shall remain reachable in the TIPS Platform at all times, either as a TIPS DCA holder or as a reachable party via a TIPS DCA holder.»·

5) το άρθρο 22 αντικαθίσταται από το ακόλουθο κείμενο:

«*Article 22*

Security Requirements and Control Procedures

1. Participants shall implement adequate security controls to protect their systems from unauthorised access and use. Participants shall be exclusively responsible for the adequate protection of the confidentiality, integrity and availability of their systems.

2. Participants shall inform the ECB of any security-related incidents in their technical infrastructure and, where appropriate, security-related incidents that occur in the technical infrastructure of the third party providers. The ECB may request further information about the incident and, if necessary, request that the participant take appropriate measures to prevent a recurrence of such an event.

3. The ECB may impose additional security requirements, in particular with regard to cybersecurity or the prevention of fraud, on all participants and/or on participants that are considered critical by the ECB.

4. Participants shall provide the ECB with: (i) permanent access to their attestation of adherence to their chosen network service provider's endpoint security requirements, and (ii) on an annual basis the TARGET2 self-certification statement as published on the ECB's website in English.

4a. The ECB shall assess the participant's self-certification statement(s) on the participants level of compliance with each of the requirements set out in the TARGET2 self-certification requirements. These requirements are listed in Appendix VII, which in addition to the other Appendices listed in Article 2(1), shall form an integral part of these Conditions.

4b. The participant's level of compliance with the requirements of the TARGET2 self-certification shall be categorised as follows, in increasing order of severity: 'full compliance'; 'minor non-compliance'; or 'major non-compliance'. The following criteria apply: full compliance is reached where participants satisfy 100% of the requirements; minor non-compliance is where a participant satisfies less than 100% but at least 66% of the requirements and major non-compliance where a participant satisfies less than 66% of the requirements. If a participant demonstrates that a specific requirement is not applicable to it, it shall be considered as compliant with the respective requirement for the purposes of the categorisation. A participant which fails to reach 'full compliance' shall submit an action plan demonstrating how it intends to reach full compliance. The ECB shall inform the relevant supervisory authorities of the status of such participant's compliance.

4c. If the participant refuses to grant permanent access to its attestation of adherence to their chosen NSPs endpoint security requirements or does not provide the TARGET2 self-certification the participant's level of compliance shall be categorised as 'major non-compliance'.

4d. The ECB shall reassess compliance of participants on an annual basis.

4e. The ECB may impose the following measures of redress on participants whose level of compliance was assessed as minor or major non-compliance, in increasing order of severity:

(i) enhanced monitoring: the participant shall provide the ECB with a monthly report, signed by a senior executive, on their progress in addressing the non-compliance. The participant shall additionally incur a monthly penalty charge for each affected account equal to its monthly fee as set out in paragraph 1 of Appendix VI excluding the transaction fees. This measure of redress may be imposed in the event the participant receives a second consecutive assessment of minor non-compliance or an assessment of major non-compliance;

(ii) suspension: participation in TARGET2-ECB may be suspended in the circumstances described in Article 28(2)(b) and (c) of this Annex. By way of derogation from Article 28 of this Annex, the participant shall be given three months' notice of such suspension. The participant shall incur a monthly penalty charge for each suspended account of double its monthly fee as set out in paragraph 1 of Appendix VI, excluding the transaction fees. This measure of redress may be imposed in the event the participant receives a second consecutive assessment of major non-compliance;

(iii) termination: participation in TARGET2-ECB may be terminated in the circumstances described in Article 28(2)(b) and (c) of this Annex. By way of derogation from Article 28 of this Annex, the participant shall be given three months' notice of such termination. The participant shall incur an additional penalty charge of EUR 1000 for each terminated account. This measure of redress may be imposed if the participant has not addressed the major non-compliance to the satisfaction of the ECB following three months of suspension.»·

6) στο άρθρο 33 η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. Participants shall be deemed to be aware of, shall comply with, and shall be able to demonstrate that compliance to the relevant competent authorities with all obligations on them relating to legislation on data protection. They shall be deemed to be aware of, and shall comply with all obligations on them relating to legislation on prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems, in particular in terms of implementing appropriate measures concerning any payments debited or credited on their PM accounts. Participants shall ensure that they are informed about the TARGET2 network service provider's data retrieval policy prior to entering into the contractual relationship with the TARGET2 network service provider.»·

7) παρεμβάλλεται το ακόλουθο άρθρο 39a:

«*Article 39a*

Transitional provisions

1. Once the TARGET system is operational and TARGET2 has ceased operation, PM account balances shall be transferred to the account holder's corresponding successor accounts in the TARGET system.

