Προτεινόμενη διαδικασία
ελέγχου ακεραιότητας εγγράφων σε μορφή PDF
που έχουν υπογραφεί με εγκεκριμένες ηλεκτρονικές
υπογραφές ή σφραγίδες
και
του τρόπου επικύρωσης αυτών

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

Ιστορικό εγγράφου		
Έκδοση 1.0	Δεκέμβριος 2021	Αρχική έκδοση

ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

Περιεχόμενα

Εισαγωγή

Το παρόν έγγραφο συντάχθηκε από την ΕΕΤΤ προκειμένου να παρασχεθούν χρηστικές πληροφορίες ενημέρωσης σε απάντηση σχετικών ερωτημάτων που της υποβάλλονται από ενδιαφερόμενους για τον τρόπο ελέγχου της ακεραιότητας εγγράφων σε μορφή PDF, τα οποία έχουν υπογραφεί με ηλεκτρονικές υπογραφές ή σφραγιστεί με ηλεκτρονικές σφραγίδες, καθώς και για τον τρόπο επικύρωσης αυτών. Περιλαμβάνονται, επιπλέον, ορισμένες γενικές οδηγίες σχετικά με τις ενέργειες ενός υπογράφοντα κατά την υπογραφή ενός εγγράφου. Τέλος, στο πλαίσιο της γενικότερης ενημέρωσης των καταναλωτών, γίνεται σύντομη αναφορά σε κενά ασφάλειας που έχουν εντοπιστεί κατά καιρούς και δίνουν τη δυνατότητα σε ένα επιτιθέμενο να εμφανίσει ως έγκυρο ένα έγγραφο PDF με περιεχόμενο διαφορετικό από αυτό που υπογράφηκε.

Λόγω της συνεχούς εξέλιξης της σχετικής τεχνολογίας των ηλεκτρονικών υπογραφών αλλά και ενδεχόμενων μελλοντικών αλλαγών στο νομικό πλαίσιο, οι παρεχόμενες πληροφορίες αφορούν στο χρόνο συγγραφής του παρόντος και ενδέχεται στο μέλλον να έχει παύσει η ισχύς τους.

Το παρόν δεν αποτελεί κείμενο κανονιστικού χαρακτήρα. Σε περίπτωση διαφοροποίησης των οριζόμενων στο παρόν με το εκάστοτε ισχύον κανονιστικό πλαίσιο, υπερισχύουν τα οριζόμενα από το εκάστοτε ισχύον κανονιστικό πλαίσιο.

Πώς μπορώ να εξακριβώσω την εγκυρότητα μιας εγκεκριμένης ηλεκτρονικής υπογραφής σε ένα έγγραφο PDF;

Η ηλεκτρονική υπογραφή δημιουργείται με βάση τα δεδομένα αποκλειστικής κατοχής (ιδιωτικό κλειδί) και τα προς υπογραφή δεδομένα και αποτελεί μια ψηφιακή «ετικέτα», η οποία επισυνάπτεται στα προς υπογραφή δεδομένα, στο έγγραφο δηλαδή. Σκοπός της διαδικασίας αυτής είναι (α) η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση του υπογεγραμμένου εγγράφου με το φυσικό πρόσωπο που υπογράφει, (β) η εγγύηση της γνησιότητας των ψηφιακών δεδομένων και (γ) η δέσμευση του υπογράφοντος, δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί ότι υπέγραψε το έγγραφο.

Οι απαιτήσεις της διαδικασίας επικύρωσης εγκεκριμένης ηλεκτρονικής υπογραφής καθορίζονται στο άρθρο 32 παρ. 1 του Κανονισμού ΕΕ 910/2014 (eIDAS), σύμφωνα με το οποίο η εγκυρότητα της υπογραφής επιβεβαιώνεται εφόσον:

α) το πιστοποιητικό που τεκμηριώνει την υπογραφή ήταν κατά τη στιγμή της υπογραφής εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής σύμφωνα με το παράρτημα Ι·
β) το εγκεκριμένο πιστοποιητικό εκδόθηκε από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και ήταν έγκυρο κατά τη στιγμή της υπογραφής·
γ) τα στοιχεία επικύρωσης της υπογραφής αντιστοιχούν στα δεδομένα που παρέχονται στο βασιζόμενο μέρος·
δ) το μοναδικό σύνολο δεδομένων που αντιπροσωπεύουν τον υπογράφοντα στο πιστοποιητικό παρέχεται ορθώς στο βασιζόμενο μέρος·
ε) η χρήση οποιουδήποτε ψευδώνυμου δηλώνεται εμφανώς στο βασιζόμενο μέρος, εάν χρησιμοποιήθηκε ψευδώνυμο κατά τη στιγμή της υπογραφής·
στ) η ηλεκτρονική υπογραφή δημιουργήθηκε από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής·
ζ) η ακεραιότητα των υπογεγραμμένων δεδομένων δεν έχει τεθεί σε κίνδυνο·
η) κατά τη στιγμή της υπογραφής πληρούνταν οι απαιτήσεις που προβλέπονται στο άρθρο 26.

Το δε άρθρο 26 του Κανονισμού αναφέρει τις απαιτήσεις που πρέπει να πληροί μια προηγμένη ηλεκτρονική υπογραφή. Συγκεκριμένα, πρέπει να:

α) συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα·
β) είναι ικανή να ταυτοποιεί τον υπογράφοντα·
γ) δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής υπογραφής τα οποία ο υπογράφων μπορεί, με υψηλό βαθμό εμπιστοσύνης, να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο, και
δ) συνδέεται με τα δεδομένα που έχουν υπογραφεί σε σχέση με αυτήν κατά τρόπο ώστε να μπορεί να ανιχνευθεί οποιαδήποτε επακόλουθη τροποποίηση των εν λόγω δεδομένων.

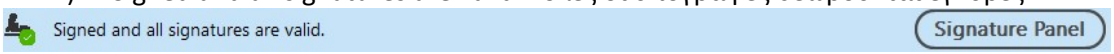
Επιπλέον, ο Κανονισμός ορίζει ότι η εγκεκριμένη ηλεκτρονική υπογραφή είναι μία προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής (ΕΔΔΥ – QSCD) και η οποία βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής (δηλαδή πιστοποιητικό που πληροί τις απαιτήσεις του Παραρτήματος Ι του Κανονισμού).

Βάσει των ανωτέρω, ο λήπτης ενός υπογεγραμμένου εγγράφου που ενδιαφέρεται να διαπιστώσει την εγκυρότητά του, πρακτικά πρέπει να εξακριβώσει (α) την ακεραιότητα του εγγράφου, ότι δηλαδή αυτό που βλέπει είναι πράγματι αυτό που υπογράφηκε και (β) την

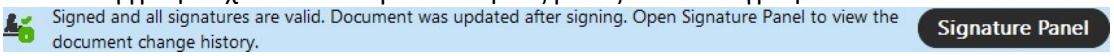
εγκυρότητα των ηλεκτρονικών υπογραφών αυτών που υπογράφουν το έγγραφο και την ταύτιση των εκδόσεων που έχει υπογράψει ο καθένας τους. Για το σκοπό αυτό, ο λήπτης του εγγράφου οφείλει να ακολουθήσει μια διαδικασία.

