In.Te.S.A. S.p.A.

Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης

Εγχειρίδιο λειτουργίας για τις διαδικασίες εγκεκριμένης ηλεκτρονικής υπογραφής εξ αποστάσεως σε πλαίσιο τραπεζικών και χρηματοπιστωτικών υπηρεσιών

Κωδικός εγγράφου: MO_REMBAN
OID: 1.3.76.21.1.50.110
Σύνταξη: Antonio Raia
Έγκριση: Franco Tafini
Ημερομηνία έκδοσης: 01/07/2019
Αρ. έκδοσης: 04

Υπεγράφη από:
ANTONIO RAIA
Οργανισμός: IN.TE.S.A. S.p.A.

An IBM Company
intesa
DIGITAL
BUSINESS SOLUTIONS

ΕΚΔΟΣΕΙΣ

Αρ. έκδοσης: 04		***Ημερομηνία Αναθεώρησης:***	***01/07/2019***
Περιγραφή αλλαγών:	Μεταβολή δεδομένων εταιρείας και λογότυπου Ενημέρωση ορισμών και κανονιστικών αναφορών Ενημέρωση διάταξης γραφικών Εισαγωγή διαδικασίας υπογραφής για Πελάτες Prospect (I.2.3)		
Λόγοι:	Ενημερώσεις κανονιστικών ρυθμίσεων: Κανονισμός (ΕΕ) 910/2014 (eIDAS), Ν.Δ. 179/2016 (ΓΚΠΔ) Οργανωτικές μεταβολές του TSP Νέα διαδικασία για την απόκτηση πελατών		
Αρ. έκδοσης: 03		***Ημερομηνία Αναθεώρησης:***	***13/06/2012***
Περιγραφή αλλαγών:	Επέκταση του εγχειριδίου για τον χρηματοπιστωτικό τομέα (Ιδρύματα πληρωμών) καθώς και τον τραπεζικό τομέα		
Λόγοι:	Ενημέρωση		
Αρ. έκδοσης: 02		***Ημερομηνία Αναθεώρησης:***	***02/04/2012***
Περιγραφή αλλαγών:	Β.4.2. - Εισαγωγή του συστήματος αναγνώρισης ταυτότητας του Κατόχου (επαρκής επαλήθευση) χωρίς τη φυσική παρουσία του ίδιου C.5. - Εισήχθησαν τρόποι λειτουργίας του συστήματος αναγνώρισης ταυτότητας του Κατόχου (επαρκής επαλήθευση) F.1.3. - Εισήχθη όριο τυποποιημένης χρήσης Z. - Εισήχθη τρόπος επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου για τις λειτουργικές επιβεβαιώσεις		
Λόγοι:	Ενημέρωση		
Αρ. έκδοσης: 01		***Ημερομηνία Αναθεώρησης:***	***01/11/2011***
Περιγραφή αλλαγών:	καμία		
Λόγοι:	πρώτη κυκλοφορία		

Περιεχόμενα

Νομικές παραπομπές

Testo Unico [Κωδικοποιημένο κείμενο] – Π. Δ. 445/00 και επακόλουθες τροποποιήσεις και ενσωματώσεις	Διάταγμα του Προέδρου της Δημοκρατίας της 28ης Δεκεμβρίου 2000, αρ. 445. *"Κωδικοποιημένο κείμενο νομοθετικών και κανονιστικών διατάξεων για θέματα διοικητικής τεκμηρίωσης*". Στο εξής αναφέρεται επίσης μόνο ως *TU*.
CAD - DLGS [Ν.Δ.] 82/05 και επακόλουθες τροποποιήσεις και ενσωματώσεις	Νομοθετικό διάταγμα 7 Μαρτίου 2005, αρ. 82. "*Κώδικας Ψηφιακής Διαχείρισης*". Στο εξής αναφέρεται επίσης μόνο ως *CAD*.
DPCM [ΔΠΥΣ] 22/02/2013 *Νέοι Τεχνικοί Κανόνες* και επακόλουθες τροποποιήσεις και ενσωματώσεις	Διάταγμα του Προέδρου του Υπουργικού Συμβουλίου 22 Φεβρουαρίου 2013 *"Τεχνικοί κανόνες για τη δημιουργία, τοποθέτηση και επαλήθευση προηγμένων, εγκεκριμένων και ψηφιακών ηλεκτρονικών υπογραφών, σύμφωνα με τα άρθρα 20 εδάφιο 3, 24 εδάφιο 4, 28 εδάφιο 3, 32 εδάφιο 3 γράμμα β), 35 εδάφιο 2, 36 εδάφιο 2 και 71 "(του CAD, σημείωση του συντάκτη).* Στο εξής αναφέρεται επίσης μόνο ως *DPCM.*
Κανονισμός (ΕΕ) αριθ. 910/2014 (eIDAS) και επακόλουθες τροποποιήσεις και ενσωματώσεις	Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2104, σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά που καταργεί την οδηγία 1999/93/ΕΚ. Στο εξής αναφέρεται επίσης μόνο ως *Καν. eIDAS.*
GDPR [ΓΚΠΔ] Γενικός Κανονισμός για την Προστασία Δεδομένων και επακόλουθες τροποποιήσεις και ενσωματώσεις	ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων όσον αφορά την επεξεργασία των προσωπικών δεδομένων, καθώς και την ελεύθερη κυκλοφορία των δεδομένων αυτών, η οποία καταργεί την οδηγία 95/46/ΕΚ (γενικός κανονισμός για την προστασία δεδομένων) Στο εξής αναφέρεται επίσης μόνο ως *ΓΚΠΔ.*
ΠΡΟΣΔΙΟΡΙΣΜΟΣ Ν. 147/2019 και επακόλουθες τροποποιήσεις και ενσωματώσεις	Κατευθυντήριες γραμμές που περιέχουν τους «Τεχνικούς Κανόνες και Συστάσεις σχετικά με τη δημιουργία εγκεκριμένων ηλεκτρονικών πιστοποιητικών, εγκεκριμένων ηλεκτρονικών υπογραφών και σφραγίδων και εγκεκριμένων ηλεκτρονικών χρονοσφραγίδων». Στο εξής αναφέρεται επίσης μόνο ως *ΠΡΟΣΔΙΟΡΙΣΜΟΣ.*

Ορισμοί και ακρωνύμια

AgID	*Ιταλική Υπηρεσία για την Ψηφιακή Τεχνολογία* (πρώην CNIPA και DigitPA) - www.agid.gov.it. Εποπτικό όργανο σύμφωνα με τον Κανονισμό ΕΕ 910/2014 (eIDAS). Στο εξής επίσης μόνο ως η *Υπηρεσία*.
QTSP Qualified Trust Service Provider. Διαπιστευμένος Φορέας Πιστοποίησης	*Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης*. Φυσικό ή νομικό πρόσωπο που παρέχει μία ή περισσότερες εγκεκριμένες υπηρεσίες εμπιστοσύνης. Πρώην *Διαπιστευμένος Φορέας Πιστοποίησης*, σύμφωνα με τον CAD. Σε αυτό το έγγραφο είναι η QTSP In.Te.S.A. S.p.A.
Εγκεκριμένη Υπηρεσία Εμπιστοσύνης	Ηλεκτρονική υπηρεσία που παρέχεται από έναν QTSP και αποτελείται από τα στοιχεία που αναφέρονται στο άρθρο 3, σημεία 16) και 17) του Καν. ΕΕ 910/2014 (eIDAS). Στο παρόν έγγραφο είναι η QTSP In.Te.S.A. SpA που παρέχει εγκεκριμένες υπηρεσίες ηλεκτρονικής υπογραφής και ηλεκτρονικής χρονοσφραγίδας και άλλες υπηρεσίες που συνδέονται με τις τελευταίες.
Εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής	Ηλεκτρονική βεβαίωση που συνδέει τα δεδομένα επικύρωσης μιας ηλεκτρονικής υπογραφής με ένα φυσικό πρόσωπο και επιβεβαιώνει τουλάχιστον το όνομα ή το ψευδώνυμο αυτού του προσώπου. Εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και συμμορφώνεται με τις απαιτήσεις του παραρτήματος I του Καν. ΕΚ 910/2014 (eIDAS).
Ιδιωτικό κλειδί	Το στοιχείο του ζεύγους ασύμμετρων κλειδιών, που χρησιμοποιείται από τον Κάτοχο, μέσω του οποίου τίθεται η ψηφιακή υπογραφή στο πληροφοριακό έγγραφο.
Δημόσιο Κλειδί	Το στοιχείο του ζεύγους ασύμμετρων κλειδιών που προορίζεται να δημοσιοποιηθεί, με το οποίο επαληθεύεται η ψηφιακή υπογραφή στο πληροφοριακό έγγραφο.
CRL	Λίστα Ανακληθέντων Πιστοποιητικών, Certificate Revocation List, μια λίστα με τα ανακληθέντα ή ανασταλμένα πιστοποιητικά, τα οποία δεν θεωρούνται πλέον έγκυρα

	από την Αρχή Πιστοποίησης που τα εξέδωσε.
OCSP	Online Certificate Status Protocol [Διαδικτυακό Πρωτόκολλο Κατάστασης Πιστοποιητικού]: υπηρεσία επαλήθευσης της κατάστασης εγκυρότητας του πιστοποιητικού σύμφωνα με το πρωτόκολλο OCSP.
Ηλεκτρονικό έγγραφο	Το ηλεκτρονικό έγγραφο που περιέχει την πληροφοριακή αναπαράσταση νομικά σημαντικών πράξεων, γεγονότων ή δεδομένων
FEQ – Εγκεκριμένη ηλεκτρονική Υπογραφή *FD - Ψηφιακή Υπογραφή*	Ηλεκτρονική υπογραφή που δημιουργήθηκε από μια συσκευή για τη δημιουργία εγκεκριμένης ηλεκτρονικής υπογραφής που βασίζεται σε ένα εγκεκριμένο πιστοποιητικό για ηλεκτρονικές υπογραφές. Στην Ιταλία συμπίπτει με την *Ψηφιακή Υπογραφή που* ορίζεται στον CAD, άρθρο 1, εδάφιο 1, σημείο s): Εγκεκριμένη ηλεκτρονική υπογραφή που βασίζεται σε ένα σύστημα κρυπτογραφικών κλειδιών, ένα δημόσιο και ένα ιδιωτικό, που σχετίζονται μεταξύ τους, το οποίο επιτρέπει στον Κάτοχο μέσω του ιδιωτικού κλειδιού και στον παραλήπτη μέσω του δημόσιου κλειδιού, αντίστοιχα, να δηλώνουν και να επαληθεύουν την προέλευση και την ακεραιότητα ενός πληροφοριακού εγγράφου ή ενός συνόλου πληροφοριακών εγγράφων.
Υπογραφή εξ αποστάσεως	Ιδιαίτερη διαδικασία εγκεκριμένης ηλεκτρονικής υπογραφής ή ψηφιακής υπογραφής, που παράγεται στο HSM, το οποίο διατηρεί και διαχειρίζεται, υπό την ευθύνη του, ο διαπιστευμένος φορέας πιστοποίησης, που επιτρέπει την εγγύηση του αποκλειστικού ελέγχου των ιδιωτικών κλειδιών από τους κατόχους των ιδίων.
HSM - Hardware Security Module	Συσκευές για τη δημιουργία εγκεκριμένης ηλεκτρονικής υπογραφής, εάν συμμορφώνονται με τις απαιτήσεις του παραρτήματος II του Καν. (ΕΕ) 910/2014. Ονομάζονται επίσης *Συσκευές Υπογραφής*.
Qualified Electronic Time Stamp (Χρονόσημο)	*Εγκεκριμένη Ηλεκτρονική Χρονοσφραγίδα*: Δεδομένα σε ηλεκτρονική μορφή που συνδέουν άλλα δεδομένα σε ηλεκτρονική μορφή με μια συγκεκριμένη ώρα και ημερομηνία, έτσι ώστε να αποδεικνύεται ότι τα τελευταία δεδομένα υπήρχαν εκείνη τη στιγμή. Πληροί τις απαιτήσεις του άρθρου 42 του κανονισμού eIDAS.
CA – Certification Authority [Αρχή Πιστοποίησης]	Αρχή που εκδίδει πιστοποιητικά για ηλεκτρονική υπογραφή.
RA – Registration Authority	*Αρχή Καταχώρησης:* φορέας που, κατ' εντολή του QTSP, είναι υπεύθυνος για την καταχώρηση και την επαλήθευση των πληροφοριών (ιδίως της ταυτότητας του Κατόχου) που είναι απαραίτητες για τον QTSP για την έκδοση του Εγκεκριμένου Πιστοποιητικού.
Μητρώο Πιστοποιητικών	Ο συνδυασμός ενός ή περισσότερων πληροφοριακών αρχείων που τηρείται από τον Φορέα Πιστοποίησης, που περιέχει όλα τα πιστοποιητικά που εκδόθηκαν.
Αιτών	Το Φυσικό Πρόσωπο που ζητά το πιστοποιητικό.
Κάτοχος	Το Φυσικό Πρόσωπο στο οποίο εκδίδεται το εγκεκριμένο πιστοποιητικό και το οποίο είναι εξουσιοδοτημένο να το χρησιμοποιεί για να θέτει την ψηφιακή του υπογραφή.
Πελάτης *Πελάτης Prospect*	Είναι ο Πελάτης (ή δυνητικός πελάτης, επίσης Prospect) της Τράπεζας / του Χρηματοοικονομικού ιδρύματος.
Χρονική Αναφορά	Πληροφορία που περιέχει την ημερομηνία και την ώρα που σχετίζεται με ένα ή περισσότερα πληροφοριακά έγγραφα.
TSA - Time Stamping Authority [Αρχή Χρονοσήμανσης]	Αρχή που εκδίδει τις ηλεκτρονικές χρονοσφραγίδες.

A. Εισαγωγή

Το παρόν έγγραφο αποτελεί το *Εγχειρίδιο Λειτουργίας για τις διαδικασίες εγκεκριμένης ηλεκτρονικής υπογραφής εξ αποστάσεως στο πλαίσιο των τραπεζικών και χρηματοπιστωτικών υπηρεσιών της FCA Bank* (εφεξής, *Εγχειρίδιο Λειτουργίας* ή ακόμη και μόνο *Εγχ. Λειτ.*) του QTSP In.Te.S.A. S.p.A.

Το περιεχόμενο αυτού του εγχειριδίου λειτουργίας συμμορφώνεται με τις διατάξεις των τεχνικών κανόνων που περιέχονται στο *Διάταγμα του Προέδρου του Υπουργικού Συμβουλίου της 22ας Φεβρουαρίου 2013* (εφεξής *DPCM*) και του *Ν.Δ.* της *7ης Μαρτίου 2005, αρ. 82, που φέρει τον «Κώδικα Ψηφιακής Διαχείρισης»,* όπως τροποποιήθηκε και συμπληρώθηκε (*«CAD»)* και συμμορφώνεται με *τον Καν. ΕΕ 910/2014* (στο εξής, *Καν. eIDAS).*

Για όσα δεν προβλέπονται ρητά σε αυτό το εγχειρίδιο λειτουργίας, γίνεται παραπομπή στους ισχύοντες και μελλοντικούς κανονισμούς που διέπουν τη συγκεκριμένη περίπτωση.