2. The requirement that PM account holders, indirect Participants and addressable BIC holders adhering to the SCT Inst scheme be reachable in the TIPS Platform pursuant to Article 5 shall apply as of 25 February 2022.»·

8) στο προσάρτημα I το στοιχείο b) της παραγράφου 8 σημείο 4 αντικαθίσταται από το ακόλουθο κείμενο:

«(b) User-to-application mode (U2A)

U2A permits direct communication between a participant and the ICM. The information is displayed in a browser running on a PC system (SWIFT Alliance WebStation or another interface, as may be required by SWIFT). For U2A access the IT infrastructure has to be able to support cookies. Further details are described in the ICM User Handbook.»·

9) στο προσάρτημα IV το στοιχείο g) της παραγράφου 6 αντικαθίσταται από το ακόλουθο κείμενο:

«(g) for contingency processing of payment orders, participants shall provide eligible assets as collateral. During contingency processing, incoming contingency payments may be used to fund outgoing contingency payments. For the purposes of contingency processing, participants' available liquidity may not be taken into account by the ECB.»·

10) προστίθεται το ακόλουθο προσάρτημα VII:

«*Appendix VII*

Requirements regarding information security management and business continuity management

Information security management

These requirements are applicable to each participant, unless the participant demonstrates that a specific requirement is not applicable to it. In establishing the scope of application of the requirements within its infrastructure, the participant should identify the elements that are part of the Payment Transaction Chain (PTC). Specifically, the PTC starts at a Point of Entry (PoE), i.e. a system involved in the creation of transactions (e.g. workstations, front-office and back-office applications, middleware), and ends at the system responsible to send the message to SWIFT (e.g. SWIFT VPN Box) or Internet (with the latter applicable to Internet-based Access).

Requirement 1.1: Information security policy

The management shall set a clear policy direction in line with business objectives and demonstrate support for and commitment to information security through the issuance, approval and maintenance of an information security policy aiming at managing information security and cyber resilience across the organisation in terms of identification, assessment and treatment of information security and cyber resilience risks. The policy should contain at least the following sections: objectives, scope (including domains such as organisation, human resources, asset management etc.), principles and allocation of responsibilities.

Requirement 1.2: Internal organisation

An information security framework shall be established to implement the information security policy within the organisation. The management shall coordinate and review the establishment of the information security framework to ensure the implementation of the information security policy (as per Requirement 1.1) across the organisation, including the allocation of sufficient resources and assignment of security responsibilities for this purpose.

Requirement 1.3: External parties

The security of the organisation's information and information processing facilities should not be reduced by the introduction of, and/or the dependence on, an external party/parties or products/services provided by them. Any access to the organisation's information processing facilities by external parties shall be controlled. When external parties or products/services of external parties are required to access the organisation's information processing facilities, a risk assessment shall be carried out to determine the security implications and control requirements. Controls shall be agreed and defined in an agreement with each relevant external party.

Requirement 1.4: Asset management

All information assets, the business processes and the underlying information systems, such as operating systems, infrastructures, business applications, off-the-shelf products, services and user-developed applications, in the scope of the Payment Transaction Chain shall be accounted for and have a nominated owner. The responsibility for the maintenance and the operation of appropriate controls in the business processes and the related IT components to safeguard the information assets shall be assigned. Note: the owner can delegate the implementation of specific controls as appropriate, but remains accountable for the proper protection of the assets.

Requirement 1.5: Information assets classification

Information assets shall be classified in terms of their criticality to the smooth delivery of the service by the participant. The classification shall indicate the need, priorities and degree of protection required when handling the information asset in the relevant business processes and shall also take into consideration the underlying IT components. An information asset classification scheme approved by the management shall be used to define an appropriate set of protection controls throughout the information asset lifecycle (including removal and destruction of information assets) and to communicate the need for specific handling measures.

Requirement 1.6: Human resources security

Security responsibilities shall be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third party users shall be adequately screened, especially for sensitive jobs. Employees, contractors and third party users of information processing facilities shall sign an agreement on their security roles and responsibilities. An adequate level of awareness shall be ensured among all employees, contractors and third party users, and education and training in security procedures and the correct use of information processing facilities shall be provided to them to minimise possible security risks. A formal disciplinary process for handling security breaches shall be established for employees. Responsibilities shall be in place to ensure that an employee's, contractor's or third party user's exit from or transfer within the organisation is managed, and that the return of all equipment and the removal of all access rights are completed.