Το πρώτο βήμα είναι να χρησιμοποιήσει το πρόγραμμα ανάγνωσης εγγράφων PDF που διαθέτει (π.χ. Acrobat Reader). Κάποια από τα προγράμματα αυτού του είδους διενεργούν αυτόματη εξακρίβωση της εγκυρότητας των υπογραφών στο έγγραφο. Το αποτέλεσμα αυτής, όμως, πρέπει να εξετάζεται με προσοχή καθώς, αφενός ο βαθμός βεβαιότητας ότι μια υπογραφή είναι έγκυρη όταν το πρόγραμμα την αναφέρει ως έγκυρη είναι μάλλον μικρός και, αφετέρου, σίγουρα υπάρχει πρόβλημα με τις υπογραφές στο έγγραφο όταν αναφέρεται κάποια παρατήρηση ή ότι κάποια υπογραφή είναι άκυρη. Για παράδειγμα, το αποτέλεσμα της διαδικασίας εξακρίβωσης του Acrobat Reader μπορεί να είναι κάποιο από τα παρακάτω, μεταξύ άλλων:

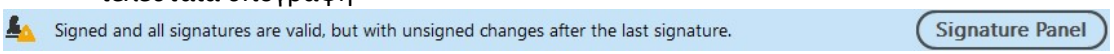
1) “Signed and all signatures are valid”: όλες οι υπογραφές θεωρούνται έγκυρες·



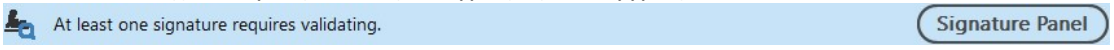
2) “Signed and all signatures are valid. Document was updated after signing. Open signature panel to view the document change history.”: το έγγραφο υπογράφεται από περισσότερους από έναν υπογράφοντες, οι υπογραφές θεωρούνται έγκυρες αλλά το έγγραφο έχει υποστεί τροποποιήσεις μεταξύ των υπογραφών·



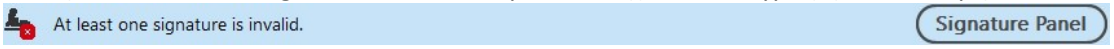
3) “Signed and all signatures are valid, but with unsigned changes after the last signature”: το έγγραφο υπογράφεται από έναν ή περισσότερους υπογράφοντες, οι υπογραφές θεωρούνται έγκυρες αλλά το έγγραφο έχει υποστεί τροποποιήσεις μετά την τελευταία υπογραφή·



4) “At least one signature requires validating”: δεν μπορεί να εξακριβωθεί η εγκυρότητα τουλάχιστον μίας από τις υπογραφές στο έγγραφο και

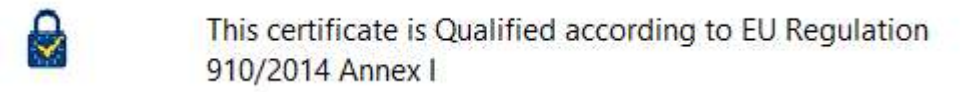


5) “At least one signature is invalid”: μία τουλάχιστον υπογραφή είναι άκυρη.

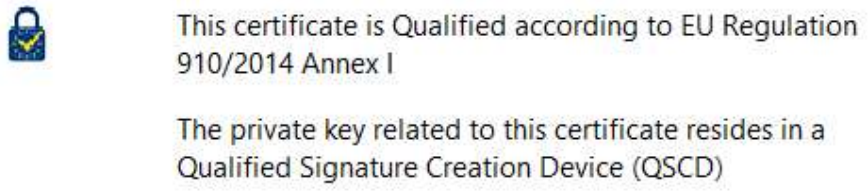


Στις περιπτώσεις 2 έως και 5 υπάρχει πρόβλημα είτε με το τελικό έγγραφο που προβάλλεται σε σχέση με το υπογεγραμμένο είτε με κάποια από τις υπογραφές που περιέχονται σ’ αυτό. Στην 1η περίπτωση το πρόγραμμα δεν αναφέρει κάποιο πρόβλημα αλλά χρειάζεται περαιτέρω έλεγχος προκειμένου να διαπιστωθεί αν η υπογραφή είναι έγκυρη. Οι διαθέσιμες επιλογές περιγράφονται στη συνέχεια.

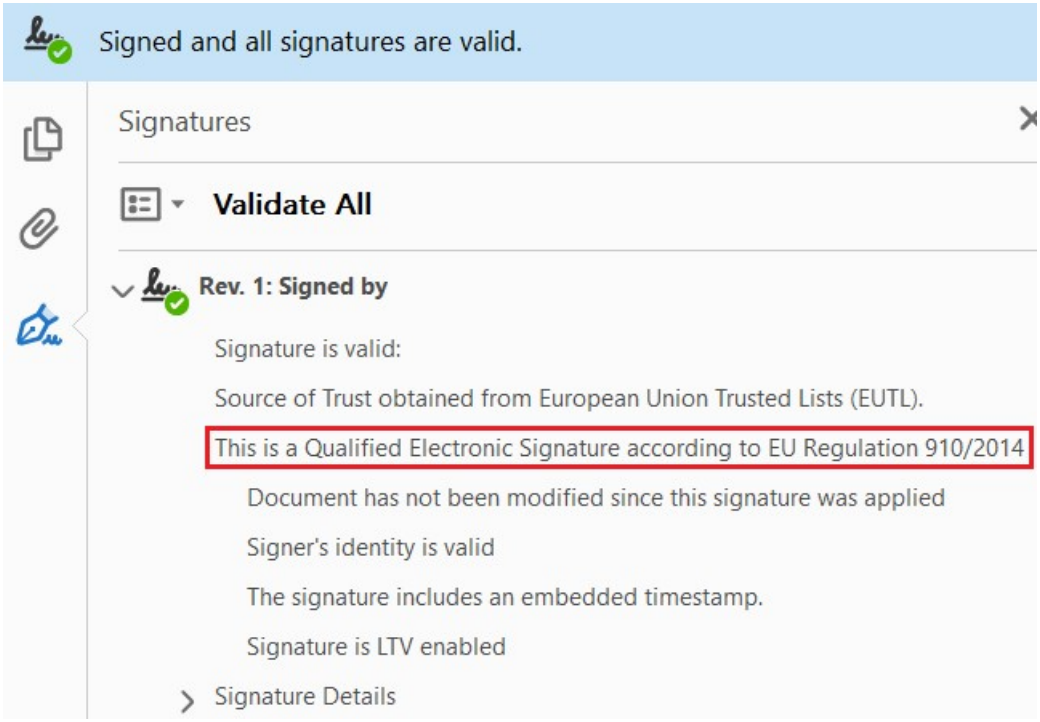
Αξίζει να αναφερθεί ότι το Acrobat Reader στις πληροφορίες του πιστοποιητικού (Signature panel → Υπογράφων → Signature details → Certificate details) μπορεί να αναφέρει ότι το πιστοποιητικό είναι εγκεκριμένο, όπως φαίνεται στην εικόνα που ακολουθεί. Επισημαίνεται ότι η πληροφορία αυτή αναφέρεται στο πιστοποιητικό και όχι στην υπογραφή! Κατά συνέπεια, η υπογραφή του συγκεκριμένου υπογράφοντος είναι προηγμένη υπογραφή βασιζόμενη σε εγκεκριμένο πιστοποιητικό (Advanced Electronic Signature based on a Qualified Certificate, AdESig-QC). Στην περίπτωση αυτή, η υπογραφή δεν χαίρει αυτόματης αναγνώρισης ως ισοδύναμης της ιδιόχειρης βάσει νόμου.