Αυτό το έγγραφο περιγράφει τους κανόνες και τις διαδικασίες λειτουργίας του *QTSP In.Te.S.A. S.p.A.* (εφεξής, μόνο *QTSP INTESA, Φορέας Πιστοποίησης* ή ακόμη και μόνο *INTESA*) για την έκδοση εγκεκριμένων πιστοποιητικών, τη δημιουργία και την επαλήθευση εγκεκριμένης ηλεκτρονικής υπογραφής και τις διαδικασίες της υπηρεσίας ηλεκτρονικής χρονοσήμανσης σύμφωνα με την ισχύουσα νομοθεσία, όταν τελεί υπό διαχείριση

που πραγματοποιείται στο πλαίσιο τραπεζικών ή χρηματοπιστωτικών έργων της FCA Bank.
Σε περίπτωση ενεργειών αυτής της τυπολογίας, η FCA Bank και οι συνδεόμενες με αυτήν εταιρείες θα λειτουργούν επίσης και ως Local Registration Authority (εφεξής, LRA) για λογαριασμό της QTSP INTESA.
Σε αυτό το πλαίσιο, οι Κάτοχοι Εγκεκριμένου Πιστοποιητικού είναι μόνο τα πρόσωπα που έχουν ταυτοποιηθεί από την ίδια την FCA Bank και από τις LRA οι οποίες, βάσει ειδικής συμφωνίας με την QTSP INTESA, είναι εξουσιοδοτημένες να εκτελούν τη λειτουργία της Registration Authority.
Επομένως, πρέπει να σημειωθεί ότι όλες οι διαδικασίες υπογραφής εγγράφων που αποτελούν αντικείμενο αυτού του Εγχειριδίου Λειτουργίας θα εφαρμόζονται αποκλειστικά στο πλαίσιο τραπεζικών ή χρηματοπιστωτικών εφαρμογών της FCA Bank.
Οι δραστηριότητες που περιγράφονται σε αυτό το Εγχειρίδιο Λειτουργίας διεξάγονται σύμφωνα με τον Καν. ΕΕ 910/2014 (eIDAS).

A.1. Πνευματική ιδιοκτησία

Το παρόν Εγχειρίδιο Λειτουργίας είναι αποκλειστική ιδιοκτησία της In.Te.S.A. SpA, που είναι Κάτοχος όλων των σχετικών πνευματικών δικαιωμάτων.

Το περιεχόμενο που περιγράφεται στο παρόν κείμενο για την εκτέλεση των δραστηριοτήτων του QTSP καλύπτεται από δικαιώματα πνευματικής ιδιοκτησίας.

A.2. Εγκυρότητα

Το περιεχόμενο που περιγράφεται σε αυτό το έγγραφο ισχύει για την QTSP INTESA (δηλαδή για τις εφοδιαστικές και τεχνικές υποδομές της, καθώς και για το προσωπικό της), για τους Κατόχους των πιστοποιητικών που η ίδια εκδίδει και για όσους χρησιμοποιούν αυτά τα πιστοποιητικά για να επαληθεύουν την αυθεντικότητα και την ακεραιότητα των εγγράφων στα οποία έχει τεθεί εγκεκριμένη ηλεκτρονική υπογραφή, χρησιμοποιώντας επίσης τα εγκεκριμένα χρονόσημα που εκδίδονται από την QTSP INTESA, και από την FCA Bank και τις LRA.

Η χρήση των κλειδιών και των σχετικών πιστοποιητικών που εκδίδονται διέπεται από τις διατάξεις του άρθρου 5, εδάφιο 4 του DPCM, στο οποίο ορίζεται ότι τα κλειδιά δημιουργίας και επαλήθευσης της υπογραφής και οι σχετικές υπηρεσίες διακρίνονται σύμφωνα με τις ακόλουθες τυπολογίες:

1. κλειδιά υπογραφής που προορίζονται για τη δημιουργία και την επαλήθευση υπογραφών που έχουν τεθεί ή σχετίζονται με τα έγγραφα
2. κλειδιά πιστοποίησης που προορίζονται για τη δημιουργία και την επαλήθευση των υπογραφών που έχουν τεθεί σε εγκεκριμένα πιστοποιητικά, για τις πληροφορίες σχετικά με το καθεστώς εγκυρότητας του πιστοποιητικού ή για την υπογραφή των πιστοποιητικών που αφορούν κλειδιά ηλεκτρονικής χρονοσφραγίδας
3. κλειδιά χρονοσήμανσης που προορίζονται για τη δημιουργία και την επαλήθευση πιστοποιημένων χρονοσήμων

B. Γενικές πληροφορίες

Το παρόν έγγραφο αποσκοπεί στην περιγραφή, υπό γενικούς όρους, των διαδικασιών και των συναφών κανόνων που διέπουν την έκδοση εγκεκριμένων πιστοποιητικών από την INTESA QTSP.

Οι προαναφερθέντες κανόνες και διαδικασίες απορρέουν από τη συμμόρφωση με τους ισχύοντες κανονισμούς αναφοράς η τήρηση των οποίων επιτρέπει στην INTESA να συμπεριλαμβάνεται στη λίστα των διαπιστευμένων φορέων πιστοποίησης.

Επομένως, για τη συμμόρφωση με τους προαναφερθέντες κανονισμούς, θα προκύπτει απαραίτητη η συμμετοχή περισσότερων οντοτήτων που θα προσδιοριστούν καλύτερα στη συνέχεια του εγγράφου.

B.1. Δεδομένα ταυτοποίησης της έκδοσης του Εγχειριδίου Λειτουργίας

Το παρόν έγγραφο αποτελεί την έκδοση αρ. 04 του Εγχειριδίου Χρήσης για διαδικασίες εγκεκριμένης ηλεκτρονικής υπογραφής εξ αποστάσεως σε τραπεζικό και χρηματοπιστωτικό πλαίσιο, που εκδόθηκε σύμφωνα με το άρθρο 40 του DPCM.

Ο κωδικός ταυτοποίησης αυτού του εγγράφου είναι **1.3.76.21.1.50.110.**
Αυτό το Εγχειρίδιο Λειτουργίας είναι δημοσιευμένο και προσβάσιμο ηλεκτρονικά:

- στη διαδικτυακή διεύθυνση του QTSP, https://www.intesa.it/e-trustcom/

- στη διαδικτυακή διεύθυνση της Ιταλικής Υπηρεσίας για την Ψηφιακή Τεχνολογία, www.agid.gov.it
- στο περιεχόμενο του επίσημου ιστότοπου της Τράπεζας/του Ιδρύματος

Σημείωση: η δημοσίευση ενημερωμένων εκδόσεων του παρόντος Εγχειριδίου Λειτουργίας μπορεί να πραγματοποιείται μόνο με την εξουσιοδότηση της Ιταλικής Υπηρεσίας για την Ψηφιακή Τεχνολογία

B.2. Δεδομένα ταυτοποίησης του QTSP - Qualified Trust Services Provider

Ο QTSP (Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης) είναι η εταιρεία In.Te.S.A. S.p.A , της οποίας τα δεδομένα ταυτοποίησης παρατίθενται στη συνέχεια.

Εταιρική Επωνυμία	**In.Te.S.A. S.p.A.**
Διεύθυνση καταστατικής έδρας	**Strada Pianezza, 289** **10151 Τορίνο**
Νομικός Εκπρόσωπος	**Διευθύνων Σύμβουλος**
Μητρώο Επιχειρήσεων του Τορίνο	**Αριθμός εγγραφής 1692/87**
Αριθμός εγγραφής ΦΠΑ	**05262890014**
Αριθμός τηλεφώνου (τηλ. κέντρο)	**+39.011.19216.111**
Διαδικτυακός τόπος	**www.intesa.it**
Διεύθυνση ηλεκτρονικού ταχυδρομείου	**marketing@intesa.it**
Διεύθυνση μητρώου πιστοποιητικών (URL)	**ldap://x500.e-trustcom.intesa.it**
Κωδικός Ταυτοποίησης Αντικειμένων (ΚΤΑ) ISO (OID-Object Identifier)	**1.3.76.21.1**

Το προσωπικό υπεύθυνο για τις δραστηριότητες πιστοποίησης, σύμφωνα με το άρθρο 38 του DPCM, χωρίζεται στους ακόλουθους ρόλους:

1. Υπεύθυνος ασφαλείας
2. Υπεύθυνος της υπηρεσίας πιστοποίησης και ηλεκτρονικής χρονοσφραγίδας
3. Υπεύθυνος για την τεχνική διαχείριση των συστημάτων
4. Υπεύθυνος τεχνικών και εφοδιαστικών υπηρεσιών
5. Υπεύθυνος επαλήθευσης και επίβλεψης (auditing)

Οι παραπάνω ρόλοι εμπίπτουν στο πλαίσιο της οργάνωσης της QTSP INTESA.

B.3. Ευθύνη για το Εγχειρίδιο Λειτουργίας

Η ευθύνη για το παρόν Εγχειρίδιο Λειτουργίας, σύμφωνα με το άρθρο 40 εδάφιο 3 γράμμα γ) του DPCM, είναι της Certification Authority INTESA, η οποία μεριμνά για τη σύνταξη και τη δημοσίευσή του.

Η INTESA προκειμένου να συλλέξει ενδεχόμενα σχόλια και αιτήματα για διευκρινίσεις παρέχει τα ακόλουθα εργαλεία επικοινωνίας:

διεύθυνση email:	*marketing@intesa.it*
αριθμός τηλεφώνου:	+39 011.192.16.111
υπηρεσία HelpDesk:	για κλήσεις από την Ιταλία 800.80.50.93 για κλήσεις από το εξωτερικό +39 02.871.193.396

B.4. Οντότητες που εμπλέκονται στις διαδικασίες

Στη διάρθρωση του QTSP ταυτοποιούνται οντότητες που συμμετέχουν στις διαδικασίες που αφορούν την έκδοση των πιστοποιητικών.

Αυτοί οι παράγοντες λειτουργούν σύμφωνα με τους κανόνες και τις διαδικασίες που εφαρμόζει ο QTSP, πραγματοποιώντας, κατά το μέρος της αρμοδιότητάς τους, τις δραστηριότητες που τους έχουν ανατεθεί.

B.4.1. Certification Authority (CA)

Η INTESA, λειτουργώντας σύμφωνα με τις διατάξεις των DPCM, CAD και eIDAS, εκτελεί δραστηριότητες

Qualified Trust Service Provider. Αυτές οι δραστηριότητες περιλαμβάνουν τις εγκεκριμένες υπηρεσίες εμπιστοσύνης για τη δημιουργία, επαλήθευση και επικύρωση ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων ή ηλεκτρονικών χρονοσφραγίδων.

Τα δεδομένα ταυτοποίησης της INTESA QTSP αναφέρονται στην προηγούμενη παράγραφο *B.2*.

B.4.2. Local Registration Authority (LRA)

Για την συγκεκριμένη τυπολογία παρεχόμενης υπηρεσίας (εγκεκριμένη ηλεκτρονική υπογραφή εξ αποστάσεως στο πλαίσιο τραπεζικών και χρηματοπιστωτικών εφαρμογών) που περιγράφεται σε αυτό το Εγχειρίδιο Λειτουργίας, η INTESA QTSP αναθέτει τη διεξαγωγή των λειτουργιών Registration Authority στην Τράπεζα / το Ίδρυμα που θα έχουν αποκτήσει την υπηρεσία.

Η LRA δεσμεύεται να διεξάγει τις ακόλουθες δραστηριότητες:

- Ταυτοποίηση του Κατόχου
- Καταχώρηση του Κατόχου

Η Τράπεζα / το Ίδρυμα κατά την άσκηση της λειτουργίας της ως Registration Authority, θα πρέπει να διασφαλίζει ότι η δραστηριότητα αναγνώρισης πραγματοποιείται σύμφωνα με την ισχύουσα νομοθεσία και με τις διατάξεις του παρόντος Εγχειριδίου Λειτουργίας.

Συγκεκριμένα, η Τράπεζα / το Ίδρυμα, σε συμμόρφωση με τη νομοθεσία για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, θα μπορεί να είναι σε θέση να προσδιορίζει τον Κάτοχο (*επαρκής επαλήθευση*) ακόμη και αν ο τελευταίος δεν παρουσιάζεται αυτοπροσώπως σε μια υπηρεσία.

Σε αυτήν την περίπτωση η Τράπεζα / το Ίδρυμα θα πρέπει εν πάση περιπτώσει να:

- εξακριβώνει την ταυτότητα μέσω εγγράφων, δεδομένων ή πρόσθετων πληροφοριών, όπως δημόσια έγγραφα, επικυρωμένα ιδιωτικά έγγραφα, πιστοποιητικά που χρησιμοποιούνται για τη δημιουργία εγκεκριμένης ηλεκτρονικής υπογραφής που σχετίζεται με πληροφοριακά έγγραφα ή μέσω δήλωσης της Ιταλικής Προξενικής Αρχής
- εφαρμόζει πρόσθετα μέτρα για την επαλήθευση των παρεχόμενων εγγράφων όπως, για παράδειγμα, πιστοποίηση επιβεβαίωσης πιστωτικού ή χρηματοπιστωτικού ιδρύματος που υπόκειται στην οδηγία
- χρησιμοποιεί την τεκμηρίωση που αποδεικνύει ότι η ανάθεση χρηματοοικονομικής κάλυψης προέρχεται από έναν λογαριασμό στο όνομα του πελάτη

C. Υποχρεώσεις

C.1. Υποχρεώσεις του Εγκεκριμένου Παρόχου Υπηρεσιών Εμπιστοσύνης (QTSP)

Κατά την άσκηση της δραστηριότητάς του, ο Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης (αναφέρεται επίσης ως *Διαπιστευμένος Φορέας Πιστοποίησης*) λειτουργεί σύμφωνα με τα όσα ορίζουν οι εξής διατάξεις:

- Νομοθετικό διάταγμα της 7ης Μαρτίου 2005, αρ. 82 και επακόλουθες τροποποιήσεις
- Διάταγμα του Προέδρου του Υπουργικού Συμβουλίου 22 Φεβρουαρίου 2013
- Κανονισμός (ΕΕ) 2016/679 (ΓΚΠΔ)
- Κανονισμός (ΕΕ) 910/2014 (eIDAS)

Συγκεκριμένα, ο QTSP:

- υιοθετεί όλα τα οργανωτικά και τεχνικά μέτρα κατάλληλα για την αποφυγή ζημιών σε τρίτους
- τηρεί τους τεχνικούς κανόνες που καθορίζονται στο DPCM και επακόλουθες τροποποιήσεις και ενσωματώσεις
- εγγυάται ότι το σύστημα ποιότητας που εφαρμόζει συμμορφώνεται με τα πρότυπα ISO 9001
- διασφαλίζει ότι η συσκευή για τη δημιουργία των υπογραφών (HSM) διαθέτει τις απαιτήσεις ασφαλείας που προβλέπονται στο άρθρο 29 του Καν. eIDAS
- εκδίδει και δημοσιοποιεί το εγκεκριμένο πιστοποιητικό, εκτός εάν ορίζεται διαφορετικά από τον Κάτοχο, σύμφωνα με τις διατάξεις του Άρθρου 32 του CAD
- ενημερώνει τους αιτούντες, με σαφήνεια και διαύγεια, σχετικά με τη διαδικασία πιστοποίησης, τις απαραίτητες τεχνικές απαιτήσεις για την πρόσβαση σε αυτήν, τα χαρακτηριστικά και τους περιορισμούς χρήσης των υπογραφών που εκδίδονται βάσει της υπηρεσίας πιστοποίησης