Requirement 1.7: Physical and environmental security

Critical or sensitive information processing facilities shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They shall be physically protected from unauthorised access, damage and interference. Access shall be granted only to individuals who fall within the scope of Requirement 1.6. Procedures and standards shall be established to protect physical media containing information assets when in transit.

Equipment shall be protected from physical and environmental threats. Protection of equipment (including equipment used off-site) and against the removal of property is necessary to reduce the risk of unauthorised access to information and to guard against loss or damage of equipment or information. Special measures may be required to protect against physical threats and to safeguard supporting facilities such as the electrical supply and cabling infrastructure.

Requirement 1.8: Operations management

Responsibilities and procedures shall be established for the management and operation of information processing facilities covering all the underlying systems in the Payment Transaction Chain end-to-end.

As regards operating procedures, including technical administration of IT systems, segregation of duties shall be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse. Where segregation of duties cannot be implemented due to documented objective reasons, compensatory controls shall be implemented following a formal risk analysis. Controls shall be established to prevent and detect the introduction of malicious code for systems in the Payment Transaction Chain. Controls shall be also established (including user awareness) to prevent, detect and remove malicious code. Mobile code shall be used only from trusted sources (e.g. signed Microsoft COM components and Java Applets). The configuration of the browser (e.g. the use of extensions and plugins) shall be strictly controlled.

Data backup and recovery policies shall be implemented by the management; those recovery policies shall include a plan of the restoration process which is tested at regular intervals at least annually.

Systems that are critical for the security of payments shall be monitored and events relevant to information security shall be recorded. Operator logs shall be used to ensure that information system problems are identified. Operator logs shall be regularly reviewed on a sample basis, based on the criticality of the operations. System monitoring shall be used to check the effectiveness of controls which are identified as critical for the security of payments and to verify conformity to an access policy model.

Exchanges of information between organisations shall be based on a formal exchange policy, carried out in line with exchange agreements among the involved parties and shall be compliant with any relevant legislation. Third party software components employed in the exchange of information with TARGET2 (like software received from a Service Bureau in scenario 2 of the scope section of the TARGET2 self-certification arrangement document) must be used under a formal agreement with the third party.

Requirement 1.9: Access control

Access to information assets shall be justified on the basis of business requirements (need-to-know ([1])) and according to the established framework of corporate policies (including the information security policy). Clear access control rules shall be defined based on the principle of least privilege ([2]) to reflect closely the needs of the corresponding business and IT processes. Where relevant (e.g. for backup management) logical access control should be consistent with physical access control unless there are adequate compensatory controls in place (e.g. encryption, personal data anonymisation).

Formal and documented procedures shall be in place to control the allocation of access rights to information systems and services that fall within the scope of the Payment Transaction Chain. The procedures shall cover all stages in the lifecycle of user access, from the initial registration of new users to the final deregistration of users that no longer require access.

Special attention shall be given, where appropriate, to the allocation of access rights of such criticality that the abuse of those access rights could lead to a severe adverse impact on the operations of the participant (e.g. access rights allowing system administration, override of system controls, direct access to business data).

Appropriate controls shall be put in place to identify, authenticate and authorise users at specific points in the organisation's network, e.g. for local and remote access to systems in the Payment Transaction Chain. Personal accounts shall not be shared in order to ensure accountability.

For passwords, rules shall be established and enforced by specific controls to ensure that passwords cannot be easily guessed, e.g. complexity rules and limited-time validity. A safe password recovery and/or reset protocol shall be established.

A policy shall be developed and implemented on the use of cryptographic controls to protect the confidentiality, authenticity and integrity of information. A key management policy shall be established to support the use of cryptographic controls.

There shall be policy for viewing confidential information on screen or in print (e.g. a clear screen, a clear desk policy) to reduce the risk of unauthorised access.

When working remotely, the risks of working in an unprotected environment shall be considered and appropriate technical and organisational controls shall be applied.

Requirement 1.10: Information systems acquisition, development and maintenance

Security requirements shall be identified and agreed prior to the development and/or implementation of information systems.

Appropriate controls shall be built into applications, including user-developed applications, to ensure correct processing. These controls shall include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls shall be determined on the basis of security requirements and risk assessment according to the established policies (e.g. information security policy, cryptographic control policy).