Όταν όμως εμφανίζεται η εικόνα που ακολουθεί, το επίπεδο της συγκεκριμένης υπογραφής είναι «εγκεκριμένη» (Qualified Electronic Signature, QESig):



Επιπλέον, στην περίπτωση αυτή, στο Signature panel → Υπογράφων θα περιλαμβάνεται το μήνυμα που έχει επισημανθεί στην εικόνα που ακολουθεί.



Σημειώνεται ότι τα παραπάνω αφορούν στο επίπεδο της υπογραφής και όχι στην εγκυρότητά της, η οποία πρέπει πάντα να ελέγχεται.

Σε κάθε περίπτωση και προτού γίνει χρήση κάποιας εκ των επιλογών για την εξακρίβωση της εγκυρότητας των υπογραφών σε ένα έγγραφο PDF (αρχείο Α), η ΕΕΤΤ συστήνει να εκτελούνται πάντα οι ακόλουθες ενέργειες (βλ. Παράρτημα Α για περισσότερες πληροφορίες):

1) Εάν το έγγραφο υπογράφεται μόνο από έναν υπογράφοντα, εξαγωγή και αποθήκευση της υπογεγραμμένης έκδοσης (αρχείο Β)[1].
2) Εάν το έγγραφο υπογράφεται από περισσότερους από έναν υπογράφοντες, εξαγωγή της υπογεγραμμένης έκδοσης του πρώτου (αρχείο Γ) και του τελευταίου υπογράφοντα (αρχείο Β) .
3) Έλεγχος αν υπάρχουν αλλαγές μεταξύ του αρχείου Α και του αρχείου Β και, εφόσον το έγγραφο υπογράφεται από περισσότερους από έναν υπογράφοντες, μεταξύ του αρχείου Β και του αρχείου Γ. Ο δεύτερος έλεγχος αποσκοπεί στην εξακρίβωση της ταύτισης της έκδοσης του εγγράφου που έχει υπογράψει ο πρώτος υπογράφων και

[1] Στο Acrobat Reader αυτό γίνεται ως εξής: επιλέγετε “Signature panel” (στο πάνω μέρος της προβολής του εγγράφου), στο παράθυρο που ανοίγει στα αριστερά επιλέγετε τον υπογράφοντα και στη συνέχεια από το drop-down menu δίπλα από το κουμπί “Validate all”, που βρίσκεται ακριβώς πάνω από τη λίστα με τους υπογράφοντες, επιλέγετε “View signed version”. Θα ανοίξει ένα νέο έγγραφο το οποίο θα είναι η έκδοση του εγγράφου που έχει υπογράψει ο συγκεκριμένος υπογράφων.

αυτής που έχει υπογράψει ο τελευταίος. Αν οι εκδόσεις του εγγράφου δεν έχουν διαφορές, τότε δεν έχουν διαφορές και οι ενδιάμεσες εκδόσεις των υπόλοιπων υπογραφόντων. Ο πρώτος έλεγχος αποσκοπεί στην εξακρίβωση της ταύτισης του κειμένου που προβάλλεται και εκτυπώνεται με αυτό που έχει πραγματικά υπογραφεί. Για τον έλεγχο αυτό μπορούν να χρησιμοποιηθούν εμπορικές αλλά και εφαρμογές ανοιχτού κώδικα (π.χ. DiffPDF, http://www.qtrac.plus.com/diffpdf-foss.html, η οποία όμως έχει σταματήσει να υποστηρίζεται καθώς πλέον διατίθεται εμπορικά), ο δε έλεγχος πρέπει να περιλαμβάνει όλα τα στοιχεία του εγγράφου (π.χ. “appearance”, “words”, “characters” στην περίπτωση του DiffPDF). Σημειώνεται ότι η ΕΕΤΤ δεν προτείνει τη χρήση κάποιου συγκεκριμένου προγράμματος για το σκοπό αυτό.

4) Μόνο εφόσον δεν διαπιστώνονται αλλαγές μεταξύ των εκδόσεων, συστήνεται να προχωρά η διαδικασία εξακρίβωσης της εγκυρότητας των υπογραφών. Σε αντίθετη περίπτωση, η φύση των αλλαγών πρέπει να διερευνάται και, ενδεχομένως, ανά περίπτωση, να ζητείται να υπογράφεται ξανά το έγγραφο με στόχο να εξασφαλιστεί ότι στο τελικό κείμενο δεν υπάρχουν αλλαγές μεταξύ των διαφόρων εκδόσεων.

Α. Χρήση εγκεκριμένης υπηρεσίας επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών

Η εγκεκριμένη υπηρεσία επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών παρέχεται μόνο από εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης και επιτρέπει στα βασιζόμενα μέρη να λαμβάνουν το αποτέλεσμα της διαδικασίας επικύρωσης με αυτοματοποιημένο τρόπο, ο οποίος είναι αξιόπιστος, αποτελεσματικός και φέρει την προηγμένη ηλεκτρονική υπογραφή ή την προηγμένη ηλεκτρονική σφραγίδα του παρόχου της εγκεκριμένης υπηρεσίας επικύρωσης.

Συνεπώς, ο πάροχος της υπηρεσίας αναλαμβάνει να εξακριβώσει την εγκυρότητα των υπογραφών σε ένα έγγραφο και να διαπιστώσει αν είναι εγκεκριμένες ή όχι, σύμφωνα με τα οριζόμενα στο άρθρο 32 του Κανονισμού, και, στη συνέχεια, να διαβιβάσει με αυτοματοποιημένο τρόπο το αποτέλεσμα στον αιτούντα, υπογεγραμμένο είτε με την προηγμένη (ή εγκεκριμένη) ηλεκτρονική υπογραφή του είτε με την προηγμένη (ή εγκεκριμένη) ηλεκτρονική σφραγίδα του. Με τον τρόπο αυτό, ο ενδιαφερόμενος αποκτά το πιστοποιημένο αποτέλεσμα της διαδικασίας εξακρίβωσης, το οποίο εγγυάται ο πάροχος της υπηρεσίας, αναλαμβάνοντας την ευθύνη που προβλέπεται στους όρους χρήσης της.

Το πλεονέκτημα της υπηρεσίας αυτής είναι ότι είναι απλή και καταλήγει στην παραλαβή ενός επίσημου πιστοποιητικού σχετικά με την εγκυρότητα ή μη των υπογραφών στο έγγραφο, το οποίο έχει νομική ισχύ. Συστήνεται στο χρήστη να ενημερώνεται για τους όρους χρήσης της υπηρεσίας προσεκτικά και να αξιολογεί τους ενδεχόμενους κινδύνους από τη χρήση της (π.χ. η μεταφόρτωση του εγγράφου σε διακομιστή του παρόχου προκειμένου να ελεγχθεί μπορεί να μην είναι αποδεκτή από τον χρήστη).