- τηρεί τα μέτρα ασφαλείας για την επεξεργασία των προσωπικών δεδομένων (ΓΚΠΔ)
- δεν αποθηκεύει δεδομένα για τη δημιουργία της υπογραφής του Κατόχου
- προβαίνει στη δημοσίευση της ανάκλησης και της αναστολής του ηλεκτρονικού πιστοποιητικού σε περίπτωση αίτησης του Κατόχου ή του ενδιαφερόμενου τρίτου μέρους
- διασφαλίζει τον ακριβή προσδιορισμό της ημερομηνίας και ώρας έκδοσης, ανάκλησης και αναστολής των ηλεκτρονικών πιστοποιητικών
- τηρεί αρχείο καταχώρησης, ακόμα και ηλεκτρονικό, όλων των πληροφοριών σχετικά με το εγκεκριμένο πιστοποιητικό για 20 (είκοσι) έτη, ιδίως προκειμένου για να παρέχει απόδειξη της πιστοποίησης σε ενδεχόμενες δικαστικές διαδικασίες
- διασφαλίζει ότι ο κωδικός ταυτοποίησης (αποκλειστικής ιδιοκτησίας του QTSP) που ανατίθεται σε κάθε Κάτοχο είναι μονοσήμαντος για τους χρήστες του
- παρέχει σε σταθερά μέσα επικοινωνίας όλες τις χρήσιμες πληροφορίες θέτοντας τες στη διάθεση όσων ζητούν την υπηρεσία πιστοποίησης· μεταξύ αυτών αναφέρουμε: τους ακριβείς όρους και προϋποθέσεις που σχετίζονται με τη χρήση του πιστοποιητικού, συμπεριλαμβανομένου κάθε ενδεχόμενου ορίου χρήσης, την ύπαρξη ενός προαιρετικού συστήματος διαπίστευσης και τις διαδικασίες καταγγελίας και επίλυσης διαφορών· οι εν λόγω πληροφορίες, οι οποίες μπορούν να μεταδίδονται ηλεκτρονικά, πρέπει να είναι καταγεγραμμένες σε σαφή γλώσσα και να παρέχονται πριν από τη συμφωνία μεταξύ του αιτούντος την υπηρεσία και του QTSP
- χρησιμοποιεί αξιόπιστα συστήματα για τη διαχείριση του μητρώου πιστοποιητικών κατά τρόπο που να διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα μπορούν να κάνουν εισαγωγές και τροποποιήσεις, ότι η γνησιότητα των πληροφοριών είναι επαληθεύσιμη, ότι τα πιστοποιητικά είναι προσβάσιμα στο κοινό για εξέταση μόνο στις περιπτώσεις που επιτρέπονται από τον Κάτοχο του πιστοποιητικού και ότι ο χειριστής μπορεί να αποκτά επίγνωση για την ύπαρξη οποιουδήποτε γεγονότος που θέτει σε κίνδυνο τις απαιτήσεις ασφαλείας
- καταγράφει την έκδοση εγκεκριμένων πιστοποιητικών στο ημερολόγιο ελέγχου όπου επίσης καταχωρεί τη συγκεκριμένη ημερομηνία και ώρας δημιουργίας

Σύμφωνα με τις διατάξεις του Άρθρου 14 του DPCM, ο Φορέας Πιστοποίησης παρέχει ή υποδεικνύει τουλάχιστον ένα σύστημα που επιτρέπει την επαλήθευση των ψηφιακών υπογραφών.

Επιπλέον, ο QTSP:

- δημιουργεί ένα εγκεκριμένο πιστοποιητικό, για καθένα από τα κλειδιά προηγμένης ηλεκτρονικής υπογραφής που χρησιμοποιούνται από την Ιταλική Υπηρεσία για την Ψηφιακή Τεχνολογία για την υπογραφή του δημόσιου καταλόγου φορέων πιστοποίησης, και το δημοσιεύει στο δικό του μητρώο πιστοποιητικών σύμφωνα με το άρθρο 42 του DPCM
- υποδεικνύει ένα σύστημα επαλήθευσης ηλεκτρονικής υπογραφής, δυνάμει του Άρθ. 10 του DPCM
- διατηρεί αντίγραφο του καταλόγου, υπογεγραμμένο από την Ιταλική Υπηρεσία για την Ψηφιακή Τεχνολογία, των πιστοποιητικών που σχετίζονται με τα κλειδιά πιστοποίησης δυνάμει του άρθρου 43 του DPCM, και τον καθιστά ηλεκτρονικά προσβάσιμο όπως ορίζεται στο άρθρο 42 εδάφιο 3 του DPCM

C.2. Υποχρεώσεις του Κατόχου

Ο Κάτοχος που ζητά ένα εγκεκριμένο πιστοποιητικό για τις υπηρεσίες που περιγράφονται σε αυτό το Εγχειρίδιο Λειτουργίας είναι πελάτης της Τράπεζας ή του Ιδρύματος Πληρωμής που λειτουργούν ως Registration Authority.

Ο Κάτοχος θα λάβει ένα εγκεκριμένο πιστοποιητικό για την Εγκεκριμένη Ηλεκτρονική Υπογραφή εξ Αποστάσεως, με το οποίο μπορεί να υπογράφει συμβόλαια και έγγραφα σχετικά με προϊόντα ή/και υπηρεσίες που προσφέρονται από την Τράπεζα / το Ίδρυμα σύμφωνα με τους τρόπους που περιγράφονται στην παρ...

Ο Κάτοχος υποχρεούται να διατηρεί τις απαραίτητες πληροφορίες για τη χρήση του ιδιωτικού κλειδιού υπογραφής του με επαρκή τρόπο και να υιοθετεί όλα τα οργανωτικά και τεχνικά μέτρα κατάλληλα για την αποφυγή ζημιών σε τρίτους (CAD, Άρθ.32, εδάφιο 1).

Ο Κάτοχος του κλειδιού πρέπει επίσης να:

- παρέχει όλες τις πληροφορίες που απαιτούνται από τον QTSP, διασφαλίζοντας την αξιοπιστία τους υπό ιδίαν ευθύνη

- μεταβιβάζει την αίτηση πιστοποίησης σύμφωνα με τους τρόπους που αναφέρονται στο παρόν Εγχειρίδιο Λειτουργίας
- κοινοποιεί στον QTSP, ακόμα και μέσω της LRA, τυχόν αλλαγές στις πληροφορίες που παρέχονται κατά τη διαδικασία καταχώρησης: προσωπικά δεδομένα, διαμονή, αριθμοί τηλεφώνου, διεύθυνση e-mail, κ.λπ.
- διατηρεί με μέγιστη προσοχή και επιμέλεια τις πληροφορίες που επιτρέπουν τη χρήση του ιδιωτικού κλειδιού
- υποβάλλει άμεση αναφορά στις αρμόδιες αρχές και στην Τράπεζα / το Ίδρυμα, σε περίπτωση απώλειας ή κλοπής των κωδικών ή/και των συσκευών που υποδεικνύονται για πρόσβαση στα κλειδιά υπογραφής του · η Τράπεζα / το Ίδρυμα θα προβεί στην άμεση ανάκληση του πιστοποιητικού
- διαβιβάζει τυχόν αιτήματα ανάκλησης και αναστολής του εγκεκριμένου πιστοποιητικού, σύμφωνα με τα όσα αναφέρονται στο παρόν Εγχειρίδιο Λειτουργίας

C.3. Υποχρεώσεις των χρηστών των πιστοποιητικών

Ο Χρήστης (*Relying Party*) είναι οποιοσδήποτε λαμβάνει ένα ψηφιακά υπογεγραμμένο έγγραφο και, προκειμένου να επαληθεύσει την εγκυρότητά του, στηρίζεται στο Εγκεκριμένο Πιστοποιητικό που χρησιμοποιείται από τον Κάτοχο για να υπογράψει το ίδιο έγγραφο.

Η επαλήθευση της ψηφιακής υπογραφής και η επακόλουθη εξαγωγή των υπογεγραμμένων αντικειμένων μπορούν να γίνουν με οποιοδήποτε λογισμικό σε θέση να επεξεργάζεται υπογεγραμμένα αρχεία σύμφωνα με τον Κανονισμό eIDAS.

Όσοι χρησιμοποιούν ένα Εγκεκριμένο Πιστοποιητικό για να επαληθεύσουν την εγκυρότητα ενός ψηφιακά υπογεγραμμένου εγγράφου θα πρέπει να:

- επαληθεύουν την εγκυρότητα του πιστοποιητικού που περιέχει το δημόσιο κλειδί του Κατόχου και υπογράφοντος του μηνύματος, όπως υποδεικνύεται από τα ισχύοντα πρότυπα κατά τη στιγμή της έκδοσής του
- επαληθεύουν την κατάσταση εγκυρότητας του πιστοποιητικού μέσω του πρωτοκόλλου OCSP ή μέσω πρόσβασης στις Λίστες Ανάκλησης
- επαληθεύουν την εγκυρότητα της διαδικασίας πιστοποίησης, βάσει της δημόσιας λίστας QTSP
- επαληθεύουν την ύπαρξη τυχόν ορίων στη χρήση του πιστοποιητικού που χρησιμοποιεί ο Κάτοχος

C.4. Υποχρεώσεις του Ενδιαφερόμενου Τρίτου Μέρους

Το Ενδιαφερόμενο Τρίτο Μέρος, στις υπηρεσίες που περιγράφονται σε αυτό το Εγχειρίδιο Λειτουργίας, είναι η Τράπεζα ή το Ίδρυμα πληρωμών. Ως εκ τούτου, η Τράπεζα / το Ίδρυμα, ως Ενδιαφερόμενο Τρίτο Μέρος:

- επαληθεύει ότι ο Πελάτης πληροί όλες τις απαραίτητες προϋποθέσεις και εξουσιοδοτεί τον ίδιο Πελάτη να ζητήσει την έκδοση του Εγκεκριμένου Πιστοποιητικού για την Ψηφιακή Υπογραφή Εξ Αποστάσεως
- διεξάγει δραστηριότητα υποστήριξης του Κατόχου
- υποδεικνύει στον QTSP τυχόν περαιτέρω όρια στη χρήση του Εγκεκριμένου Πιστοποιητικού για την Ψηφιακή Υπογραφή εκτός από εκείνα που προβλέπονται στην παρ. *F.1.1.*

Η Τράπεζα / το Ίδρυμα, ως Ενδιαφερόμενο Τρίτο Μέρος, επομένως, μπορεί να υποδεικνύει στον QTSP τυχόν όρια στη χρήση του πιστοποιητικού, ενδεχόμενες εξουσίες εκπροσώπησης και θα πρέπει να γνωστοποιεί οποιαδήποτε τροποποίηση των ιδίων.

Αναφέρονται ενδεικτικά οι ακόλουθες περιπτώσεις:

- τροποποίηση ή παύση των εξουσιών εκπροσώπησης
- διαφοροποίηση ρόλων και εσωτερικών θέσεων
- παύση της σχέσης εξάρτησης

Το αίτημα ανάκλησης ή αναστολής από πλευράς του Ενδιαφερόμενου Τρίτου Μέρους που λαμβάνεται από την LRA θα πρέπει να διαβιβάζεται αμέσως στην CA όταν δεν υφίστανται πλέον οι προϋποθέσεις βάσει των οποίων εκδόθηκε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής στον Κάτοχο.

C.5. Υποχρεώσεις των εξωτερικών Αρχών εγγραφής (LRA)

Η QTSP INTESA, για ανάγκες που σχετίζονται με την παροχή της υπηρεσίας, χρησιμοποιεί επιπλέον φορείς σε όλη την εθνική επικράτεια (εφεξής ονομαζόμενοι εξωτερικές RA ή LRA - Local Registration Authority) για τη διεξαγωγή μέρους των δραστηριοτήτων της Υπηρεσίας καταχώρησης.

Η QTSP In.Te.S.A. S.p.A. αναθέτει τη διεξαγωγή της λειτουργίας Registration Authority στην Τράπεζα ή στο Ίδρυμα Πληρωμών μέσω συγκεκριμένης *Σύμβασης Εντολής*, η οποία υπογράφεται και από τα δύο μέρη.

Συγκεκριμένα, οι εξωτερικές RA εκτελούν τις ακόλουθες δραστηριότητες:

- ταυτοποίηση με βεβαιότητα του αιτούντος την πιστοποίηση (εφεξής ο Κάτοχος του πιστοποιητικού)
- καταχώρηση του αιτούντος / Κατόχου
- παράδοση των συσκευών ή/και κωδικών στον Κάτοχο που θα του επιτρέπει να έχει πρόσβαση στο κλειδί υπογραφής του σύμφωνα με τα Άρθ. 8 και 10 εδάφιο 2 του DPCM
- αποστολή της υπογεγραμμένης τεκμηρίωσης στην Υπηρεσία RA του QTSP INTESA, εκτός εάν έχει συμφωνηθεί διαφορετικά για τη σύμβαση εντολής

Στη Σύμβαση Εντολής καθορίζονται οι υποχρεώσεις με τις οποίες πρέπει να συμμορφώνεται η Τράπεζα / το Ίδρυμα στην οποία η QTSP INTESA αναθέτει τον ρόλο της LRA που ο QTSP υποχρεούται να εποπτεύει.

Ειδικότερα, η LRA καλείται να:

- διασφαλίζει ότι η εφαρμοζόμενη δραστηριότητα ταυτοποίησης διεξάγεται σύμφωνα με την ισχύουσα νομοθεσία (CAD και επακόλουθες τροποποιήσεις και ενσωματώσεις, DPCM, Καν. eIDAS και τη νομοθεσία κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες)
- χρησιμοποιεί και να επεξεργάζεται τα προσωπικά δεδομένα που αποκτήθηκαν κατά την αναγνώριση σύμφωνα με τον ΓΚΠΔ
- καθιστά διαθέσιμο στην QTSP INTESA το υλικό που συλλέχθηκε κατά τη φάση ταυτοποίησης και καταχώρησης

Η διαχείριση της υπηρεσίας ταυτοποίησης (επαρκής επαλήθευση) μπορεί να γίνει με τους τρεις διαφορετικούς τρόπους που περιγράφονται στη συνέχεια:

- *Κανονική*: ο Αιτών ταυτοποιείται σε υποκατάστημα της Τράπεζας ή του Ιδρύματος Πληρωμών
- *On demand*: κατά το άνοιγμα ενός νέου τρεχούμενου λογαριασμού, ο Αιτών θα μπορεί να ζητήσει να έρθει σε επικοινωνία με έναν *Personal Financial Adviser* ο οποίος, μετά το κλείσιμο ραντεβού, θα υποστηρίξει τον Πελάτη σε όλες τις διαδικασίες που σχετίζονται με το άνοιγμα Τρέχοντος Λογαριασμού· σε αυτήν τη φάση, ο Πελάτης θα καθοδηγείται επίσης (αφού ταυτοποιηθεί και καταχωρηθεί) στην αίτηση για εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής
- *On line*: εάν ο Αιτών επιλέξει αντ' αυτού τη μέθοδο άμεσης εγγραφής και έχει ήδη τρεχούμενο λογαριασμό σε τράπεζα στην εθνική επικράτεια, για να ταυτοποιηθεί στο πλαίσιο της εφαρμογής του νόμου, θα μπορεί να:
  - χρησιμοποιεί μια διαδικασία SEPA (ή SDD - SEPA Direct Debit)
  - δώσει εντολή μεταφοράς από τον τρέχοντα λογαριασμό που έχει ήδη ανοιχτεί στην προαναφερόμενη Τράπεζα

Μέσω των παραπάνω διαδικασιών, η LRA της Τράπεζας ή του Ιδρύματος Πληρωμών θα αποκτά όλες τις πληροφορίες που απαιτούνται από τον νόμο, με απόλυτη ασφάλεια και σεβασμό του απορρήτου.