([1]) The need-to-know principle refers to the identification of the set of information that an individual needs access to in order to carry out her/his duties.

([2]) The principle of least privilege refers to tailoring a subject's access profile to an IT system in order to match the corresponding business role.

The operational requirements of new systems shall be established, documented and tested prior to their acceptance and use. As regards network security, appropriate controls, including segmentation and secure management, should be implemented based on the criticality of data flows and the level of risk of the network zones in the organisation. There shall be specific controls to protect sensitive information passing over public networks.

Access to system files and program source code shall be controlled and IT projects and support activities conducted in a secure manner. Care shall be taken to avoid exposure of sensitive data in test environments. Project and support environments shall be strictly controlled. Deployment of changes in production shall be strictly controlled. A risk assessment of the major changes to be deployed in production shall be conducted.

Regular security testing activities of systems in production shall also be conducted according to a predefined plan based on the outcome of a risk assessment, and security testing shall include, at least, vulnerability assessments. All of the shortcomings highlighted during the security testing activities shall be assessed and action plans to close any identified gap shall be prepared and followed up in a timely fashion.

Requirement 1.11: Information security in supplier ([3]) relationships

To ensure protection of the participant's internal information systems that are accessible by suppliers, information security requirements for mitigating the risks associated with supplier's access shall be documented and formally agreed upon with the supplier.

Requirement 1.12: Management of information security incidents and improvements

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses, roles, responsibilities and procedures, at business and technical level, shall be established and tested to ensure a quick, effective and orderly and safely recover from information security incidents including scenarios related to a cyber-related cause (e.g. a fraud pursued by an external attacker or by an insider). Personnel involved in these procedures shall be adequately trained.

Requirement 1.13: Technical compliance review

A participant's internal information systems (e.g. back office systems, internal networks and external network connectivity) shall be regularly assessed for compliance with the organisation's established framework of policies (e.g. information security policy, cryptographic control policy).

Requirement 1.14: Virtualisation

Guest virtual machines shall comply with all the security controls that are set for physical hardware and systems (e.g. hardening, logging). Controls relating to hypervisors must include: hardening of the hypervisor and the hosting operating system, regular patching, strict separation of different environments (e.g. production and development). Centralised management, logging and monitoring as well as managing of access rights, in particular for high privileged accounts, shall be implemented based on a risk assessment. Guest virtual machines managed by the same hypervisor shall have a similar risk profile.

Requirement 1.15: Cloud computing

The usage of public and/or hybrid cloud solutions in the Payment Transaction Chain must be based on a formal risk assessment, taking into account the technical controls and the contractual clauses related to the cloud solution.

([3]) A supplier in the context of this exercise should be understood as any third party (and its personnel) which is under contract (agreement), with the institution, to provide a service and under the service agreement the third party (and its personnel) is granted access, either remotely or on-site, to information and/or information systems and/or information processing facilities of the institution in scope or associated to the scope covered under the exercise of the TARGET2 self-certification.

If hybrid cloud solutions are used, it is understood that the criticality level of the overall system is the highest one of the connected systems. All on-premises components of the hybrid solutions must be segregated from the other on-premises systems.

Business continuity management (applicable only to critical participants)

The following requirements (2.1 to 2.6) relate to business continuity management. Each TARGET2 participant classified by the Eurosystem as being critical for the smooth functioning of the TARGET2 system shall have a business continuity strategy in place comprising the following elements.

Requirement 2.1: Business continuity plans shall be developed and procedures for maintaining them are in place.

Requirement 2.2: An alternate operational site shall be available.

Requirement 2.3: The risk profile of the alternate site shall be different from that of the primary site, in order to avoid that both sites are affected by the same event at the same time. For example, the alternate site shall be on a different power grid and central telecommunication circuit from those of the primary business location.

Requirement 2.4: In the event of a major operational disruption rendering the primary site inaccessible and/or critical staff unavailable, the critical participant shall be able to resume normal operations from the alternate site, where it shall be possible to properly close the business day and open the following business day(s).

Requirement 2.5: Procedures shall be in place to ensure that the processing of transactions is resumed from the alternate site within a reasonable timeframe after the initial disruption of service and commensurate to the criticality of the business that was disrupted.

Requirement 2.6: The ability to cope with operational disruptions shall be tested at least once a year and critical staff shall be appropriately trained. The maximum period between tests shall not exceed one year.»