Στην Ελλάδα, η υπηρεσία αυτή δεν παρέχεται από κάποιον πάροχο. Κατά συνέπεια, ο ενδιαφερόμενος πρέπει να χρησιμοποιήσει υπηρεσία που παρέχεται σε άλλο Κράτος Μέλος.

Β. Χρήση διαθέσιμων online υπηρεσιών εξακρίβωσης

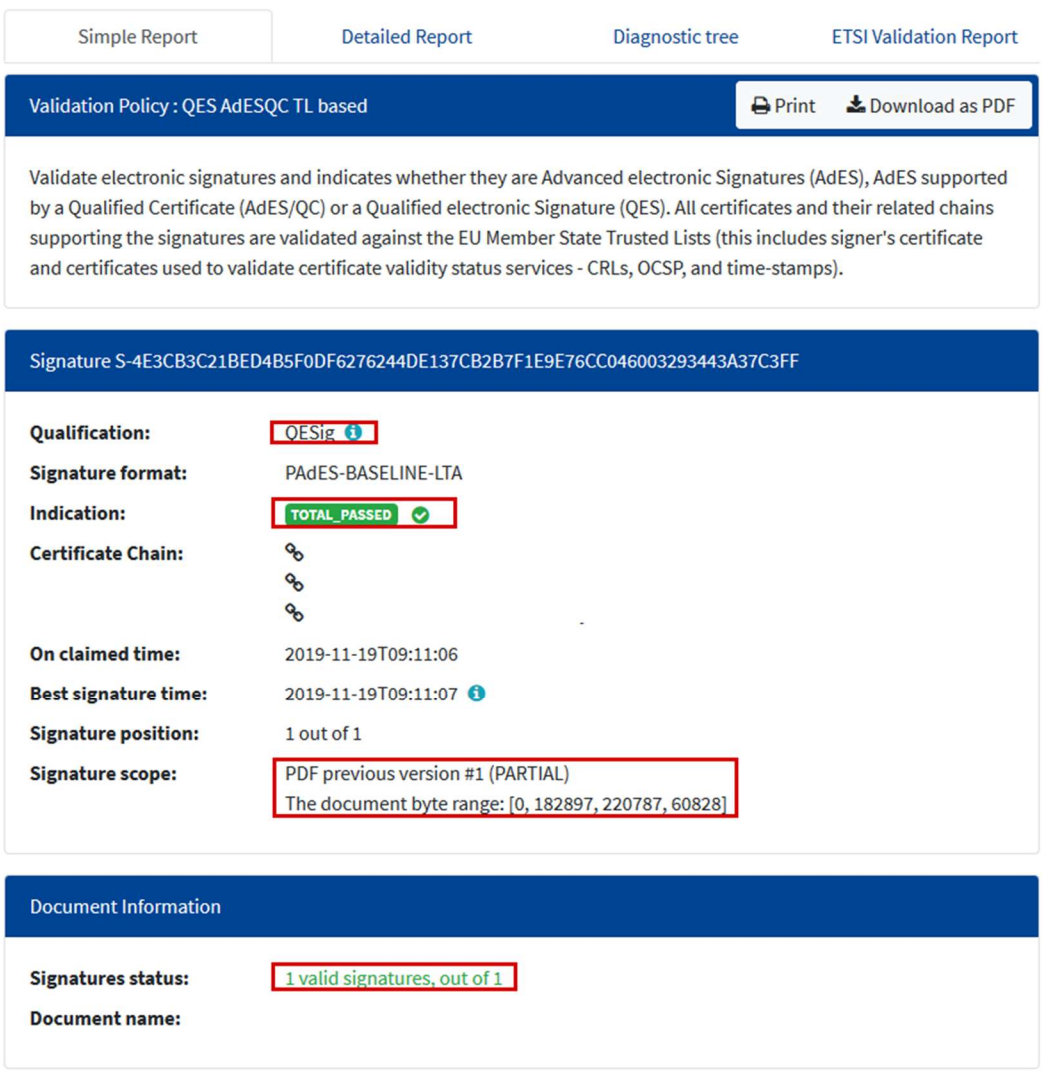
Εάν ο λήπτης του εγγράφου ενδιαφέρεται απλώς να εξακριβώσει την εγκυρότητα των υπογραφών στο έγγραφο και δεν επιθυμεί να λάβει ένα επίσημο πιστοποιητικό της εγκυρότητας ή μη αυτών, μπορεί να χρησιμοποιήσει τις υπηρεσίες που παρέχονται στη σελίδα “DSS Demonstration WebApp” της Ευρωπαϊκής Επιτροπής (https://ec.europa.eu/cefdigital/DSS/

webapp-demo/validation). Στη σελίδα αυτή παρέχονται διάφορες δυνατότητες, μεταξύ των οποίων και η εξακρίβωση της εγκυρότητας των υπογραφών σε ένα έγγραφο ("Validate a signature"). Η υλοποίηση των υπηρεσιών αυτών βασίζεται στο Digital Signature Services (DSS) Framework, μια βιβλιοθήκη ανοιχτού κώδικα για δημιουργία και επικύρωση ηλεκτρονικών υπογραφών, που αναπτύσσεται από ιδιωτική εταιρεία για λογαριασμό της Ευρωπαϊκής Επιτροπής υπό την επίβλεψη του CEF Digital.

Η υπηρεσία εξακρίβωσης που παρέχεται στη σελίδα αυτή, δεν είναι εγκεκριμένη υπηρεσία επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών και, κατά συνέπεια, το αποτέλεσμά της δεν έχει νομική ισχύ. Παρόλα αυτά, βασίζεται σε λογισμικό που αναπτύσσεται για λογαριασμό της Ευρωπαϊκή Επιτροπής, το οποίο συντηρείται τακτικά και ακολουθεί για τον έλεγχο της εγκυρότητας τα πρότυπα του ETSI και την «πολιτική» που έχει οριστεί στη συγκεκριμένη υλοποίηση, ένα σύνολο κανόνων δηλαδή που ορίζουν τον τρόπο που αντιμετωπίζονται διάφορα στάδια στη διαδικασία και την επίδραση που έχουν στο τελικό αποτέλεσμα. Για το λόγο αυτό, κρίνεται ότι επαρκεί για την περίπτωση που δεν απαιτείται η εγκυρότητα των υπογραφών να βεβαιώνεται με κάποιο πιστοποιητικό που παρέχεται από εγκεκριμένη υπηρεσία επικύρωσης εγκεκριμένων ηλεκτρονικών υπογραφών.

Η χρήση της υπηρεσίας είναι απλή. Ο χρήστης ανεβάζει το υπογεγραμμένο έγγραφο ("Signed file") και επιλέγει "Submit" ώστε να ελεγχθεί. Σημειώνεται ότι το έγγραφο θα μεταφορτωθεί στο διακομιστή της ΕΕ. Εναπόκειται στο χρήστη να αποφασίσει αν αυτό είναι αποδεκτό, ανάλογα με το επίπεδο ασφάλειας του εγγράφου. Εφόσον το έγγραφο δεν περιέχει εμπιστευτική ή απόρρητη πληροφορία, ή ο λήπτης του εγγράφου αποδέχεται τον όποιο κίνδυνο προκύπτει από τη μεταφόρτωση του εγγράφου στο διακομιστή, μπορεί να προχωρήσει στη χρήση της υπηρεσίας.