D. Ευθύνες και όρια αποζημιώσεων

D.1. Ευθύνη του QTSP – Όριο αποζημιώσεων

Η QTSP INTESA είναι υπεύθυνη έναντι των Κατόχων για την εκπλήρωση όλων των υποχρεώσεων που απορρέουν από την εκτέλεση των δραστηριοτήτων που προβλέπονται από το DPCM, ΓΚΠΔ, CAD και Καν. eIDAS (και κάθε επακόλουθη τροποποίηση και ενσωμάτωση), όπως περιγράφεται στην παρ. *C.1. Υποχρεώσεις του Εγκεκριμένου Παρόχου Υπηρεσιών Εμπιστοσύνης (QTSP).*

Η INTESA, με την επιφύλαξη περιπτώσεων δόλου ή αμελείας, (Καν. eIDAS, Άρθ. 13), δεν αναλαμβάνει καμία ευθύνη για τις συνέπειες που απορρέουν από τη χρήση των πιστοποιητικών που διαφέρει από τα όσα ορίζονται από το Άρθρο 5 του DPCM, και ιδίως από τη μη συμμόρφωση του Κατόχου και του Τρίτου Ενδιαφερόμενου

Μέρους ως προς τα όσα ορίζονται στο παρόν Εγχειρίδιο Λειτουργίας ή/και από τη μη συμμόρφωση των ιδίων με την ισχύουσα νομοθεσία.

Ομοίως, η INTESA δεν μπορεί να θεωρηθεί υπεύθυνη για τις συνέπειες που οφείλονται σε αιτίες που δεν οφείλονται στην ίδια, όπως για παράδειγμα: φυσικές καταστροφές, ανεπαρκείς υπηρεσίες ή/και τεχνικές και εφοδιαστικές δυσλειτουργίες πέρα από τον έλεγχό της, παρεμβάσεις της Αρχής, εξεγέρσεις ή πολεμικές πράξεις που πλήττουν επίσης ή μόνο τους φορείς στις δραστηριότητες των οποίων INTESA στηρίζεται για να παρέχει τις υπηρεσίες πιστοποίησης.

Η QTSP INTESA δεν θα φέρει ευθύνη για ζημιές που προκύπτουν από μη συμβατή χρήση του Εγκεκριμένου Πιστοποιητικού για την Ψηφιακή Υπογραφή εξ Αποστάσεως σε σχέση με τα όρια χρήσης όπως ορίζεται στην παρ. *F.1.1*.

Ο Κάτοχος, αφού διαβάσει αυτό το Εγχειρίδιο Λειτουργίας, πρέπει να εφαρμόζει όλα τα μέτρα ειδικής επιμέλειας που αποσκοπούν στην αποφυγή ζημιών σε τρίτους που σχετίζονται με την ακατάλληλη χρήση των όσων παρέχονται από τον διαπιστευμένο φορέα πιστοποίησης. Ειδικότερα, υπενθυμίζεται να τηρούνται με τη δέουσα επιμέλεια οι συσκευές OTP και οι μυστικοί κωδικοί απαραίτητοι για την πρόσβαση στα κλειδιά υπογραφής.

D.2. Ασφάλιση

Η INTESA QTSP είναι ο δικαιούχος ασφαλιστικών συμβάσεων για την κάλυψη των κινδύνων που σχετίζονται με την επιχειρησιακή δραστηριότητα και των ζημιών που προκαλούνται σε τρίτους, το περιεχόμενο των οποίων συνάδει με ό,τι είναι απαραίτητο για τη διεξαγωγή της εν λόγω επαγγελματικής δραστηριότητας.

Ειδική δήλωση σύναψης της εν λόγω σύμβασης αποστέλλεται στην Υπηρεσία AgID.

E. Τιμές

Η Υπηρεσία παρέχεται από την Τράπεζα (ή το Ίδρυμα πληρωμών) στους πελάτες της: οι Τιμές για την έκδοση, ανανέωση, ανάκληση και αναστολή του εγκεκριμένου πιστοποιητικού θα αναφέρεται στις συμβάσεις που συνάπτονται μεταξύ του Πελάτη και της Τράπεζας / του Ιδρύματος.

F. Τρόπος ταυτοποίησης και καταχώρησης των χρηστών

F.1. Ταυτοποίηση των χρηστών

Ο QTSP πρέπει να επαληθεύει με βεβαιότητα την ταυτότητα του αιτούντος κατά την πρώτη αίτηση για έκδοση εγκεκριμένου πιστοποιητικού.

Η προαναφερθείσα συναλλαγή μεταβιβάζεται στην Τράπεζα / στο Ίδρυμα που ως LRA και σύμφωνα με τις διατάξεις της ισχύουσας νομοθεσίας κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, θα ταυτοποιήσει και θα καταχωρήσει τον Κάτοχο.

Για τις επακόλουθες ανανεώσεις, εάν πραγματοποιηθούν όταν το εγκεκριμένο πιστοποιητικό είναι ακόμα εν ισχύ, η εν λόγω δραστηριότητα δεν θα πρέπει να επαναληφθεί: ο Κάτοχος θα μεριμνήσει για την γνωστοποίηση ενδεχόμενων αλλαγών σχετικά με τα δεδομένα καταχώρησής του.

Μεταξύ των δεδομένων καταχώρησης που είναι απαραίτητα για την εκτέλεση της υπηρεσίας που αποτελεί αντικείμενου αυτού του εγγράφου υπενθυμίζουμε:

- Όνομα και επώνυμο
- Ημερομηνία γέννησης
- Δήμος ή αλλοδαπό κράτος γέννησης
- ΑΦΜ
- Διεύθυνση κατοικίας
- Κατοικία όπου θα αποστέλλεται έντυπο επικοινωνιακό υλικό
- Αριθμός κινητού τηλεφώνου
- Διεύθυνση email
- Τυπολογία και αριθμός του εγγράφου ταυτότητας που παρουσιάζεται

- Αρχή που εξέδωσε το έγγραφο και ημερομηνία και τόπος έκδοσης και λήξης

Στο τέλος αυτής της φάσης καταχώρησης, στον Κάτοχο ενδέχεται να παραχωρηθεί συσκευή κωδικού πρόσβασης μίας χρήσης [One Time Password] με οθόνη που δημιουργεί αριθμητικούς κωδικούς μίας χρήσης (εφεξής αναφερόμενοι ως *κωδικοί OTP* ή απλά *OTP*).

Ως εναλλακτική λύση σε ένα φυσικό OTP token, η Τράπεζα ή το Ίδρυμα Πληρωμών θα μπορούν να υποδείξουν στους Κατόχους τους τρόπους ενεργοποίησης ενός συστήματος αυθεντικοποίησης λογισμικού για κινητές συσκευές (εφόσον ο Κάτοχος διαθέτει ένα και επιλέξει αυτήν τη λειτουργία ως προτιμότερη λόγω ευκολίας χρήσης σε σχέση με τη χρήση ενός φυσικού token). Αυτό το σύστημα λογισμικού θα επιτρέψει τη δημιουργία ενός κωδικού μίας χρήσης [OTP] στην κινητή συσκευή του Κατόχου και θα μπορεί επομένως να χρησιμοποιείται ως εργαλείο αυθεντικοποίησης για συστήματα υπογραφής εξ αποστάσεως.

Εκτός από το OTP, στον Κάτοχο θα παρέχονται όλες οι απαραίτητες πληροφορίες και ένας *Προσωπικός Αριθμός Ταυτοποίησης* (*PIN*) που θα του εγγυώνται την ασφαλή πρόσβαση στην υπηρεσία υπογραφής εξ αποστάσεως που διατίθεται από την Τράπεζα / το Ίδρυμα.

Το ίδιο PIN θα μπορεί να χρησιμοποιείται ως κωδικός έκτακτης ανάγκης (σε περίπτωση απώλειας ή/και εξαφάνισης του OTP token ή του κινητού για παράδειγμα) για την άμεση αναστολή του εγκεκριμένου πιστοποιητικού στο όνομά του (παρ. *H.2.2*).
Το PIN μπορεί στη συνέχεια να τροποποιηθεί ή να ενημερωθεί από τον Κάτοχο χρησιμοποιώντας τις υπηρεσίες που η Τράπεζα ή το Ίδρυμα Πληρωμών θα θέσει στη διάθεσή του.

Σε αυτήν τη φάση, στον Κάτοχο παρέχονται επίσης οι απαραίτητες πληροφορίες που του επιτρέπουν να αλλάξει οποιαδήποτε στιγμή τον αριθμό κινητού τηλεφώνου που παρείχε προηγουμένως.

Επιπλέον, απευθείας στο ταμείο της Τράπεζας / του Ιδρύματος, ή στη συνέχεια, μέσω σύνδεσης με την υπηρεσία internet banking που παρέχεται από την ίδια Τράπεζα / το Ίδρυμα, αλλά σε κάθε περίπτωση πριν από την αίτηση για έκδοση εγκεκριμένου πιστοποιητικού, ο Κάτοχος θα πρέπει να:

- μελετήσει το Εγχειρίδιο Λειτουργίας της QTSP INTESA
- εξουσιοδοτήσει την Τράπεζα ή το Ίδρυμα Πληρωμών για την επεξεργασία των προσωπικών του δεδομένων για τους σκοπούς που σχετίζονται με την έκδοση εγκεκριμένου πιστοποιητικού για την ηλεκτρονική υπογραφή

Η προηγούμενη τεκμηρίωση, σχετικά με την εγγραφή των κατόχων, διατηρείται για 20 (είκοσι) χρόνια από τη λήξη του πιστοποιητικού.

F.1.1. Όρια χρήσης

Στο Εγκεκριμένο Πιστοποιητικό για την ηλεκτρονική υπογραφή, το οποίο εκδίδεται στο πλαίσιο των υπηρεσιών που περιγράφονται στο παρόν Εγχειρίδιο και που προσφέρεται από την Τράπεζα / το Ίδρυμα, περιλαμβάνεται πάντα ένα όριο χρήσης.

Η τυποποιημένη διατύπωση είναι η εξής:

Η χρήση του πιστοποιητικού περιορίζεται για τις συναλλαγές με Ονομασία Τράπεζας / Ιδρύματος

This certificate may only be used in dealings with Ονομασία Τράπεζας / Ιδρύματος

Συγκεκριμένα όρια χρήσης μπορούν να συμφωνηθούν με την Τράπεζα ή με το Ίδρυμα Πληρωμών.
Η INTESA δεν φέρει ευθύνη για ζημιές που απορρέουν από τη χρήση ενός εγκεκριμένου πιστοποιητικού που υπερβαίνει τα όρια που τίθενται σε αυτό ή που απορρέουν από την υπέρβαση αυτού του ορίου.

F.1.2. Τίτλοι και άδειες ασκήσεως επαγγέλματος

Εάν στο εγκεκριμένο πιστοποιητικό απαιτείται η ένδειξη αδειών ασκήσεως επαγγέλματος (π.χ. συμμετοχή σε επαγγελματική ένωση), ο αιτών πρέπει να προσκομίσει κατάλληλη τεκμηρίωση που αποδεικνύει το υποστατό των εν λόγω αδειών ασκήσεως επαγγέλματος ή ισοδύναμη τεκμηρίωση.

Αντίγραφο αυτής της τεκμηρίωσης διατηρείται για 20 (είκοσι) χρόνια από τη λήξη του πιστοποιητικού.

Η τεκμηρίωση για την υποστήριξη της αίτησης εισαγωγής τίτλων ή αδειών ασκήσεως επαγγέλματος στο εγκεκριμένο πιστοποιητικό δεν θα μπορεί να έχει ημερομηνία προγενέστερη των 10 (δέκα) ημερών από την ημερομηνία υποβολής της αίτησης για την έκδοση του προαναφερθέντος πιστοποιητικού.

Η INTESA δεν φέρει ευθύνη για ζημίες που απορρέουν από την ακατάλληλη χρήση ενός εγκεκριμένου πιστοποιητικού με πληροφορίες σχετικά με άδειες ασκήσεως επαγγέλματος.

Η INTESA, σε περίπτωση αυτοπιστοποίησης, δεν αναλαμβάνει καμία ευθύνη, εκτός από περιπτώσεις δόλου ή αμέλειας (Καν. EIDAS, άρθρο 13), για την ενδεχόμενη εισαγωγή στο πιστοποιητικό πληροφοριών που

αυτοπιστοποιούνται από τον Κάτοχο.

F.1.3. Εξουσίες εκπροσώπησης

Σε περίπτωση που στο εγκεκριμένο πιστοποιητικό απαιτείται η ένδειξη εξουσιών εκπροσώπησης (π.χ. συμμετοχή σε οργανισμό και η αρμοδιότητα που κατέχεται σε αυτόν, η άδεια διεξαγωγής συναλλαγών στο όνομα και εκ μέρους του πελάτη κ.λπ.), ο αιτών πρέπει να προσκομίσει κατάλληλη τεκμηρίωση που αποδεικνύει το υποστατό των εν λόγω εξουσιών εκπροσώπησης.

Για την εκπροσώπηση φυσικών προσώπων, ο αιτών πρέπει να προσκομίσει αυθεντικό αντίγραφο της εξουσιοδότησης ή του συμβολαιογραφικού πληρεξούσιου που υπογράφεται από το πρόσωπο που εκπροσωπείται, μαζί με τη δήλωση συναίνεσης του τελευταίου για την εισαγωγή του ρόλου στο πιστοποιητικό.

Σε περίπτωση που στο πιστοποιητικό απαιτείται ένδειξη ενός ρόλου που σχετίζεται με την εκπροσώπηση οργανισμών ή φορέων ιδιωτικού δικαίου, ο Κάτοχος πρέπει να παρουσιάσει τεκμηρίωση που αποδεικνύει τον ρόλο για τον οποίο ζητείται η εισαγωγή στο πιστοποιητικό και δήλωση του οργανισμού ή του φορέα στον οποίο ανήκει, μέσω του οποίου ο φορέας ή ο οργανισμός εξουσιοδοτεί τον QTSP να εισαγάγει τον συγκεκριμένο ρόλο στο πιστοποιητικό. Αυτό το τελευταίο έγγραφο δεν θα πρέπει να έχει ημερομηνία προγενέστερη των 20 (είκοσι) ημερών από την ημερομηνία έκδοσης του εγκεκριμένου πιστοποιητικού.

Η εισαγωγή πληροφοριών στο εγκεκριμένο πιστοποιητικό σχετικά με την άσκηση δημοσίων καθηκόντων ή εξουσιών εκπροσώπησης σε φορείς ή οργανισμούς δημοσίου δικαίου θα υπόκειται σε ειδικές συμφωνίες με τους ίδιους φορείς. Δυνάμει των εν λόγω συμφωνιών θα είναι δυνατόν να προσδιορίζεται ο ρόλος που αναλαμβάνεται από τον Κάτοχο εντός του φορέα ή του δημόσιου οργανισμού.

Η τεκμηρίωση που προσκομίζεται θα διατηρείται για μια περίοδο 20 (είκοσι) ετών.

Η INTESA δεν φέρει ευθύνη για ζημιές που απορρέουν από την ακατάλληλη χρήση ενός εγκεκριμένου πιστοποιητικού με πληροφορίες σχετικά με εξουσίες εκπροσώπησης.

F.1.4. Χρήση ψευδωνύμων

Ο Κάτοχος μπορεί να ζητήσει να αναγράφεται εναλλακτικά στο πιστοποιητικό, σε συγκεκριμένες περιπτώσεις, ένα ψευδώνυμο αντί των πραγματικών δεδομένων του.

Οι πληροφορίες σχετικά με την πραγματική ταυτότητα του χρήστη θα διατηρούνται για 20 (είκοσι) χρόνια.

F.2. Καταχώρηση των χρηστών που ζητούν πιστοποίηση

Μετά τη φάση ταυτοποίησης, ακολουθεί η καταχώρηση των δεδομένων των Κατόχων στα αρχεία της Certification Authority.