.

ΠΑΡΑΡΤΗΜΑ II

Το παράρτημα II της απόφασης ΕΚΤ/2007/7 τροποποιείται ως εξής:

1) το άρθρο 1 τροποποιείται ως εξής:

α) ο ορισμός «instant payment order» αντικαθίσταται από το ακόλουθο κείμενο:

«— “instant payment order” means, in line with the European Payments Council’s SEPA Instant Credit Transfer (SCT Inst) scheme, a payment instruction which can be executed 24 hours a day any calendar day of the year, with immediate or close to immediate processing and notification to the payer and includes (i) the TIPS DCA to TIPS DCA instant payment orders, (ii) TIPS DCA to TIPS AS technical account instant payment orders, (iii) TIPS AS technical account to TIPS DCA instant payment orders and (iv) TIPS AS technical account to TIPS AS technical account instant payment orders,»·

β) παρεμβάλλονται οι ακόλουθοι ορισμοί:

«— “TIPS ancillary system technical account (TIPS AS technical account)” means an account held by an ancillary system or a CB on an ancillary system’s behalf in the CB’s TARGET2 component system for use by the ancillary system for the purpose of settling instant payments in its own books,

— “TIPS DCA to TIPS AS technical account liquidity transfer order” means the instruction to transfer a specified amount of funds from a TIPS DCA to a TIPS AS technical account to fund the TIPS DCA holder’s position (or the position of another participant of the ancillary system) in the books of the ancillary system,

— “TIPS AS technical account to TIPS DCA liquidity transfer order” means the instruction to transfer a specified amount of funds from a TIPS AS technical account to a TIPS DCA to defund the TIPS DCA holder’s position (or the position of another participant of the ancillary system) in the books of the ancillary system,

— “Network Service Provider (NSP)” means an undertaking that has been awarded a concession with the Eurosystem to provide connectivity services via the Eurosystem Single Market Infrastructure Gateway.»·

γ) ο ορισμός «T2S network service provider» διαγράφεται·

2) στο άρθρο 4 παράγραφος 2 το στοιχείο (fc) αντικαθίσταται από το ακόλουθο κείμενο:

«(fc) TIPS DCA to PM liquidity transfer orders and PM to TIPS DCA liquidity transfer orders;»·

3) στο άρθρο 4 παράγραφος 2 προστίθεται το ακόλουθο στοιχείο (fd):

«(fd) TIPS DCA to TIPS AS technical account liquidity transfer orders and TIPS AS technical account to TIPS DCA liquidity transfer orders; and»·

4) στο άρθρο 4 η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts, T2S DCAs and TIPS DCAs. TARGET2 is established and functions on the basis of the SSP through which payment orders are submitted and processed and through which payments are ultimately received in the same technical manner. As far as the technical operation of the T2S DCAs is concerned, TARGET2 is technically established and functions on the basis of the T2S Platform. As far as the technical operation of the TIPS DCAs and TIPS AS technical accounts is concerned, TARGET2 is technically established and functions on the basis of the TIPS Platform. The ECB is the provider of services under these Conditions. Acts and omissions of the SSP-providing NCBs and the 4CBs shall be considered acts and omissions of the ECB, for which it shall assume liability in accordance with Article 21 of this Annex. Participation pursuant to these Conditions shall not create a contractual relationship between T2S DCA holders and the SSP-providing NCBs or the 4CBs when any of the latter acts in that capacity. Instructions, messages or information which a T2S DCA holder receives from, or sends to, the SSP or T2S Platform in relation to the services provided under these Conditions are deemed to be received from, or sent to, the ECB.»·

5) στο άρθρο 8 η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. Where the ECB has granted a request by a T2S DCA holder pursuant to paragraph 1, that T2S DCA holder is deemed to have given the participating CSD(s) a mandate to debit the T2S DCA with the amounts relating to securities transactions executed on those securities accounts.»·

6) στο άρθρο 28 η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. T2S DCA holders shall be deemed to be aware of, shall comply with, and shall be able to demonstrate that compliance to the relevant competent authorities with all obligations on them relating to legislation on data protection. They shall be deemed to be aware of, and shall comply with all obligations on them relating to legislation on prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems, in particular in terms of implementing appropriate measures concerning any payments debited or credited on their T2S DCAs. Prior to entering into the contractual relationship with its T2S network service provider, T2S DCA holders shall ensure that they are informed about its data retrieval policy.»·

7) το άρθρο 30 αντικαθίσταται από το ακόλουθο κείμενο:

«*Article 30*

Contractual relationship with an NSP

1. T2S DCA holders shall either:

(a) have concluded a contract with an NSP within the framework of the concession contract with that NSP in order to establish a technical connection to TARGET2- ECB; or

(b) connect via another entity which has concluded a contract with an NSP within the framework of the concession contract with that NSP.