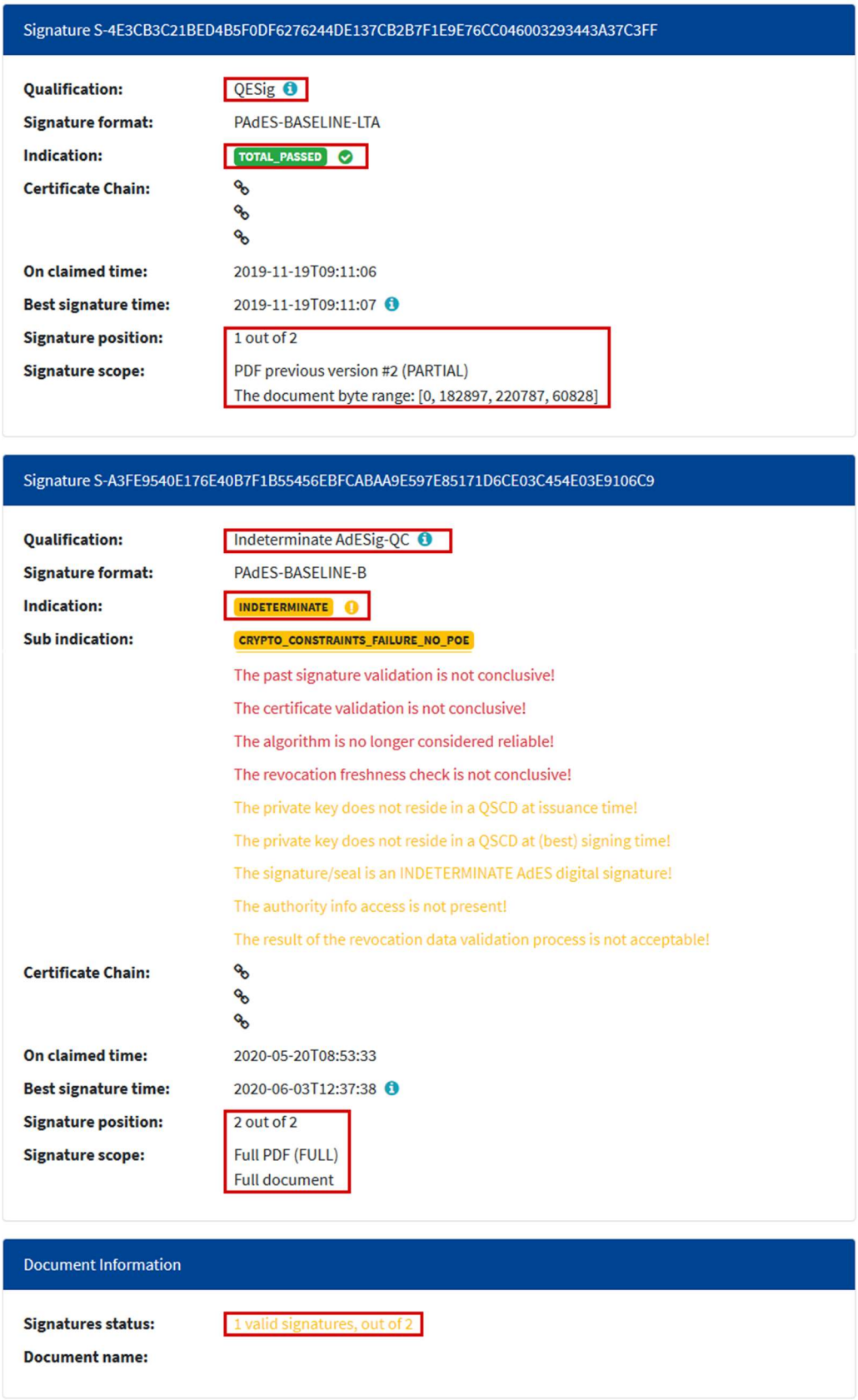
Το αποτέλεσμα του ελέγχου μπορεί να είναι όπως στην εικόνα που ακολουθεί. Έχουν σημειωθεί με κόκκινο πλαίσιο τα σημεία που χρήζουν προσοχής ενώ έχει αφαιρεθεί η πληροφορία για τον υπογράφοντα και το όνομα του εγγράφου που χρησιμοποιήθηκε στο παράδειγμα.



Παρατηρούμε ότι το έγγραφο έχει υπογραφεί από 1 υπογράφοντα ("1 valid signatures, **out of 1**"), με εγκεκριμένη ηλεκτρονική υπογραφή ("QESig", Qualified Electronic Signature) και το αποτέλεσμα του ελέγχου είναι "TOTAL_PASSED", που σημαίνει ότι δεν διαπιστώθηκε κάποιο πρόβλημα κατά τον έλεγχό της. Στο αποτέλεσμα αναφέρεται και το «εύρος κάλυψης» της υπογραφής. Στο συγκεκριμένο έγγραφο η «κάλυψη» είναι μερική ("PARTIAL"). Η παρατήρηση αυτή μπορεί να έχει μικρή σημασία (για παράδειγμα, ακολουθεί timestamp το οποίο δεν «καλύπτεται» από την υπογραφή) ή πολύ μεγάλη (να υπάρχουν μεταγενέστερα στοιχεία στο έγγραφο που να το αλλάζουν). Ο χρήστης πρέπει πάντα να ακολουθεί τη διαδικασία που έχει περιγραφεί προηγουμένως προκειμένου να διαπιστώνει αν υπάρχουν διαφορές μεταξύ της έκδοσης που έχει υπογράψει ο υπογράφων και της τελικής έκδοσης. Αν δεν υπάρχουν διαφορές τότε η παρατήρηση μπορεί να αγνοηθεί. Αν υπάρχουν τότε (α) η υπογραφή «καλύπτει», προφανώς, την υπογεγραμμένη έκδοση του εγγράφου και όχι την τελική (με τις διαφορές) και (β) συστήνεται στο χρήστη να εξακριβώσει την αιτία ύπαρξης των διαφορών αυτών.

Το αποτέλεσμα της διαδικασίας στην περίπτωση ενός εγγράφου που υπογράφεται από 2 υπογράφοντες, έναν με έγκυρη εγκεκριμένη ηλεκτρονική υπογραφή και έναν με προηγμένη

ηλεκτρονική υπογραφή που βασίζεται σε εγκεκριμένο πιστοποιητικό (AdESig-QC) φαίνεται στην εικόνα που ακολουθεί.