Αυτή η λειτουργία θα μπορεί να εκτελεστεί χρησιμοποιώντας μια εφαρμογή λογισμικού που παρέχει τη δυνατότητα να ανακαλείται απευθείας από τις εφαρμογές της Τράπεζας ή του Ιδρύματος Πληρωμών.

G. Δημιουργία κλειδιών Πιστοποίησης, Ηλεκτρονικής Χρονοσφραγίδας και Υπογραφής

G.1. Δημιουργία κλειδιών πιστοποίησης

Η δημιουργία των κλειδιών εντός των συσκευών υπογραφής πραγματοποιείται παρουσία του Υπεύθυνου Πιστοποίησης, όπως απαιτείται από το DPCM Άρθ.7.

Πριν από την προαναφερθείσα λειτουργία προηγείται η αρχικοποίηση των συσκευών υπογραφής για το σύστημα δημιουργίας των πιστοποιητικών με τις οποίες υπογράφονται τα πιστοποιητικά των Κατόχων και εκείνων της ηλεκτρονικής χρονοσφραγίδας.

Όλα αυτά γίνονται με τρόπο λειτουργίας διπλού ελέγχου για την αποφυγή αθέμιτων λειτουργιών.

Οι λειτουργίες που ακολουθούν τη δημιουργία των ζευγών κλειδιών του Φορέα Πιστοποίησης είναι εφικτές μόνο μέσω συγκεκριμένων συσκευών εξουσιοδότησης (token usb): η προνομιακή πρόσβαση στα HSM μπορεί να πραγματοποιείται μόνο μέσω των κλειδιών που περιέχονται στις εν λόγω συσκευές εξουσιοδότησης όπως αναφέρθηκε παραπάνω.

Για μεγαλύτερη ασφάλεια, αυτά τα πλήκτρα διαχωρίζονται σε περισσότερες συσκευές, σύμφωνα με μια λογική εγγραφή τύπου «*n από m*», έτσι ώστε μόνο η ταυτόχρονη παρουσία τουλάχιστον *n* από *m* τμημάτων του

κλειδιού να επιτρέπουν τη λειτουργία με τα κατάλληλα προνόμια. Επομένως, αυτά φυλάσσονται σε ειδικά ξεχωριστά χρηματοκιβώτια.

Το μήκος των κλειδιών πιστοποίησης είναι τουλάχιστον 2048 bit.

G.2. Δημιουργία κλειδιών του συστήματος ηλεκτρονικής χρονοσφραγίδας

Η δημιουργία των κλειδιών χρονοσφραγίδας πραγματοποιείται σύμφωνα με τις διατάξεις του Άρθρου 49 του DPCM. Το μήκος των κλειδιών του συστήματος χρονοσφραγίδας είναι τουλάχιστον 2048 bit.

G.3. Δημιουργία κλειδιών υπογραφής

Μόλις ολοκληρωθεί η φάση καταχώρησης, κατά τη διάρκεια της οποίας τα δεδομένα των Κατόχων απομνημονεύονται στα αρχεία του Φορέα πιστοποίησης, καθίσταται δυνατή η δημιουργία των κλειδιών υπογραφής.

Ο Κάτοχος μπορεί να ξεκινήσει τη διαδικασία δημιουργίας των κλειδιών και να ζητήσει το Πιστοποιητικό υπογραφής που σχετίζεται με αυτά με έναν από τους τρόπους που περιγράφονται στην παρ. *I. Λειτουργικές διαδικασίες για την υπογραφή εγγράφων*.

Τα ζεύγη κλειδιών υπογραφής δημιουργούνται σε ασφαλείς συσκευές υπογραφής (HSM - Hardware Security Module), που συμμορφώνονται με τις προδιαγραφές που ορίζονται στο *Παράρτημα II* του Καν. eIDAS.

Το μήκος των κλειδιών υπογραφής είναι τουλάχιστον 2048 bit.

H. Τρόπος έκδοσης των πιστοποιητικών

H.1. Διαδικασία έκδοσης Πιστοποιητικών πιστοποίησης

Μετά τη δημιουργία των κλειδιών πιστοποίησης, όπως περιγράφηκε στην παρ. *G.1*, δημιουργούνται τα πιστοποιητικά των δημοσίων κλειδιών, σε συμμόρφωση με τις διατάξεις του DPCM, που υπογράφονται με τα αντίστοιχα ιδιωτικά κλειδιά και καταχωρούνται στο μητρώο πιστοποιητικών σύμφωνα με τις προβλεπόμενες διαδικασίες.

Τα πιστοποιητικά των κλειδιών πιστοποίησης διαβιβάζονται στην Ιταλική Υπηρεσία για την Ψηφιακή Τεχνολογία μέσω του συστήματος επικοινωνίας που αναφέρεται στο άρθρο 12, εδάφιο 1, του DPCM.

Ο Φορέας Πιστοποίησης δημιουργεί ένα εγκεκριμένο πιστοποιητικό για καθένα από τα κλειδιά εγκεκριμένης ηλεκτρονικής υπογραφής που χρησιμοποιεί η Υπηρεσία για την υπογραφή του δημόσιου καταλόγου των φορέων πιστοποίησης και το δημοσιεύει στο δικό του μητρώο πιστοποιητικών. Ο Φορέας Πιστοποίησης πρέπει στη συνέχεια να διατηρεί αντίγραφο του καταλόγου πιστοποιητικών που σχετίζονται με το κλειδί πιστοποίησης, το οποίο έχει συνυπογραφεί από το τμήμα, και να τον διαθέσει ηλεκτρονικά (DPCM, Άρθ. 42, εδάφια 1 και 3).

H.2. Διαδικασία έκδοσης των Πιστοποιητικών υπογραφής

Η INTESA εκδίδει πιστοποιητικά χρησιμοποιώντας ένα σύστημα που συνάδει με το Άρθ. 33 του DPCM.

Μετά τη δημιουργία του ζεύγους κλειδιών υπογραφής, που περιγράφεται στην παρ. *G.3*, δημιουργείται νέα αίτηση πιστοποιητικού σε μορφή *PKCS #10* που παρέχει αυτόματα απόδειξη κατοχής του ιδιωτικού κλειδιού και επαλήθευση της σωστής λειτουργίας του ζεύγους κλειδιών.

Μόλις δημιουργηθούν τα κλειδιά, η αίτηση πιστοποιητικού θα διαβιβαστεί αμέσως από την εφαρμογή της Τράπεζας / του Ιδρύματος στην Certification Authority του QTSP.

Η δημιουργία των πιστοποιητικών καταγράφεται στο ημερολόγιο ελέγχου (DPCM, Άρθ.18, εδάφιο 4).

H.2.1. Πληροφορίες που περιέχονται στα πιστοποιητικά υπογραφής

Τα πιστοποιητικά INTESA, που εκδίδονται στο πλαίσιο του παρόντος εγχειριδίου, είναι εγκεκριμένα πιστοποιητικά σύμφωνα με τον Κανονισμό (ΕΕ) 910/2014 (eIDAS) και, ως εκ τούτου, η διαλειτουργικότητα και αναγνώρισή τους σε κοινοτικό επίπεδο είναι εγγυημένες.

Το Εγκεκριμένο Πιστοποιητικό προσδιορίζει με βεβαιότητα τον Φορέα Πιστοποίησης που το εξέδωσε και περιέχει τα απαραίτητα δεδομένα για την επαλήθευση της Ψηφιακής Υπογραφής.

Κάθε Εγκεκριμένο Πιστοποιητικό για την ηλεκτρονική υπογραφή συμμορφώνεται με τον Κανονισμό eIDAS και

με τον ΠΡΟΣΔΙΟΡΙΣΜΟ AgID Αρ. 147/2019 (*Κατευθυντήριες γραμμές που περιέχουν τους Τεχνικούς Κανόνες και Συστάσεις σχετικά με τη δημιουργία πιστοποιητικών*).

Όλα τα Εγκεκριμένα Πιστοποιητικά που εκδίδονται στο πλαίσιο των υπηρεσιών που περιγράφονται στο παρόν Εγχειρίδιο περιέχουν ένα όριο χρήσης (παρ. *F.1.1*).

H.2.2. Κωδικός Έκτακτης ανάγκης

Ο Φορέας Πιστοποίησης εγγυάται, συνάδοντας με τις διατάξεις του Άρθ.21 του DPCM, έναν *κωδικό έκτακτης ανάγκης που* θα χρησιμοποιείται για αιτήματα **επείγουσας αναστολής** του Πιστοποιητικού.

Στις εφαρμογές που περιγράφονται σε αυτό το Εγχειρίδιο Λειτουργίας, το PIN που παραδόθηκε στον Κάτοχο κατά τη διαδικασία της καταχώρησής του θα θεωρείται ως κωδικός έκτακτης ανάγκης.

I. Λειτουργικές διαδικασίες για την υπογραφή εγγράφων

Η INTESA QTSP, μέσω των υπηρεσιών της Τράπεζας ή του Ιδρύματος Πληρωμών, θέτει στη διάθεση των Κατόχων τα απαραίτητα μέσα για τη δημιουργία εγκεκριμένων ηλεκτρονικών υπογραφών σύμφωνα με τις διατάξεις της ισχύουσας νομοθεσίας.

Η συγκεκριμένη τυπολογία υπηρεσίας δεν απαιτεί την παροχή μιας εφαρμογής υπογραφής εγκατεστημένης στον προσωπικό υπολογιστή, αλλά μάλλον λειτουργίες υπογραφής που μπορούν να ανακληθούν είτε με πρόσβαση στην υπηρεσία home banking της Τράπεζας ή του Ιδρύματος Πληρωμών είτε απευθείας στο ταμείο ενός υποκαταστήματος της Τράπεζας ή του Ιδρύματος Πληρωμών.

Οι εγκεκριμένες ηλεκτρονικές υπογραφές που λαμβάνονται μέσω αυτών των διαδικασιών θα συμμορφώνονται πλήρως με τις προβλέψεις του DPCM στο Άρθ. 4 εδάφιο 2 σχετικά με τους χρησιμοποιούμενους αλγόριθμους.

Αυτά τα έγγραφα, επιπλέον, όπως απαιτείται από το άρθ. 4 εδάφιο 3 του ίδιου DPCM, δεν θα περιέχουν μακροεντολές ή εκτελέσιμους κωδικούς, που ενεργοποιούν λειτουργίες που καθιστούν δυνατή, χωρίς τη γνώση του υπογράφοντος, την τροποποίηση πράξεων, γεγονότων και δεδομένων που εκπροσωπούνται στα ίδια έγγραφα.

Περιγράφονται στη συνέχεια δύο διαφορετικοί τρόποι αυθεντικοποίησης που, σύμφωνα με την ισχύουσα νομοθεσία, επιτρέπουν σε έναν Κάτοχο, εφόσον καταχωρηθεί, να προβαίνει πρώτα στη δημιουργία των κλειδιών υπογραφής και σε αίτηση ενός εγκεκριμένου πιστοποιητικού και στη συνέχεια στη χρήση των ιδίων για την πραγματοποίηση εγκεκριμένων ηλεκτρονικών υπογραφών.

Για επιβεβαίωση της εκτέλεσης των λειτουργιών υπογραφής θα αποστέλλονται SMS. Εάν ο Κάτοχος διαθέτει smartphone ενεργοποιημένο για την ανάγνωση ηλεκτρονικής αλληλογραφίας, θα μπορούν εναλλακτικά να αποστέλλονται e-mail κατόπιν αιτήματος του Κατόχου.

I.1. Αυθεντικοποίηση τύπου «Call Drop»

Αυτός ο τρόπος αυθεντικοποίησης απαιτεί από τον χρήστη, που έχει προηγουμένως ταυτοποιηθεί, να πραγματοποιεί μια κλήση με το προσωπικό του κινητό τηλέφωνο (από τον ίδιο αριθμό που παρείχε κατά την ταυτοποίηση), προκειμένου να επιβεβαιώσει τη βούληση του να υπογράψει ένα έγγραφο.

Με τη λήψη της προαναφερθείσας κλήσης, η προέλευσή της επαληθεύεται από τον αριθμό τηλεφώνου (*Call Identifier*) που προηγουμένως συσχετίστηκε με τον χρήστη κατά την καταχώρηση και, σε περίπτωση θετικής επαλήθευσης, επιτρέπεται η λειτουργία εγκεκριμένης ηλεκτρονικής υπογραφής.

Επομένως, όταν ο Κάτοχος θελήσει να υπογράψει ένα έγγραφο μέσω πρόσβασης στον ιστοχώρο της Τράπεζας / του Ιδρύματος, θα χρησιμοποιήσει μια διαδικασία αυθεντικοποίησης με δύο παράγοντες εισάγοντας ένα PIN (πληροφορία που μόνο ο χρήστης γνωρίζει) και έναν αριθμό τηλεφώνου (που παρέχεται από την SIM που μόνο ο χρήστης κατέχει).

Αυτή η τυπολογία αυθεντικοποίησης ονομάζεται επίσης «*Call Drop*», επειδή όταν ο Κάτοχος καλεί για την αυθεντικοποίησή του: δεν ενεργοποιείται καμία συνομιλία και η κλήση ολοκληρώνεται μετά από λίγα δευτερόλεπτα.

Ο Κάτοχος χρήστης δεν λαμβάνει ποτέ απάντηση στην κλήση του και ως εκ τούτου δεν επιβαρύνεται με κανένα κόστος κλήσης.
Ένα από τα πλεονεκτήματα αυτής της μεθόδου είναι ότι είναι απόλυτα οικονομική και πρακτική, καθώς δεν απαιτείται καμία χρήση φυσικής συσκευής αυθεντικοποίησης και είναι πολύ εύκολη στη χρήση.

Θα δούμε παρακάτω πώς είναι άκρως αποδεκτή αυτή η διαδικασία αυθεντικοποίησης όταν ο Κάτοχος

πραγματοποιεί συναλλαγές σε μη επανδρωμένους σταθμούς (συνήθως με πρόσβαση στις υπηρεσίες της Τράπεζας ή του Ιδρύματος Πληρωμών με τον προσωπικό του υπολογιστή μέσω των υπηρεσιών home banking που διατίθενται από την Τράπεζα ή το Ίδρυμα Πληρωμών), αλλά, αντίθετα, είναι ελάχιστα πρακτική όταν ο Κάτοχος πραγματοποιεί συναλλαγές σε επαφή με εξωτερικό χειριστή, για παράδειγμα με ταμία της Τράπεζας ή του Ιδρύματος Πληρωμών.

Για τη διαχείριση των εν λόγω καταστάσεων, σχεδιάστηκε μια λύση που στηρίζεται σε μια δυναμική διαχείριση των αριθμών τηλεφώνου που καλούνται για να ολοκληρωθεί η διαδικασία αυθεντικοποίησης στους χώρους που θα ονομάσουμε επανδρωμένους σταθμούς.

I.1.1. Διαδικασία Υπογραφής σε μη επανδρωμένους σταθμούς (Home banking)

Ο Κάτοχος, εφόσον αποκτήσει τους απαραίτητους κωδικούς κατά τη φάση ταυτοποίησης, θα μπορεί σε ένα επόμενο στάδιο να ζητήσει το ψηφιακό του Πιστοποιητικό και στη συνέχεια να προχωρήσει στην υπογραφή ενός εγγράφου με τους τρόπους που περιγράφονται παρακάτω.