2. The legal relationship between a T2S DCA holder and the NSP shall be exclusively governed by the terms and conditions of the separate contract concluded with an NSP as referred to in paragraph 1(a).

3. The services to be provided by the NSP shall not form part of the services to be performed by the ECB in respect of TARGET2.

4. The ECB shall not be liable for any acts, errors or omissions of the NSP (including its directors, staff and subcontractors), or for any acts, errors or omissions of third parties selected by participants to gain access to the NSP's network.»·

8) παρεμβάλλεται άρθρο 34a ως εξής:

«*Article 34a*

Transitional provisions

Once the TARGET system is operational and TARGET2 has ceased operation, T2S DCA holders shall become T2S DCA holders in the TARGET system.»·

9) Οι αναφορές στον όρο «T2S network service provider» (στον ενικό ή πληθυντικό) στα άρθρα 6 παράγραφος (1) στοιχείο (a) σημείο (i), 9 παράγραφος (5), 10 παράγραφος (6), 14 παράγραφος (1) στοιχείο (a), 22 παράγραφος (1), 22 παράγραφος (2), 22 παράγραφος (3), 27 παράγραφος (5), 28 παράγραφος (1), 29 παράγραφος (1) του παραρτήματος II και η παράγραφος 1 του προσαρτήματος I αντικαθίστανται από αναφορές σε «NSP»·

10) στο προσάρτημα I το στοιχείο (b) της παραγράφου 8 σημείο 4 αντικαθίσταται από το ακόλουθο κείμενο:

«(b) User-to-application mode (U2A)

U2A permits direct communication between a T2S DCA holder and the T2S GUI. The information is displayed in a browser running on a PC system. For U2A access the IT infrastructure has to be able to support cookies. Further details are described in the T2S User Handbook.».

ΠΑΡΑΡΤΗΜΑ III

Το παράρτημα III της απόφασης ΕΚΤ/2007/7 τροποποιείται ως εξής:

1) Οι αναφορές στον όρο «TIPS network service provider» (στον ενικό ή πληθυντικό) στο παρόν παράρτημα αντικαθίστανται από αναφορές στον όρο «NSP»·

2) το άρθρο 1 τροποποιείται ως εξής:

α) ο ορισμός «reachable party» αντικαθίσταται από το ακόλουθο κείμενο:

«— "reachable party" means an entity which: (a) holds a BIC, (b) is designated as a reachable party by a TIPS DCA holder or by an ancillary system; (c) is a correspondent, customer or branch of a TIPS DCA holder or a participant of an ancillary system or a correspondent, customer or branch of a participant of an ancillary system; and (d) is addressable through the TIPS Platform and is able to submit instant payment orders and receive instant payment orders either via the TIPS DCA holder or the ancillary system or, if so authorised by the TIPS DCA holder or by the ancillary system, directly,»·

β) ο ορισμός «payment order» αντικαθίσταται από το ακόλουθο κείμενο:

«— "payment order", except where used in Articles 16 to 18 of this Annex, means an instant payment order, a positive recall answer, a PM to TIPS DCA liquidity transfer order, a TIPS DCA to PM liquidity transfer order, a TIPS AS technical account to TIPS DCA liquidity transfer order or a TIPS DCA to TIPS AS technical account liquidity transfer order,»·

γ) ο ορισμός «instant payment order» αντικαθίσταται από το ακόλουθο κείμενο:

«— "instant payment order" means, in line with the European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme, a payment instruction which can be executed 24 hours a day any calendar day of the year, with immediate or close to immediate processing and notification to the payer and includes (a) TIPS DCA to TIPS DCA instant payment orders, (b) TIPS DCA to TIPS AS technical account instant payment orders, (c) TIPS AS technical account to TIPS DCA instant payment orders and (d) TIPS AS technical account to TIPS AS technical account instant payment orders,»·

δ) παρεμβάλλονται οι ακόλουθοι ορισμοί:

«— "TIPS ancillary system technical account (TIPS AS technical account)" means an account held by an ancillary system or the CB on an ancillary system's behalf in the CB's TARGET2 component system for use by that ancillary system for the purpose of settling instant payments in its own books,

— "TIPS DCA to TIPS AS technical account liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS DCA to a TIPS AS technical account to fund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system,

— "TIPS AS technical account to TIPS DCA liquidity transfer order" means the instruction to transfer a specified amount of funds from a TIPS AS technical account to a TIPS DCA to defund the TIPS DCA holder's position (or the position of another participant of the ancillary system) in the books of the ancillary system,

— "European Payments Council's SEPA Instant Credit Transfer (SCT Inst) scheme" or "SCT Inst scheme" means an automated, open standards scheme providing a set of interbank rules to be complied with by SCT Inst participants, allowing payment services providers in SEPA to offer an automated, SEPA-wide euro instant credit transfer product,

— "mobile proxy look-up (MPL) service" means a service which enables TIPS DCA holders, ancillary systems using TIPS AS technical accounts and reachable parties, who receive from their customers a request to execute an instant payment order in favour of a beneficiary identified with a proxy (e.g. a mobile number), to retrieve from the central MPL repository the corresponding beneficiary IBAN and the BIC to be used to credit the relevant account in TIPS,

— "Network Service Provider (NSP)" means an undertaking that has been awarded a concession with the Eurosystem to provide connectivity services via the Eurosystem Single Market Infrastructure Gateway,

— "IBAN" means the international bank account number which uniquely identifies an individual account at a specific financial institution in a particular country.»·

ε) ο ορισμός «TIPS network service provider» διαγράφεται·

3) στο άρθρο 3 παράγραφος 1 η αναφορά στο «Appendix V: TIPS connectivity technical requirements» διαγράφεται·

4) το άρθρο 4 τροποποιείται ως εξής:

α) στην παράγραφο 2 προστίθεται το ακόλουθο στοιχείο (k):

«(k) TIPS DCA to TIPS AS technical account liquidity transfer orders and TIPS AS technical account to TIPS DCA liquidity transfer orders; and»·

β) η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«3. TARGET2 provides real-time gross settlement for payments in euro, with settlement in central bank money across PM accounts, T2S DCAs and TIPS DCAs. TARGET2 is established and functions on the basis of the SSP through which payment orders are submitted and processed and through which payments are ultimately received in the same technical manner. As far as the technical operation of the TIPS DCAs and TIPS AS technical accounts is concerned, TARGET2 is technically established and functions on the basis of the TIPS Platform. As far as the technical operation of the T2S DCAs is concerned, TARGET2 is technically established and functions on the basis of the T2S Platform.»·

5) το άρθρο 6 παράγραφος 1 στοιχείο (a) σημείο (i) αντικαθίσταται από το ακόλουθο κείμενο:

«(i) install, manage, operate and monitor and ensure the security of the necessary IT infrastructure to connect to the TIPS Platform and submit payment orders to it. In doing so, applicant TIPS DCA holders may involve third parties, but retain sole liability. In particular, unless an instructing party is used, applicant TIPS DCA holders shall enter into an agreement with one or more NSPs to obtain the necessary connection and admissions, in accordance with the technical specifications in Appendix I; and»·

6) το άρθρο 9 αντικαθίσταται από το ακόλουθο κείμενο:

«*Article 9*

Contractual relationship with an NSP

1. Participants shall either:

(a) conclude a contract with an NSP within the framework of the concession contract with that NSP in order to establish a technical connection to TARGET2-ECB; or

(b) connect via another entity which has concluded a contract with an NSP within the framework of the concession contract with that NSP.

2. The legal relationship between a participant and the NSP shall be exclusively governed by the terms and conditions of their separate contract as referred to in paragraph 1(a).

3. The services to be provided by the NSP shall not form part of the services to be performed by the ECB in respect of TARGET2.

4. The ECB shall not be liable for any acts, errors or omissions by the NSP (including its directors, staff and subcontractors), or for any acts, errors or omissions by third parties selected by participants to gain access to the NSP's network.»·

7) το άρθρο 10 διαγράφεται•

8) παρεμβάλλεται άρθρο 11a ως εξής:

«*Article 11a*

MPL repository

1. The central MPL repository contains the proxy – IBAN mapping table for the purposes of the MPL service.

2. Each proxy may be linked to only one IBAN. An IBAN may be linked to one or multiple proxies.

3. Article 29 shall apply to the data contained in the MPL repository.»·

9) το άρθρο 12 παράγραφος 9 διαγράφεται.