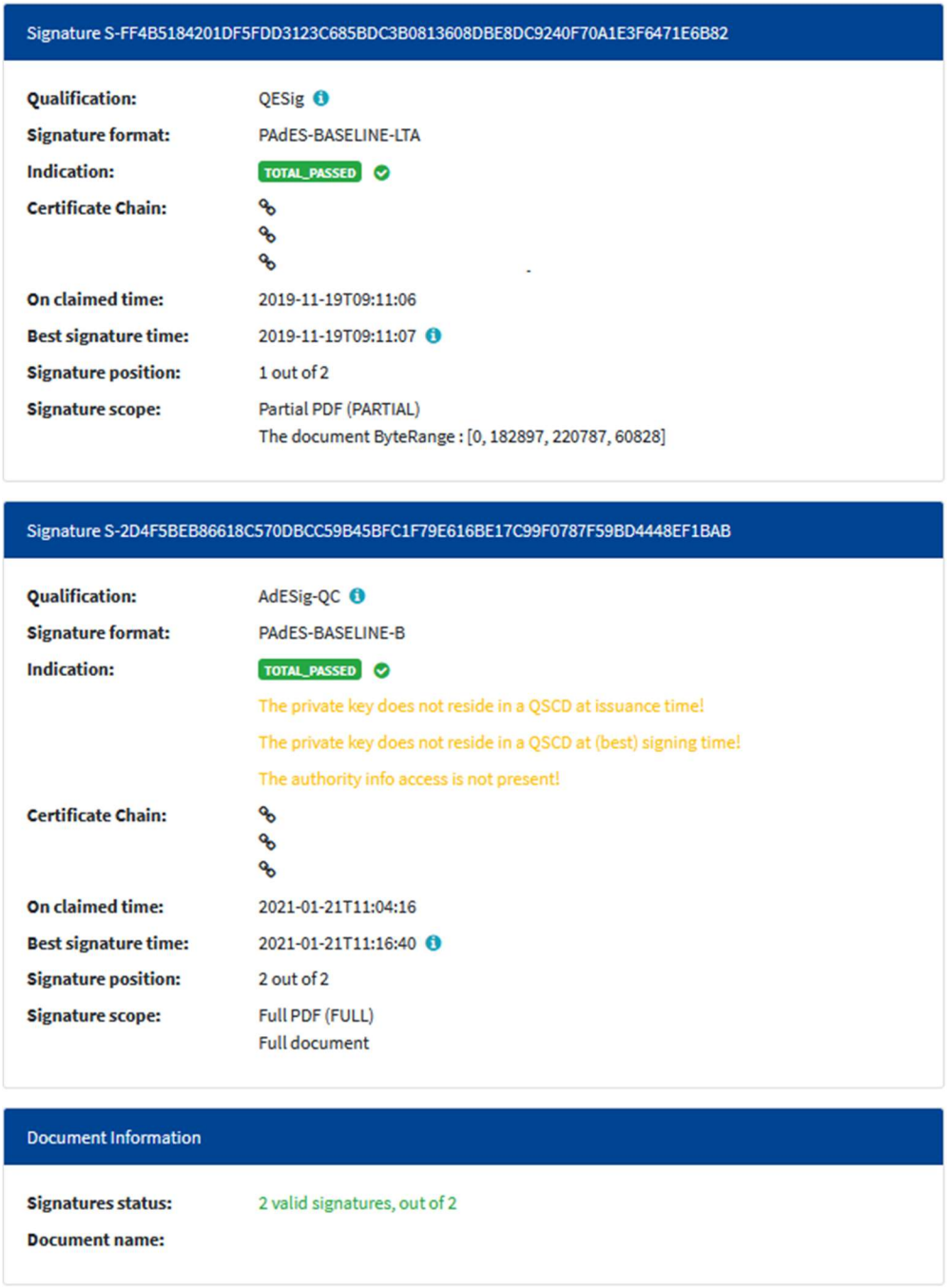
Για τον πρώτο υπογράφοντα (θέση υπογραφής “1 out of 2”) ισχύουν όσα αναφέρθηκαν προηγουμένως. Παρατηρούμε ότι η υπογραφή του δεύτερου υπογράφοντα είναι “AdESig-QC” και όχι “QESig”, δηλαδή προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε εγκεκριμένο πιστοποιητικό άρα δεν χαίρει απευθείας αναγνώρισης της ισοδυναμίας της με ιδιόχειρη υπογραφή. Επιπλέον, το αποτέλεσμα της επαλήθευσής της δεν είναι “TOTAL_PASSED” αλλά “INDETERMINATE”, που καταδεικνύει ότι υπάρχει κάποιο πρόβλημα. Πράγματι, η λίστα με τα προβλήματα αναφέρεται ακριβώς από κάτω. Τέλος, παρατηρούμε ότι η συγκεκριμένη υπογραφή καλύπτει όλο το έγγραφο.

Στην περίπτωση λοιπόν αυτή, το έγγραφο δεν θεωρείται υπογεγραμμένο από το δεύτερο υπογράφοντα με υπογραφή ισοδύναμη της ιδιόχειρης υπογραφής βάσει νόμου. Επιπλέον, η υπογραφή του υπογράφοντα έχει τεχνικές αδυναμίες / προβλήματα που, ενδεχομένως, την καθιστούν μη αξιόπιστη.

Επισημαίνεται ότι, ειδικά για τις υπογραφές της παλιάς υποδομής της ΑΠΕΔ, το αναμενόμενο αποτέλεσμα της διαδικασίας επικύρωσης της συγκεκριμένης υπηρεσίας είναι “INDETERMINATE” με αιτία CRYPTO_CONSTRAINTS_FAILURE_NO_POE. Αυτό οφείλεται στο ότι η «πολιτική» ελέγχου της, στην οποία αναφερθήκαμε προηγουμένως, χαρακτηρίζει τον αλγόριθμο SHA-1, που χρησιμοποιείται από την «παλιά» ΑΠΕΔ, ως μη ασφαλή. Αν και νέες Αρχές Πιστοποίησης εγκεκριμένων παρόχων που εκδίδουν εγκεκριμένα πιστοποιητικά με χρήση του αλγορίθμου SHA-1, δεν γίνονται πλέον δεκτές από την ΕΕΤΤ, οι συγκεκριμένες Αρχές Πιστοποίησης της ΑΠΕΔ δεν έχουν αποσυρθεί και, κατά συνέπεια, η χρήση αυτού του αλγορίθμου δεν μπορεί να καθιστά την υπογραφή άκυρη. Για να παρακάμψετε αυτό το πρόβλημα μπορεί να χρησιμοποιηθεί μια τροποποιημένη πολιτική ελέγχου που δημιουργείται με την ακόλουθη διαδικασία. Στη σελίδα

https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html#_the_default_xml_policy

δίνεται το περιεχόμενο του αρχείου “constraint.xml” το οποίο μπορεί να αποθηκευτεί σε ένα νέο αρχείο με όνομα π.χ. policy.xml και στη συνέχεια να αλλαχθεί η ημερομηνία λήξης του αλγορίθμου SHA-1 (AlgoExpirationDate) από 2009 σε π.χ. 2029 σε αυτό. Στη συνέχεια, στη σελίδα της εφαρμογής, μέσω της επιλογής More options → Custom validation constraints file εισάγεται το αρχείο policy.xml. Το αποτέλεσμα της επικύρωσης του προηγούμενου εγγράφου μετά την εφαρμογή της νέας πολιτικής απεικονίζεται στο σχήμα που ακολουθεί.