1. Ο Κάτοχος συνδέεται με την τραπεζική ή χρηματοπιστωτική εφαρμογή μέσω των προσωπικών του κωδικών για πρόσβαση στην εφαρμογή.
2. Επιλέγει και επαληθεύει το έγγραφο που πρέπει να υπογράψει.
3. Εισαγάγει τον κωδικό PIN του.
4. Μόλις επικυρωθεί το PIN, ο Κάτοχος, εντός ενός προκαθορισμένου χρονικού διαστήματος (που δεν υπερβαίνει το πρώτο λεπτό) και χρησιμοποιώντας το προηγούμενως καταχωρημένο κινητό τηλέφωνο, πρέπει, για να επιβεβαιώσει την πρόθεσή του να υπογράψει το έγγραφο, να καλέσει αμέσως έναν αριθμό τηλεφώνου που εν τω μεταξύ θα εμφανιστεί στην οθόνη του.
5. Το σύστημα, αφού έχει διαπιστώσει ότι ο αριθμός που καλεί είναι εκείνος που είχε προηγουμένως καταχωρηθεί και συσχετιστεί με τον Κάτοχο, συνεχίζει με τη διαδικασία υπογραφής και στέλνει επιβεβαίωση επιτυχούς έκβασης της ίδιας λειτουργίας.
6. Εάν, αντιθέτως, ο προκαθορισμένος χρόνος έχει παρέλθει χωρίς το σύστημα να έχει λάβει κλήση στον αριθμό που αναφέρεται στο σημείο 4, η λειτουργία θεωρείται άκυρη και ολοκληρώνεται χωρίς την υπογραφή του εγγράφου.

Εάν υπάρχουν περισσότερα από ένα έγγραφα για υπογραφή, ο Κάτοχος για κάθε έγγραφο πρέπει να επαναλάβει τα βήματα από το 2 έως το 5.

I.1.2. Διαδικασία Υπογραφής σε επανδρωμένους σταθμούς (ταμείο τραπέζης ή πιστωτικού ιδρύματος)

Μόλις ληφθεί το εγκεκριμένο πιστοποιητικό, ο Κάτοχος θα μπορεί να προχωρήσει στην υπογραφή ενός εγγράφου.

Όπως αναφέρθηκε προηγουμένως, σε ταμείο τραπέζης ή χρηματοπιστωτικού ιδρύματος και μπροστά από έναν χειριστή, ο Κάτοχος θα μπορούσε να αντιμετωπίσει δυσκολία να εισαγάγει προσωπικούς και εμπιστευτικούς κωδικούς όπως το PIN.

Για αυτό, εξετάστηκε η εφαρμογή εναλλακτικής λύσης, η οποία εγγυάται εν πάση περιπτώσει μέγιστη ασφάλεια:

1. Ο χρήστης παρουσιάζεται στο ταμείο ενός υποκαταστήματος της Τράπεζας / του Ιδρύματος (επανδρωμένος σταθμός) και αναγνωρίζεται από το αρμόδιο προσωπικό (τον ταμία, για παράδειγμα) σε κανονική λειτουργία.
2. Έχοντας δει το έγγραφο που πρόκειται να υπογραφεί, ο Κάτοχος μπορεί να ξεκινήσει τη διαδικασία υπογραφής.
3. Σε αυτό το σημείο προβάλλεται σε μια οθόνη ένας αριθμός τηλεφώνου, ορατός στον Κάτοχο, (που επιλέγεται τυχαία από ένα μεγάλο σύνολο διαθέσιμων αριθμών) και ταυτόχρονα ξεκινά ένα χρονόμετρο.
4. Ο Κάτοχος, σε χρονικό διάστημα που έχει ρυθμιστεί να μην υπερβαίνει το πρώτο λεπτό, πρέπει να καλέσει τον αριθμό που εμφανίστηκε στην οθόνη (χρησιμοποιώντας το κινητό του τηλέφωνο που έχει ήδη καταχωρηθεί) για να επιβεβαιώσει την πρόθεσή του να υπογράψει το έγγραφο·
5. Το σύστημα, σε αυτό το σημείο, εάν ανιχνεύσει την ορθότητα των στοιχείων του καλούντος, προχωρά σε υπογραφή του εγγράφου και στέλνει επιβεβαίωση της λειτουργίας μέσω SMS.
6. Εάν, αντιθέτως, ο καθορισμένος χρόνος έχει παρέλθει χωρίς το σύστημα να έχει λάβει κλήση στον αριθμό που αναφέρεται στο σημείο 3, η λειτουργία ακυρώνεται.

Εάν υπάρχουν περισσότερα από ένα έγγραφα προς υπογραφή, ο Κάτοχος για κάθε έγγραφο πρέπει να επαναλάβει τα βήματα 2 έως 5.

I.2. Αυθεντικοποίηση τύπου OTP για Κινητά

Ως εναλλακτική λύση στο εργαλείο αυθεντικοποίησης Call Drop, διατίθεται ένας δεύτερος τρόπος αυθεντικοποίησης που ονομάζεται "*OTP Mobile*".

Για την ενεργοποίηση αυτού του τρόπου λειτουργίας, ο Κάτοχος θα πρέπει να έχει στη διάθεση του ένα smartphone με τα χαρακτηριστικά που καθορίζονται από την Τράπεζα / το Ίδρυμα ως κατάλληλα για αυτήν την υπηρεσία.

Μόλις πραγματοποιηθεί αυτή η επαλήθευση, κατά τη φάση ταυτοποίησης στο ταμείο της Τράπεζας / του Ιδρύματος όπου έγινε η καταχώρηση, στον Κάτοχο θα κοινοποιηθεί μια συγκεκριμένη διαδικτυακή διεύθυνση στον ιστότοπο της Τράπεζας ή του Ιδρύματος Πληρωμών από όπου θα κάνει λήψη μιας εφαρμογής στο smartphone του που ονομάζεται "*OTP Mobile*" και θα του δοθεί ένα PIN.

Για αυτόν τον δεύτερο τρόπο αυθεντικοποίησης περιγράφουμε επίσης τη διαδικασία υπογραφής ανάλογα με το αν πραγματοποιείται σε επανδρωμένους ή μη επανδρωμένους σταθμούς.

I.2.1. Διαδικασία Υπογραφής σε μη επανδρωμένους σταθμούς (Home banking)

Ο Κάτοχος, μόλις αποκτήσει το εγκεκριμένο πιστοποιητικό του, θα μπορεί να υπογράψει ένα έγγραφο ακολουθώντας τα εξής βήματα:

1. Ο Κάτοχος συνδέεται με την τραπεζική ή χρηματοπιστωτική εφαρμογή χρησιμοποιώντας τους προσωπικούς του κωδικούς για πρόσβαση στην εφαρμογή.
2. Επιλέγει και επαληθεύει το έγγραφο που πρέπει να υπογράψει.
3. Εισαγάγει στη συνέχεια το PIN του.
4. Στη συνέχεια, θα ξεκινήσει την εφαρμογή που είχε προηγουμένως κατεβάσει στο smartphone του λαμβάνοντας ένα OTP Mobile για εισαγωγή μετά το PIN.
5. Το σύστημα αφού διαπιστωθεί η ορθότητα του PIN και του OTP Mobile που έχουν εισαχθεί, προχωρά με την υπογραφή και στέλνει επιβεβαίωση της επιτυχούς έκβασης της ίδιας συναλλαγής.

Εάν υπάρχουν περισσότερα από ένα έγγραφα προς υπογραφή, ο Κάτοχος για κάθε έγγραφο πρέπει να επαναλάβει τα βήματα 2 έως 5.

I.2.2. Διαδικασία Υπογραφής σε επανδρωμένους σταθμούς (ταμείο τραπέζης ή πιστωτικού ιδρύματος)

Έχει σχεδιαστεί και σε αυτήν την περίπτωση μια λύση που δεν απαιτεί από τον Κάτοχο να εισάγει εμπιστευτικούς κωδικούς μπροστά στο προσωπικό της Τράπεζας ή του Ιδρύματος Πληρωμών, που θα μπορούσαν να χρησιμοποιηθούν διαπράττοντας απάτη εις βάρος του.

Μόλις ο Κάτοχος αποκτήσει το εγκεκριμένο πιστοποιητικό, θα μπορεί να υπογράψει ένα έγγραφο με τον εξής τρόπο:

1. Ο χρήστης παρουσιάζεται στο ταμείο ενός υποκαταστήματος Τράπεζας ή Ιδρύματος Πληρωμών (επανδρωμένος σταθμός) και αναγνωρίζεται από το προσωπικό (τον ταμία, για παράδειγμα) σε κανονική λειτουργία.
2. Κατά την υπογραφή ενεργοποιείται μπροστά από τον χρήστη μια ειδική οθόνη εξοπλισμένη με κάμερα web.
3. Ο Κάτοχος, αφού επαληθεύσει στην οθόνη αυτή το έγγραφο προς υπογραφή και αποφασίσει να προχωρήσει με τη λειτουργία υπογραφής, ξεκινά στο smartphone του τη δημιουργία ενός OTP το οποίο εμφανίζεται επίσης σε μορφή γραμμικού κώδικα.
4. Ο Κάτοχος μπορεί σε αυτό το σημείο, τοποθετώντας το smartphone του προς την κάμερα web, να επιτρέπει την ανάγνωση του OTP που δημιουργήθηκε στο βήμα 3 και να ξεκινήσει την καθαυτή διαδικασία υπογραφής.
5. Μόλις υπογραφεί το έγγραφο, το σύστημα ειδοποιεί άμεσα μέσω SMS.

Για την υπογραφή περισσότερων εγγράφων, επαναλαμβάνονται τα βήματα 2 έως 5.

I.2.3. Διαδικασία υπογραφής για πελάτες Prospect

Η διαχείριση της διαδικασίας έκδοσης του εγκεκριμένου πιστοποιητικού υπογραφής εξ αποστάσεως γίνεται επίσης και από Πελάτες Prospect κατά τη διάρκεια δραστηριοτήτων Onboarding (απόκτηση πελάτη).

Η διαδικασία είναι συμβατή με τα κύρια προγράμματα περιήγησης (Chrome, Firefox, Edge, Safari) και με τις πιο πρόσφατες κινητές συσκευές τεχνολογίας Android ή Apple.

Αποτελείται από τα εξής βήματα:

1. Στην αρχή της διαδικασίας, ζητείται από τον Πελάτη Prospect να εισαγάγει τα προσωπικά του δεδομένα προκειμένου να επιτραπεί η επακόλουθη βέβαιη ταυτοποίηση, μετά από την υπογραφή της πολιτικής απορρήτου της QTSP INTESA.
2. Η Τράπεζα / Ίδρυμα προβαίνει στην αποστολή ενός SMS του οποίου το κείμενο περιέχει ένα OTP (One Time Password) με προσωρινή ισχύ: ο Πελάτης Prospect πρέπει να εισαγάγει αυτόν τον κωδικό για την επαλήθευση της διαθεσιμότητας της κινητής συσκευής που δηλώθηκε κατά την εισαγωγή δεδομένων.
3. Μόλις ολοκληρωθεί η επαλήθευση που αναφέρθηκε στο προηγούμενο σημείο, ο Πελάτης Prospect προχωρά στη συνέχεια στην διαβίβαση των εγγράφων ταυτότητας στην Τράπεζα / Ίδρυμα: τα δημογραφικά δεδομένα θα εισαχθούν από τον Prospect ή θα ληφθούν από τα έγγραφα μέσω ενός συστήματος OCR.
4. Μόλις ολοκληρωθεί η καταχώρηση, η Τράπεζα θα στείλει στον Πελάτη Prospect τη συμβατική τεκμηρίωση που ο Πελάτης Prospect μπορεί να υπογράψει με ένα εγκεκριμένο πιστοποιητικό ψηφιακής υπογραφής εξ αποστάσεως (FDR) που εκδίδεται από την QTSP INTESA.
5. Όπως και με τη διαδικασία που περιγράφηκε για τις διαδικτυακές τραπεζικές συναλλαγές, στον Πελάτη Prospect θα παρουσιαστεί η τεκμηρίωση αίτησης του πιστοποιητικού της QTSP INTESA.
6. Η λήψη και προβολή αυτής της τεκμηρίωσης θα πρέπει να υπογραφεί υποχρεωτικά διαγράφοντας τα τετραγωνάκια στη λίστα του εγγράφου και τοποθετώντας μια ηλεκτρονική υπογραφή μέσω της εισαγωγής ενός OTP που λαμβάνεται μέσω SMS από την QTSP INTESA.
7. Εάν το OTP που παρασχέθηκε από την INTESA QTSP επαληθευτεί θετικά, θα είναι δυνατόν στη συνέχεια να εκδοθεί το εγκεκριμένο πιστοποιητικό, διαφορετικά θα πρέπει να ζητηθεί ένα νέο OTP.
8. Κατά τη δημιουργία του πιστοποιητικού, ωστόσο, είναι απαραίτητο να εισαχθεί ένα PIN, το οποίο στη συνέχεια θα ζητείται κάθε φορά που χρησιμοποιείται το πιστοποιητικό υπογραφής.
9. Το πιστοποιητικό που έχει μόλις εκδοθεί θα μπορεί, ωστόσο, να χρησιμοποιηθεί μόνο για την υπογραφή της συμβατικής πρότασης και για κανένα άλλο έγγραφο έως ότου η Τράπεζα ολοκληρώσει τους απαραίτητους προκαταρκτικούς ελέγχους για το άνοιγμα τρεχούμενου λογαριασμού.
10. Εάν οι επαληθεύσεις της Τράπεζας έχουν θετική έκβαση και ο τρεχούμενος λογαριασμός ενεργοποιηθεί, ο Πελάτης Prospect θα είναι σε θέση να χρησιμοποιήσει το πιστοποιητικό που εκδόθηκε, σύμφωνα με τα όρια χρήσης του, σε συναλλαγές με την Τράπεζα· εάν, αντιθέτως, η Τράπεζα αποφασίσει να μην ολοκληρώσει τη διαδικασία του αιτήματος για άνοιγμα τρεχούμενου λογαριασμού, το ίδιο πιστοποιητικό θα ανακληθεί, εμποδίζοντας την περαιτέρω χρήση του.
11. Και στις δύο περιπτώσεις που αναφέρθηκαν στο προηγούμενο σημείο, ο Πελάτης Prospect θα εξακολουθεί να ενημερώνεται για το αποτέλεσμα των επαληθεύσεων και για την ενδεχόμενη ανάκληση του πιστοποιητικού.

I.3. Αυθεντικοποίηση με OTP Token

Τέλος, μπορεί να χρησιμοποιηθεί αυθεντικοποίηση που συνδέεται με τη χρήση φυσικών OTP token (πολύ διαδεδομένα στον τραπεζικό και χρηματοοικονομικό κόσμο).

Η χρήση αυτού του φυσικού OTP token προορίζεται επί του παρόντος μόνο για πρόσβαση σε μη επανδρωμένους σταθμούς (συνήθως σε τραπεζικό σταθμό εξ αποστάσεως home banking).

Ο Κάτοχος συνδέεται με την τραπεζική ή οικονομική εφαρμογή μέσω των προσωπικών του κωδικών για πρόσβαση στην εφαρμογή και, για να ξεκινήσει η διαδικασία υπογραφής, θα εισάγει τον κωδικό PIN και τον OTP που θα έχει εν τω μεταξύ δημιουργηθεί και προβληθεί στην οθόνη Token.

J. Λειτουργικές διαδικασίες για την επαλήθευση της υπογραφής

Τα έγγραφα που υπογράφονται με τους τρόπους που περιγράφηκαν παραπάνω θα είναι αποκλειστικά σε μορφή

PDF: αυτή η μορφή υπογραφής θεωρείται όντως εύχρηστη στο πλαίσιο τραπεζικών ή χρηματοοικονομικών εφαρμογών.