10) το άρθρο 16 αντικαθίσταται από το ακόλουθο κείμενο:

«*Article 16*

Types of payment orders in TIPS DCA

The following are classified as payment orders for the purposes of the TIPS service:

(a) instant payment orders;

(b) positive recall answers;

(c) TIPS DCA to PM liquidity transfer orders;

(d) TIPS DCA to TIPS AS technical account liquidity transfer orders; and

(e) TIPS AS technical account to TIPS DCA liquidity transfer orders.»·

11) στο άρθρο 18 η παράγραφος 6 αντικαθίσταται από το ακόλουθο κείμενο:

«6. After a TIPS DCA to PM liquidity transfer order, a TIPS DCA to TIPS AS technical account liquidity transfer order or a TIPS AS technical account to TIPS DCA liquidity transfer order has been accepted as referred to in Article 17, the TARGET2-ECB shall check whether sufficient funds are available on the payer's account. If sufficient funds are not available the liquidity transfer order shall be rejected. If sufficient funds are available the liquidity transfer order shall be settled immediately.»·

12) το άρθρο 20 παράγραφος 1 στοιχείο (b) αντικαθίσταται από το ακόλουθο κείμενο:

«(b) TIPS DCA to PM liquidity transfer orders, positive recall answers and TIPS DCA to TIPS AS technical account liquidity transfer orders are deemed entered into TARGET2-ECB and irrevocable at the moment that the relevant TIPS DCA is debited. TIPS AS technical account to TIPS DCA liquidity transfer orders are deemed entered into TARGET2-ECB and irrevocable at the moment that the relevant TIPS AS technical account is debited.»·

13) στο άρθρο 30 η παράγραφος 1 αντικαθίσταται από το ακόλουθο κείμενο:

«1. TIPS DCA holders shall be deemed to be aware of, shall comply with and shall be able to demonstrate that compliance to the relevant competent authorities with all obligations on them relating to legislation on data protection. They shall be deemed to be aware of, and shall comply with all obligations on them relating to legislation on prevention of money laundering and the financing of terrorism, proliferation-sensitive nuclear activities and the development of nuclear weapons delivery systems, in particular in terms of implementing appropriate measures concerning any payments debited or credited on their TIPS DCAs. TIPS DCA holders ensure that they are informed about their chosen NSP's data retrieval policy prior to entering into a contractual relationship with that NSP.»·

14) παρεμβάλλεται άρθρο 35a ως εξής:

«*Article 35a*

Transitional provision

Once the TARGET system is operational and the TARGET2 has ceased operation, TIPS DCA holders shall become TIPS DCA holders in the TARGET system.»·

15) στο προσάρτημα I ο πίνακας της παραγράφου 2 αντικαθίσταται από το ακόλουθο κείμενο:

«Message Type	Message Name
Pacs.002	FIToFIPayment Status Report
Pacs.004	PaymentReturn
Pacs.008	FIToFICustomerCreditTransfer
Pacs.028	FIToFIPaymentStatusRequest
camt.003	GetAccount
camt.004	ReturnAccount
camt.005	GetTransaction
camt.006	ReturnTransaction
camt.011	ModifyLimit
camt.019	ReturnBusinessDayInformation
camt.025	Receipt
camt.029	ResolutionOfInvestigation
camt.050	LiquidityCreditTransfer
camt.052	BankToCustomerAccountReport
camt.053	BankToCustomerStatement
camt.054	BankToCustomerDebitCreditNotification
camt.056	FIToFIPaymentCancellationRequest
acmt.010	AccountRequestAcknowledgement
acmt.011	AccountRequestRejection
acmt.015	AccountExcludedMandateMaintenanceRequest
reda.016	PartyStatusAdviceV01
reda.022	PartyModificationRequestV01»

16) στο προσάρτημα I το στοιχείο (b) της παραγράφου 6 σημείο 1 αντικαθίσταται από το ακόλουθο κείμενο:

«(b) User-to-application mode (U2A)

U2A permits direct communication between a TIPS DCA holder and the TIPS GUI. The information is displayed in a browser running on a PC system. For U2A access the IT infrastructure has to be able to support cookies. Further details are described in the TIPS User Handbook.»·

17) στο προσάρτημα IV η παράγραφος 2 διαγράφεται·

18) το προσάρτημα V διαγράφεται.