Signature S-FF4B5184201DF5FDD3123C685BDC3B0813608DBE8DC9240F70A1E3F6471E6B82

Qualification:	QESig
Signature format:	PAdES-BASELINE-LTA
Indication:	TOTAL_PASSED
Certificate Chain:	
On claimed time:	2019-11-19T09:11:06
Best signature time:	2019-11-19T09:11:07
Signature position:	1 out of 2
Signature scope:	Partial PDF (PARTIAL) The document ByteRange : [0, 182897, 220787, 60828]

Signature S-2D4F5BEB86618C570DBCC59B45BFC1F79E616BE17C99F0787F59BD4448EF1BAB

Qualification:	AdESig-QC
Signature format:	PAdES-BASELINE-B
Indication:	TOTAL_PASSED The private key does not reside in a QSCD at issuance time! The private key does not reside in a QSCD at (best) signing time! The authority info access is not present!
Certificate Chain:	
On claimed time:	2021-01-21T11:04:16
Best signature time:	2021-01-21T11:16:40
Signature position:	2 out of 2
Signature scope:	Full PDF (FULL) Full document

Document Information

Signatures status:	2 valid signatures, out of 2
Document name:	

Όπως αναμενόταν, το αποτέλεσμα του ελέγχου της 2ης υπογραφής άλλαξε σε “TOTAL_PASSED". Προφανώς, αν το αποτέλεσμα εξακολουθεί να είναι “INDETERMINATE” μετά την εφαρμογή της τροποποιημένης πολιτικής τότε υπάρχουν άλλα προβλήματα που καθιστούν την υπογραφή (με μεγάλο βαθμό βεβαιότητας) άκυρη.

Προσοχή! Αυτή είναι η μόνη αλλαγή που επιτρέπεται να γίνει στην πολιτική. Επιπλέον, μόλις αποσυρθούν οι συγκεκριμένες Αρχές Πιστοποίησης της ΑΠΕΔ από την ΕΕΤΤ ή λήξει και το τελευταίο εκδοθέν πιστοποιητικό από αυτές ή κατόπιν Απόφασης της ΕΕΤΤ σχετικά με τη χρήση του αλγορίθμου SHA-1, η συγκεκριμένη διαδικασία τροποποίησης της πολιτικής δεν πρέπει να εφαρμόζεται!

Αντίστοιχη υπηρεσία παρέχεται από την Αυστριακή ρυθμιστική αρχή RTR στη σελίδα: https://www.rtr.at/TKP/was_wir_tun/vertrauensdienste/Signatur/signaturpruefung/Pruefu

ng.en.html. Η υπηρεσία αυτή δεν προσφέρει τη δυνατότητα ορισμού πολιτικής ελέγχου, όμως δεν θεωρεί άκυρο τον αλγόριθμο SHA-1. Το επίπεδο της υπογραφής (QES ή AdES-QC ή όχι) αναφέρεται στο verification report, στη γραμμή "Quality" (π.χ. "qualified certificate (Source: TSL), secure signature-creation device (Source: certificate)", που μεταφράζεται σε QES ενώ αν έλειπε το "secure signature-creation device" θα επρόκειτο για AdES-QC).

Τι πλεονεκτήματα προσφέρει η χρήση χρονοσφραγίδας (timestamp) κατά την υπογραφή ενός εγγράφου;

Για να γίνουν κατανοητά τα πλεονεκτήματα που προκύπτουν από τη χρήση χρονοσφραγίδας, χρειάζεται να αναφερθούν τα διάφορα επίπεδα υπογραφής. Στο πρότυπο ETSI EN 319 142-1, που αφορά στις υπογραφές σε έγγραφα PDF, ορίζονται τα εξής επίπεδα:

- B-B: βασικό επίπεδο υπογραφής·
- B-T: δημιουργία και συμπερίληψη χρονοσφραγίδας σε μία υπογραφή·
- B-LT: συμπερίληψη όλου του υλικού που απαιτείται για την επικύρωση μιας δεδομένης υπογραφής στο έγγραφο·
- B-LTA: συμπερίληψη χρονοσφραγίδων, όταν και όποτε απαιτείται, που επιτρέπουν την επικύρωση της υπογραφής για μεγάλο διάστημα μετά τη δημιουργία της.

Ο τρόπος που γίνεται η επικύρωση μιας υπογραφής εξαρτάται από το επίπεδό της. Αν επικεντρωθούμε στα δύο πρώτα επίπεδα, η επικύρωση μιας B-B υπογραφής γίνεται, σύμφωνα με τα πρότυπα του ETSI, στον τρέχοντα χρόνο στον οποίο ζητείται η επικύρωση. Ο λόγος είναι ότι δεν υπάρχει στο έγγραφο PDF αξιόπιστη πληροφορία που να βεβαιώνει ότι η υπογραφή υπήρχε μια δεδομένη στιγμή στο παρελθόν. Αντίθετα, στην περίπτωση μιας B-T υπογραφής, η πληροφορία αυτή παρέχεται από την (εγκεκριμένη) χρονοσφραγίδα, με αποτέλεσμα η επικύρωση να γίνεται στο χρόνο που ορίζεται στη χρονοσφραγίδα.

Συνέπεια αυτής της πρακτικής είναι ότι αν χρησιμοποιηθεί B-B υπογραφή, δηλαδή βασικού επιπέδου χωρίς χρονοσφραγίδα, στην περίπτωση που η επικύρωση διενεργηθεί εντός του χρόνου ισχύος του πιστοποιητικού, το αποτέλεσμά της θα είναι ότι η υπογραφή είναι έγκυρη. Σε περίπτωση, όμως, που η επικύρωση γίνει μετά τη λήξη του χρόνου ισχύος του πιστοποιητικού, η υπογραφή θα φαίνεται ως άκυρη, με αποτέλεσμα να δημιουργούνται προβλήματα για τον υπογράφοντα που ενδεχομένως θα χρειαστεί να ανατρέψει το αποτέλεσμα της επικύρωσης, αποδεικνύοντας την εγκυρότητα της υπογραφής του και την ισχύ του πιστοποιητικού κατά το χρόνο υπογραφής του ηλεκτρονικού εγγράφου.

Σημειώνεται ότι αν και τα πρότυπα του ETSI δεν είναι υποχρεωτικά σύμφωνα με τον Κανονισμό eIDAS, οι περισσότερες υπηρεσίες επικύρωσης τα ακολουθούν. Επιπλέον, αν και έχει διαπιστωθεί το κενό στη διαδικασία αναφορικά με την πιστοποίηση της ύπαρξης του εγγράφου στη δεδομένη μορφή από άλλη εξωτερική πηγή χρόνου (π.χ. ηλεκτρονικό πρωτόκολλο), τα εν λόγω πρότυπα δεν έχουν τροποποιηθεί ακόμα. Τέλος, αν και η επικύρωση ενός εγγράφου με B-B υπογραφή σε χρόνο άλλο από τον τρέχοντα χρόνο είναι δυνατή με χρήση της βιβλιοθήκης DSS, απαιτούνται γνώσεις προγραμματισμού για την υλοποίησή της καθώς δεν είναι διαθέσιμη ως επιλογή στις δημόσια προσβάσιμες υπηρεσίες επικύρωσης.