Η επαλήθευση των υπογεγραμμένων εγγράφων θα μπορεί εύκολα να πραγματοποιείται χρησιμοποιώντας το λογισμικό *Acrobat Reader DC*, μια εφαρμογή ικανή να επαληθεύει όλους τους τύπους εγκεκριμένης ηλεκτρονικής υπογραφής σε μορφή PDF που παράγονται στην Ευρωπαϊκή Ένωση σύμφωνα με τον Κανονισμό eIDAS.

Μπορείτε να κατεβάσετε το Acrobat Reader DC δωρεάν από τον ιστότοπο της Adobe, *https://www.adobe.com/it/*

Κ. Τρόποι ανάκλησης και αναστολής πιστοποιητικών

Σύμφωνα με τον Κανονισμό eIDAS, οι πληροφορίες που αφορούν την κατάσταση του πιστοποιητικού είναι διαθέσιμες μέσω του πρωτοκόλλου OCSP, στη διεύθυνση URL που αναφέρεται στο ίδιο το πιστοποιητικό.

Η επικύρωση της ανάκλησης και της αναστολής των πιστοποιητικών μπορεί επίσης να πραγματοποιείται με την εισαγωγή τους στον κατάλογο CRL (Άρθ.22 του DPCM). Το προφίλ των CRL συμμορφώνεται με το πρότυπο RFC 3280. Αυτή η λίστα, υπογεγραμμένη από την Certification Authority που εκδίδει το πιστοποιητικό, ενημερώνεται με προκαθορισμένη συχνότητα και σύμφωνα με την ισχύουσα νομοθεσία.

Η λίστα CRL είναι επίσης διαθέσιμη στο μητρώο πιστοποιητικών.

Σε περιπτώσεις όπου η ανάκληση ή αναστολή πραγματοποιείται με πρωτοβουλία του Φορέα Πιστοποίησης ή του Ενδιαφερόμενου Τρίτου Μέρους (άρθ. 23, 25, 27 και 29 του DPCM), ο Φορέας Πιστοποίησης ειδοποιεί τον Κάτοχο για το αίτημα και τη στιγμή κατά την οποία το απαιτούμενο συμβάν θα τεθεί σε ισχύ.

Κατά τη διάρκεια του αιτήματος, θα καθοριστεί η ημερομηνία και η ώρα από την οποία θα ανακληθεί το πιστοποιητικό (Άρθ.24, εδάφιο 1, DPCM).

Κ.1. Ανάκληση πιστοποιητικών

Ένα πιστοποιητικό μπορεί να ανακληθεί κατόπιν αιτήματος του Κατόχου, του Ενδιαφερόμενου Τρίτου Μέρους ή της Certification Authority (δηλαδή του QTSP).

Το ανακληθέν πιστοποιητικό δεν μπορεί να επανεργοποιηθεί με κανέναν τρόπο.

Κ.1.1. Ανάκληση κατόπιν αιτήματος του Κατόχου

Ο Κάτοχος μπορεί να ζητήσει την ανάκληση με πρόσβαση σε μια συγκεκριμένη ενότητα που διατίθεται στο πλαίσιο των υπηρεσιών της Τράπεζας ή του Ιδρύματος Πληρωμών ή επικοινωνώντας απευθείας με την Εξυπηρέτηση Πελατών της Τράπεζας ή του Ιδρύματος Πληρωμών.

Ο QTSP, που ειδοποιείται από την Τράπεζα / το Ίδρυμα, ο οποίος στο μεταξύ θα έχει επίσης κλειδώσει τους κωδικούς πρόσβασης του Κατόχου, θα προβεί στην άμεση ανάκληση του πιστοποιητικού.

Κ.1.2. Ανάκληση κατόπιν αιτήματος του Ενδιαφερόμενου Τρίτου Μέρους

Η Τράπεζα ή το Ίδρυμα Πληρωμών, ως Ενδιαφερόμενο Τρίτο Μέρος, μπορεί να ζητήσει την ανάκληση του πιστοποιητικού.

Ο QTSP, αφού εξακριβωθεί η ορθότητα του αιτήματος, θα ειδοποιήσει τους ενδιαφερόμενους Κατόχους σχετικά με την ανάκληση χρησιμοποιώντας τα κανάλια επικοινωνίας που έχουν προσδιοριστεί με τον Κάτοχο κατά την καταχώρηση ή όπως είχαν ενημερωθεί και γνωστοποιηθεί από τον Κάτοχο στον QTSP, επίσης μέσω των LRA (παρ. C.2. *Υποχρεώσεις του Κατόχου*).

Κ.1.3. Ανάκληση με πρωτοβουλία του Φορέα Πιστοποίησης

Ο Φορέας Πιστοποίησης που σκοπεύει να ανακαλέσει το Εγκεκριμένο Πιστοποιητικό, εκτός από περιπτώσεις δικαιολογημένης έκτακτης ανάγκης, δίνει σχετική προηγούμενη ειδοποίηση μέσω e-mail ή PEC στην Τράπεζα / στο Ίδρυμα (Ενδιαφερόμενο Τρίτο Μέρος) ενώ ταυτόχρονα θα σταλεί ειδοποίηση στον Κάτοχο χρησιμοποιώντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου που παρασχέθηκε κατά την αίτηση του πιστοποιητικού ή στη διεύθυνση κατοικίας, προσδιορίζοντας τους λόγους της ανάκλησης, καθώς και την ημερομηνία και την ώρα από την οποία ισχύει η ανάκληση.

Κ.1.4. Ανάκληση πιστοποιητικών που σχετίζονται με κλειδιά πιστοποίησης

Όσον αφορά τις εξής περιπτώσεις:

- διακινδύνευσης του κλειδιού πιστοποίησης
- τερματισμού της δραστηριότητας

ο Φορέας Πιστοποίησης προβαίνει στην ανάκληση των αντίστοιχων πιστοποιητικών πιστοποίησης και των πιστοποιητικών εγγραφής που έχουν υπογραφεί με το ίδιο κλειδί πιστοποίησης.

Εντός 24 ωρών, ο Φορέας Πιστοποίησης θα ειδοποιήσει σχετικά με την ανάκληση την Ιταλική Υπηρεσία για την Ψηφιακή Τεχνολογία και τους Κατόχους.

K.2. Αναστολή πιστοποιητικών

Όσον αφορά τις μεθόδους αναστολής και γνωστοποίησης της, το ίδιο ισχύει και για τις μεθόδους ανάκλησης όπως επεξηγήθηκε στην παρ. *K.1*.

Η αναστολή ενός πιστοποιητικού προβλέπεται σε περίπτωση που πρέπει να πραγματοποιηθούν συμπληρωματικές έρευνες για να εξακριβωθεί εάν όντως πρέπει να ανακληθεί (για παράδειγμα σε περιπτώσεις όπου υπάρχει φόβος για απώλεια / κλοπή του OTP token ή εάν πρέπει να γίνουν διερευνήσεις ώστε να επιβεβαιωθεί και να αποδειχθεί ο τερματισμός του Κατόχου από το καθήκον σχετικά με το οποίο του εκδόθηκε το πιστοποιητικό, κ.λπ.).

Η αίτηση αναστολής μπορεί να υποβληθεί από όλες τις οντότητες που προβλέπονται στο DPCM βάσει των Άρθρων 27, 28 και 29 (Φορέας Πιστοποίησης, Κάτοχος, Ενδιαφερόμενο Τρίτο Μέρος).

Ελλείψει ενημερώσεων από τον Κάτοχο, το πιστοποιητικό θα ανακαλείται αυτόματα μετά από περίοδο αναστολής 90 (ενενήντα) ημερών ή οπωσδήποτε εντός της ημερομηνίας λήξης του ίδιου πιστοποιητικού.

Σε κάθε περίπτωση, η ημερομηνία έναρξης ισχύος της ανάκλησης θα συμπίπτει με την ημερομηνία έναρξης ισχύος της αναστολής.

K.2.1. Αναστολή κατόπιν αιτήματος του Κατόχου

Ο Κάτοχος μπορεί να ζητήσει την αναστολή του πιστοποιητικού αφού αποκτήσει πρόσβαση σε μια συγκεκριμένη ενότητα που διατίθεται στο πλαίσιο των υπηρεσιών της Τράπεζας ή του Ιδρύματος Πληρωμών ή επικοινωνώντας απευθείας με την Εξυπηρέτηση Πελατών της Τράπεζας ή του Ιδρύματος Πληρωμών.

Ο Φορέας Πιστοποίησης προβαίνει στην αναστολή η οποία θα γνωστοποιηθεί στον Κάτοχο χρησιμοποιώντας συγκεκριμένες λειτουργίες που διατίθενται στο πλαίσιο των υπηρεσιών της Τράπεζας ή του Ιδρύματος Πληρωμών.

Ο Κάτοχος θα μπορεί στη συνέχεια να ζητήσει την επαναφορά του πιστοποιητικού σύμφωνα με τις μεθόδους που διατίθενται πάντα από την Τράπεζα ή το Ίδρυμα Πληρωμών.

Ελλείψει περαιτέρω ενημερώσεων, το πιστοποιητικό που αναστάλθηκε θα ανακληθεί αυτόματα στο τέλος της περιόδου αναστολής και η ημερομηνία ανάκλησης θα συμπίπτει με την ημερομηνία έναρξης ισχύος της αναστολής.

K.2.2. Αναστολή κατόπιν αιτήματος του Ενδιαφερόμενου Τρίτου μέρους

Η Τράπεζα ή το Ίδρυμα Πληρωμών, ως Ενδιαφερόμενο Τρίτο Μέρος, μπορεί να ζητήσει την αναστολή του πιστοποιητικού.

Ο Φορέας Πιστοποίησης, αφού εξακριβωθεί η ορθότητα του αιτήματος, θα αναστείλει έγκαιρα το πιστοποιητικό και θα ειδοποιήσει τους ενδιαφερόμενους Κατόχους σχετικά με την αναστολή μέσω e-mail ή με γνωστοποίηση μέσω των υπηρεσιών που παρέχονται από την Τράπεζα ή το Ίδρυμα Πληρωμών.

K.2.3. Αναστολή με πρωτοβουλία του Φορέα Πιστοποίησης

Με εξαίρεση περιπτώσεις δικαιολογημένης έκτακτης ανάγκης, ο Φορέας Πιστοποίησης μπορεί να αναστείλει το πιστοποιητικό ειδοποιώντας προηγουμένως τον Κάτοχο σχετικά στη διεύθυνση ηλεκτρονικού ταχυδρομείου που παρασχέθηκε κατά την αίτηση του πιστοποιητικού όταν έγινε η καταχώρηση ή στη διεύθυνση διαμονής, διευκρινίζοντας τους λόγους της αναστολής και ημερομηνία και ώρα από τις οποίες θα τεθεί σε ισχύ αυτή η αναστολή.

Παρόμοια γνωστοποίηση θα αποσταλεί επίσης από τον Φορέα Πιστοποίησης στο Ενδιαφερόμενο Τρίτο Μέρος.

L. Τρόπος αντικατάστασης των κλειδιών

L.1. Αντικατάσταση των εγκεκριμένων πιστοποιητικών και των κλειδιών του Κατόχου

Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικής υπογραφής που εκδίδονται από τον Φορέα Πιστοποίησης στο πλαίσιο που περιγράφεται σε αυτό το Εγχειρίδιο Λειτουργίας ισχύει για 36 (τριάντα έξι) μήνες από την ημερομηνία έκδοσης.

Στο τέλος της προαναφερόμενης προθεσμίας, θα καταστεί απαραίτητη η δημιουργία ενός νέου ζεύγους κλειδιών υπογραφής και ταυτόχρονα η έκδοση ενός νέου πιστοποιητικού.

Σε αυτήν την περίπτωση, η διαδικασία που ακολουθείται για την έκδοση του νέου πιστοποιητικού θα είναι παρόμοια με εκείνη που αναφέρεται στη φάση της πρώτης χορήγησης, μετά τη φάση ταυτοποίησης του Κατόχου που δεν πρέπει να επαναληφθεί.

L.2. Αντικατάσταση των κλειδιών του Φορέα Πιστοποίησης

L.2.1. Αντικατάσταση των κλειδιών πιστοποίησης λόγω έκτακτης ανάγκης

Η διαδικασία που χρησιμοποιείται σε περίπτωση βλάβης της συσκευής υπογραφής (HSM) η οποία περιέχει τα κλειδιά πιστοποίησης (CA και TSCA) ή καταστροφής στα κεντρικά γραφεία περιγράφεται στην ενότητα *P*. *Διαδικασία διαχείρισης καταστροφικών γεγονότων.*

L.2.2. Προγραμματισμένη αντικατάσταση των κλειδιών πιστοποίησης

Εντός ενός χρονικού διαστήματος που συνάδει με την ισχύουσα νομοθεσία, πριν από τη λήξη του πιστοποιητικού που σχετίζεται με τα ζεύγη Κλειδιών Πιστοποίησης (CA και TSCA), που χρησιμοποιούνται από τα συστήματα έκδοσης των πιστοποιητικών υπογραφής και των πιστοποιητικών TSA και τα συστήματα έκδοσης πιστοποιητικών, ο Φορέας Πιστοποίησης θα ενεργήσει σύμφωνα με όσα έχουν καθοριστεί από το Άρθ.30 του DPCM.

L.3. Κλειδιά του συστήματος ηλεκτρονικής χρονοσφραγίδας (TSA)

Σύμφωνα με τις διατάξεις του Άρθρου 49, εδάφιο 2, του DPCM, προκειμένου να περιοριστεί ο αριθμός των χρονοσήμων που δημιουργούνται με το ίδιο ζεύγος κλειδιών χρονοσφραγίδας, αυτά αντικαθίστανται εντός 90 (ενενήντα) ημερών από την ημερομηνία της έκδοσής τους. Ταυτόχρονα, εκδίδεται πιστοποιητικό σε σχέση με το νέο ζεύγος κλειδιών (χωρίς ανάκληση του προηγούμενου που σχετίζεται με το ζεύγος κλειδιών που αντικαταστάθηκε).

M. Μητρώο πιστοποιητικών

M.1. Τρόπος διαχείρισης του Μητρώου Πιστοποιητικών

Στο μητρώο πιστοποιητικών, η INTESA δημοσιεύει:

1. Τα πιστοποιητικά των κλειδιών υπογραφής και του συστήματος χρονοσφραγίδας
2. Τα πιστοποιητικά των κλειδιών πιστοποίησης (CA και TSCA)
3. Τα πιστοποιητικά που εκδόθηκαν μετά την αντικατάσταση των κλειδιών πιστοποίησης
4. Πιστοποιητικά για τα κλειδιά υπογραφής της Ιταλικής Υπηρεσίας για την Ψηφιακή Τεχνολογία (DPCM Άρθ.42, εδάφιο 1)
5. Οι λίστες ανάκλησης και αναστολής (CRL)

Οι πράξεις που αφορούν το μητρώο πιστοποιητικών διεξάγονται μόνο από άτομα εξουσιοδοτημένα για τον σκοπό αυτό, των οποίων ο αριθμός είναι επαρκής για την πρόληψη αθέμιτων ενεργειών από ένα περιορισμένο αριθμό υπαλλήλων.

Ο Φορέας Πιστοποίησης διατηρεί ένα αντίγραφο αναφοράς του μητρώου πιστοποιητικών μη προσβάσιμο στους μη έχοντας εργασία. Το αντίγραφο αυτό ενημερώνει το λειτουργικό αντίγραφο σε πραγματικό χρόνο, προσβάσιμο από τους χρήστες με το πρωτόκολλο LDAP.

Η επαλήθευση της συμμόρφωσης μεταξύ του αντιγράφου αναφοράς και του λειτουργικού αντιγράφου γίνεται συστηματικά.

Μ.2. Λογική πρόσβαση στο Μητρώο Πιστοποιητικών

Το αντίγραφο αναφοράς τοποθετείται εντός ενός αποκλειστικού δικτύου που προστατεύεται από κατάλληλες συσκευές, επομένως δεν είναι προσβάσιμο σε άλλους παρά από τον διακομιστή έκδοσης πιστοποιητικών, ο οποίος καταγράφει τα πιστοποιητικά που εκδόθηκαν και τα CRL.

Η πρόσβαση στα λειτουργικά αντίγραφα γίνεται στη διεύθυνση ***ldap: //x500.e-trustcom.intesa.it*** με πρωτόκολλο LDAP.

Ο Φορέας Πιστοποίησης επιτρέπει επίσης την πρόσβαση στα CRL μέσω του πρωτοκόλλου http, στη διεύθυνση URL που αναφέρεται στο πεδίο CDP (CRL Distribution Point) του πιστοποιητικού.

Μ.3. Φυσική πρόσβαση στις εγκαταστάσεις των συστημάτων που προορίζονται για το μητρώο πιστοποιητικών

Οι υπάλληλοι που είναι εξουσιοδοτημένοι για την άμεση διαχείριση του μητρώου πιστοποιητικών μπορούν να έχουν πρόσβαση στον χώρο όπου είναι εγκατεστημένο το σύστημα και να το χειρίζονται μόνο σε λειτουργία διπλού ελέγχου για την αποφυγή αθέμιτων ενεργειών.

Οι υπάλληλοι αρμόδιοι για τη διαχείριση των συστημάτων, τη διαχείριση δικτύου, συντήρηση, κ.λπ. μπορούν να έχουν πρόσβαση στον χώρο όπου είναι εγκατεστημένο το σύστημα και οι συγκεκριμένοι υπάλληλοι μπορούν να το χειρίζονται μόνο παρουσία υπαλλήλων εξουσιοδοτημένων για τη διαχείριση του μητρώου πιστοποιητικών σύμφωνα με τις μεθόδους που επεξηγήθηκαν προηγουμένως για τους εξουσιοδοτημένους υπάλληλους.

Ν. Τρόπος προστασίας των προσωπικών δεδομένων

Τα μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων συμμορφώνονται με τα μέτρα που προβλέπονται από τον Ευρωπαϊκό Κανονισμό 679/2016 (ΓΚΠΔ) και τις επακόλουθες τροποποιήσεις και ενσωματώσεις.

Ο. Διαδικασία διαχείρισης αντιγράφων ασφαλείας

Τα πληροφοριακά αρχεία που αποτελούν αντικείμενο αντιγράφων ασφαλείας έχουν ως εξής:

- ΜΗΤΡΩΟ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ, ψηφιακό αρχείο που περιέχει όσα ορίζονται στην παρ. Μ
- ΛΕΙΤΟΥΡΓΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ, ψηφιακό αρχείο στο οποίο αποθηκεύονται όλες οι πληροφορίες που έλαβε ο Κάτοχος κατά την καταχώρηση και την αίτηση πιστοποιητικού, καθώς και αιτήσεις ανάκλησης και αναστολής, συνοδευόμενες από τα σχετικά έγγραφα
- ΗΜΕΡΟΛΟΓΙΟ ΕΛΕΓΧΟΥ, αρχείο που αποτελείται από το σύνολο των καταχωρήσεων που έγιναν αυτόματα από τα συστήματα εγκατεστημένα στην υπηρεσία πιστοποίησης του QTSP (Άρθ.36 του DPCM)
- ΨΗΦΙΑΚΟ ΑΡΧΕΙΟ ΧΡΟΝΟΣΗΜΩΝ, περιέχει τα χρονόσημα που δημιουργούνται από το σύστημα ηλεκτρονικής χρονοσφραγίδας (άρθρο 53, εδάφιο 1, του DPCM)
- ΛΕΙΤΟΥΡΓΙΚΟ ΜΗΤΡΩΟ ΤΩΝ ΓΕΓΟΝΟΤΩΝ ΧΡΟΝΟΣΦΡΑΓΙΔΑΣ, μητρώο στο οποίο αποθηκεύονται αυτόματα τα γεγονότα που εμπίπτουν στις δραστηριότητες χρονοσφραγίδας για τα οποία προβλέπεται η καταχώρηση οποιασδήποτε ανωμαλίας ή απόπειρας παραβίασης που θα μπορούσε να θέσει σε κίνδυνο τη λειτουργία του συστήματος χρονοσφραγίδας (Άρθ.52) του DPCM)

Η διατήρηση, που αφορά όλα τα αντίγραφα ασφαλείας που περιγράφηκαν, συμμορφώνεται με τις διατάξεις των σχετικών ισχυόντων κανονισμών.

Ρ. Διαδικασία διαχείρισης καταστροφικών γεγονότων

Η INTESA QTSP διαθέτει σχέδιο έκτακτης ανάγκης για τη διαχείριση καταστροφικών γεγονότων που περιλαμβάνει τις ακόλουθες φάσεις:

- διαχείριση έκτακτης ανάγκης: σε αυτήν τη φάση, είναι εγγυημένη η συνεχής πρόσβαση στα CRL· η

έκδοσή τους μπορεί να υποστεί καθυστερήσεις λόγω της ανάγκης ενεργοποίησης του εφεδρικού διακομιστή της CA που βρίσκεται στον εφεδρικό χώρο

- μεταβατική διαχείριση: κατά την περίοδο αυτή, εξασφαλίζεται η έκδοση πιστοποιητικών και η επαναφορά περαιτέρω λύσεων disaster recovery
- επιστροφή στην κανονική λειτουργία: στον ίδιο αρχικό χώρο ή σε άλλο εναλλακτικό αλλά οριστικό

Θα πρέπει να σημειωθεί ότι η παρουσία αντιγράφων του λειτουργικού αντιγράφου του μητρώου πιστοποιητικών που διανέμονται σε διάφορα σημεία επιτρέπει ούτως ή άλλως, σε περίπτωση διακοπής λειτουργίας ενός από τους χώρους κεντρικών γραφείων, την πρόσβαση στο περιεχόμενο του μητρώου πιστοποιητικών ενημερωμένου έως τη στιγμή της διακοπής.

Για την ανταπόκριση στη διαχείριση έκτακτης ανάγκης, προβλέπεται η αντιγραφή στον εφεδρικό χώρο του μητρώου πιστοποιητικών, των δεδομένων του συστήματος έκδοσης των πιστοποιητικών και η παρέμβαση εντός 24 ωρών από προσωπικό ικανό να ενεργοποιήσει τη λειτουργία έκδοσης CRL. Εκτός από τη διαχείριση των SW και HW, το εν λόγω προσωπικό εκπαιδεύεται επίσης σε καταστάσεις έκτακτης ανάγκης.

Ένα έντυπο αντίγραφο του σχεδίου έκτακτης ανάγκης κατατίθεται σε όλα τα κεντρικά γραφεία που συμμετέχουν στη διαχείριση καταστροφικών γεγονότων.

Q. Διαδικασίες τοποθέτησης και προσδιορισμού της χρονικής αναφοράς

Όλα τα μηχανήματα του συστήματος PKI του Φορέα Πιστοποίησης συγχρονίζονται με το *I.N.RI.M. - Εθνικό Ινστιτούτο Μετρολογικής Έρευνας* του Τορίνο (πρώην *Εθνικό Ηλεκτροτεχνικό Ινστιτούτο Galileo Ferraris*). Αυτή η λειτουργία διεξάγεται με ένα στοχευμένο λογισμικό εγκατεστημένο σε κάθε διακομιστή το οποίο, μέσω του πρωτοκόλλου NTP (Network Time Protocol), συνδέεται με τον διαμορφωμένο απομακρυσμένο διακομιστή.

Το Network Time Protocol (NTP) είναι ένας από τους πιο προσεγμένους και ευέλικτους τρόπους μετάδοσης πληροφοριών ώρας και ημερομηνίας στο διαδίκτυο. Επιτρέπει τη διατήρηση του συγχρονισμού υπολογιστών συνδεδεμένων ο ένας με τον άλλο μέσω τοπικών, μητροπολιτικών ή ακόμη και παγκόσμιων δικτύων (Διαδίκτυο) χρησιμοποιώντας μια ιεραρχική δομή τύπου πυραμίδας.

Το *I.N.RI.M.* παρέχει μια υπηρεσία συγχρονισμού για πληροφοριακά συστήματα που είναι συνδεδεμένα στο Διαδίκτυο, που βασίζεται σε δύο κύριους διακομιστές NTP εγκατεστημένους στο Εργαστήριο Δείγματος Χρόνου και Συχνότητας. Συγχρονίζονται, μέσω ενός συστήματος δημιουργίας κωδικών ημερομηνίας, από τα ατομικά δείγματα δέσμης καισίου που χρησιμοποιούνται για τη δημιουργία της Ιταλικής εθνικής κλίμακας UTC (IT). Η χρονική απόκλιση μεταξύ των διακομιστών NTP του I.N.RI.M και της Ιταλικής εθνικής χρονικής κλίμακας τηρείται υπό έλεγχο και συνήθως είναι μικρότερη από μερικά χιλιοστά του δευτερολέπτου. Η επιτευκτή ακρίβεια συγχρονισμού εξαρτάται από την τυπολογία του δικτύου και από την απόσταση μεταξύ του διακομιστή NTP και του υπολογιστή που θα επιλεγεί για τον συγχρονισμό. Οι τυπικές τιμές απόκλισης είναι μικρότερες από ένα χιλιοστό του δευτερολέπτου για συστήματα που ανήκουν στο ίδιο δίκτυο και μπορούν να φτάσουν μερικές εκατοντάδες χιλιοστά του δευτερολέπτου για απομακρυσμένα δίκτυα.

Το λογισμικό που είναι εγκατεστημένο σε χώρο του Φορέα Πιστοποίησης συνδέεται με τον απομακρυσμένο διακομιστή σε τακτά χρονικά διαστήματα και, αφού αποκτήσει την τρέχουσα ώρα, προχωρά στη διόρθωση του clock της τοπικής μηχανής μέσω εξελιγμένων αλγορίθμων.

Οι χρονικές αναφορές που τίθενται από τις εφαρμογές είναι συμβολοσειρές σε μορφή ημερομηνίας (HH/MM/EEEE ωω: λλ: δδ), με την ακρίβεια του δευτερολέπτου, που αντιπροσωπεύουν την τοπική ώρα, με βάση τη διαμόρφωση του μηχανήματος. Αυτές οι αναφορές συμμορφώνονται με το DPCM Άρθ.51.

Κάθε καταχώρηση που πραγματοποιείται στο ημερολόγιο ελέγχου περιέχει μια χρονική αναφορά η οποία, εφόσον δημιουργείται με τον τρόπο που περιγράφηκε εδώ, μπορεί να αντιταχθεί έναντι τρίτων (άρθ.41 του DPCM).

Q.1. Τρόπος αίτησης και επαλήθευσης χρονοσήμων

Ο Φορέας Πιστοποίησης θέτει ένα χρονόσημο (*εγκεκριμένη ηλεκτρονική χρονοσφραγίδα* σύμφωνα με τον Καν. eIDAS) σε όλα τα έγγραφα που υπογράφει ο Κάτοχος στο πλαίσιο των υπηρεσιών που περιγράφονται σε αυτό το Εγχειρίδιο Λειτουργίας.

Η τοποθέτηση αυτού του χρονοσήμου είναι διαδικασία ενσωματωμένη στη λειτουργία υπογραφής και δεν απαιτεί καμία συγκεκριμένη δραστηριότητα εκ μέρους του Κατόχου.

R. Lead Time και πίνακας Raci για την έκδοση πιστοποιητικών

Παρατίθεται στη συνέχεια ο πίνακας που σχετίζεται με τον «Lead Time Διαδικασίας» για τη διαχείριση των αιτήσεων έκδοσης, ανάκλησης, αναστολής και επανεργοποίησης πιστοποιητικών.

Θέμα	Αίτηση	Εμπλεκόμενος Φορέας	Δράση Εμπλεκόμενου Φορέα	Εμπλεκόμενος Φορέας	Δράση Εμπλεκόμενου Φορέα
Χρήστης, Αιτών, Κάτοχος πιστοποιητικού	*Αίτηση έκδοσης πιστοποιητικού προς LRA*	*Τράπεζα / Ίδρυμα (ενεργεί ως) Τοπική RA*	*Εκδίδει εντολή δημοσίευσης του πιστοποιητικού προς CA μετά την επαλήθευση ταυτότητας*	*Certification Authority*	*Διεκπεραίωση αίτησης πιστοποίησης*
Χρήστης, Αιτών, Κάτοχος πιστοποιητικού	*Αίτημα ανάκλησης πιστοποιητικού προς RA ή LRA*	*Intesa (ενεργεί ως Registration Authority (RA) ή Τράπεζα / Ίδρυμα (ενεργεί ως LRA)*	*Εκδίδει εντολή ανάκλησης του πιστοποιητικού προς CA μετά την επαλήθευση ταυτότητας*	*Certification Authority*	*Διεκπεραίωση αιτήματος ανάκλησης*
Χρήστης, Αιτών, Κάτοχος πιστοποιητικού	*Αίτημα αναστολής πιστοποιητικού προς RA ή LRA*	*Intesa (ενεργεί ως Registration Authority (RA) ή Τράπεζα / Ίδρυμα (ενεργεί ως LRA)*	*Εκδίδει εντολή αναστολής του πιστοποιητικού προς CA μετά την επαλήθευση ταυτότητας*	*Certification Authority*	*Διεκπεραίωση αιτήματος αναστολής*
Χρήστης, Αιτών, Κάτοχος πιστοποιητικού	*Αίτημα επανεργοποίησης πιστοποιητικού προς RA ή LRA*	*Intesa (ενεργεί ως Registration Authority (RA) ή Τράπεζα / Ίδρυμα (ενεργεί ως LRA)*	*Εκδίδει εντολή επανεργοποίησης πιστοποιητικού προς CA μετά την επαλήθευση ταυτότητας*	*Certification Authority*	*Διεκπεραίωση αιτήματος επανεργοποίησης*

Παρατίθεται στη συνέχεια ο πίνακας RACI σχετικά με τον προσδιορισμό των αρμοδιοτήτων των φορέων που εμπλέκονται στις αιτήσεις έκδοσης, ανάκλησης, αναστολής και επανεργοποίησης πιστοποιητικών.

Εμπλεκόμενο Πρόσωπο	Responsible	Accountable	Consulted	Informed
Registration Authority	***X***			
Local Registration Authority	***X***			
Certification Authority		***X***		
Χρήστης, Αιτών, Κάτοχος πιστοποιητικού			***X***	***X***

5. Τεχνικές Αναφορές

ETSI-319.401	ETSI EN 319 401 v2.1.1 - Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 V2.1.0 - Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.411-3	ETSI EN 319 411-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates Part 3: Policy requirements for Certification Authorities issuing public key certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI), Certificate Profiles Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI), Certificate Profiles Part 2: Certificate profile for certificates issued to natural persons
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI), Certificate Profiles Part 5: QCStatements
Rec ITU-R	Recommandation ITU-R TF.460-6, Annex 1 – Time Scales
RFC5905	Network Time Protocol (Πρωτόκολλο NTP)
ETSI-319.421	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI), Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic Signatures and Infrastructures (ESI), Time-stamping protocol and timestamp token profiles
Rec ITU-R	Recommandation ITU-R TF.460-6, Annex 1 – Time Scales
RFC5905	Network Time Protocol (Πρωτόκολλο NTP)

------- ΤΕΛΟΣ ΕΓΓΡΑΦΟΥ -------