Τι πρέπει να κάνω προτού υπογράψω ένα PDF έγγραφο που έχουν υπογράψει προηγουμένως άλλοι;

Εφόσον είστε ο λήπτης ενός εγγράφου PDF που έχει υπογραφεί από άλλους και το οποίο καλείστε να υπογράψετε, πρέπει να εκτελέσετε τη διαδικασία που περιγράφηκε προηγουμένως. Εφόσον δεν διαπιστώσετε κάποιο πρόβλημα, μπορείτε να προχωρήσετε με την υπογραφή του εγγράφου.

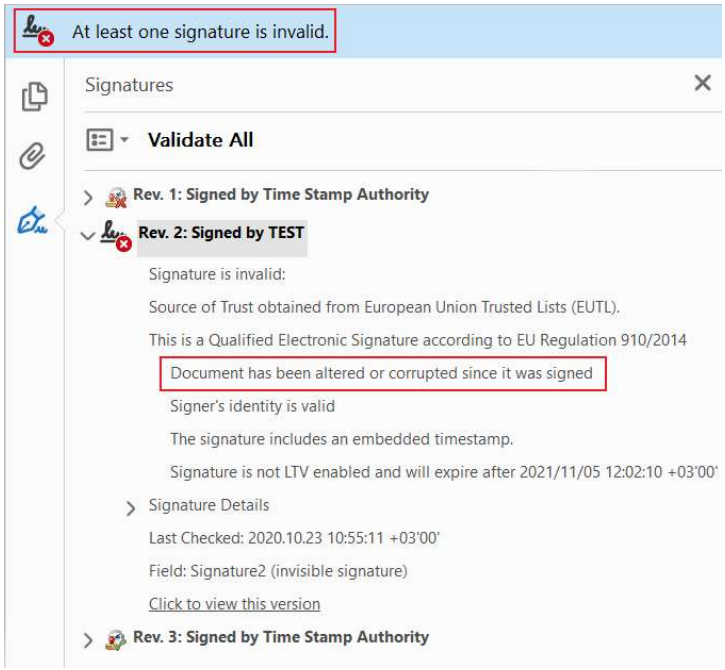
Συστήνεται, για λόγους ασφαλείας, ο συντάκτης ενός εγγράφου να το υπογράφει πρώτος, αφού το μετατρέψει σε μορφή PDF, προτού το διανείμει στους υπόλοιπους υπογράφοντες. Μια καλή πρακτική είναι να χρησιμοποιείται η μορφή PDF/A ώστε να αποκλείεται τυχόν κρυφό ή δυναμικό περιεχόμενο[2].

Τέλος, για να αποφύγετε μελλοντικά προβλήματα σχετικά με τη χρήση του αλγορίθμου SHA-1, πρέπει πάντα να επιλέγετε κατάλληλο αλγόριθμο (π.χ. SHA-256, SHA-512, κ.λπ.) στο πρόγραμμα υπογραφής που χρησιμοποιείτε. Η ισχύς των αλγορίθμων κρυπτογράφησης ορίζεται στην τρέχουσα έκδοση του προτύπου ETSI TS 119 312. Συστήνεται η επιλογή κατάλληλου επιπέδου υπογραφής, ανάλογα με τη χρήση του εγγράφου.

[2] Πληροφορία για τον τρόπο δημιουργίας ενός PDF/A εγγράφου υπάρχει στο Web, π.χ. https://library.princeton.edu/special-collections/sites/default/files/Creating_PDFA.pdf

Παράρτημα: Shadow attacks σε έγγραφα PDF

Ο λόγος που προτείνεται η διαδικασία αυτή είναι ότι κατά καιρούς ερευνητές έχουν διαπιστώσει κενά ασφαλείας στη διαδικασία επικύρωσης που διενεργούν τα προγράμματα ανάγνωσης εγγράφων PDF. Συγκεκριμένα, το 2010 ο Florian Zumbiehl ενημέρωσε[3] σχετικά με ένα κενό ασφαλείας που επέτρεπε να αλλαχθεί η εμφάνιση ενός εγγράφου PDF (δηλαδή και το κείμενο που εμφανίζεται) αφότου αυτό είχε υπογραφεί, χωρίς κατ' ανάγκη να εμφανίζει το πρόγραμμα ανάγνωσης κάποιο πρόβλημα κατά την επικύρωση της υπογραφής. Το 2019, ερευνητές του Ruhr-Universität Bochum και της εταιρείας Hackmanit GmbH στη Γερμανία έδειξαν[4] ότι ήταν δυνατόν να τροποποιηθούν υπογεγραμμένα έγγραφα PDF χωρίς πολλά από τα προγράμματα ανάγνωσης εγγράφων PDF να αντιλαμβάνονται την τροποποίηση με αποτέλεσμα να εξακολουθούν να εμφανίζουν ότι δεν υπάρχει κάποιο πρόβλημα με την υπογραφή. Τέλος, πρόσφατα, τον Ιούνιο του 2020, ερευνητές του Ruhr-Universität Bochum ανακοίνωσαν[5] ότι ανακάλυψαν ένα νέο τρόπο παραβίασης υπογεγραμμένων εγγράφων PDF που ονόμασαν "shadow attacks". Στο σενάριο που εξέτασαν, ο επιτιθέμενος θεωρείται ότι έχει πρόσβαση στο έγγραφο PDF προτού υπογραφεί οπότε μπορεί να το τροποποιήσει κατάλληλα ώστε να περιλαμβάνει δύο διαφορετικά περιεχόμενα: το περιεχόμενο που περιμένει ο υπογράφων και το περιεχόμενο που θα εμφανίζεται αφού ο επιτιθέμενος τροποποιήσει το έγγραφο μετά την υπογραφή του. Τονίζεται ότι, σε κάθε περίπτωση, οι εταιρείες που αναπτύσσουν τα προγράμματα ανάγνωσης εγγράφων PDF ενημερώνονται πριν τη δημοσίευση των αποτελεσμάτων των ερευνητών και προχωρούν στις απαραίτητες διορθώσεις στον κώδικά τους. Για το λόγο αυτό, συστήνεται να ενημερώνονται πάντα τα προγράμματα αυτά στην τελευταία τους έκδοση. Για παράδειγμα, μετά την ενημέρωση αυτή, το αποτέλεσμα που βγάζει το Adobe Acrobat μετά την επικύρωση της υπογραφής ενός εγγράφου που έχει δεχθεί την «επίθεση» που ανακοινώθηκε τον Ιούλιο του 2020 φαίνεται στην εικόνα που ακολουθεί:



[3] Collisions in PDF Signatures (http://pdfsig-collision.florz.de/)
[4] Mladenov, V., Mainka, C., Meyer zu Selhausen, K., Grothe, M., & Schwenk, J. (November 2019). *1 trillion dollar refund – how to spoof pdf signatures*. (ACM Conference on Computer and Communications Security, διαθέσιμο στο https://www.nds.ruhr-uni-bochum.de/media/ei/veroeffentlichungen/2019/06/28/PDF_Signature.pdf)
[5] Mainka, C., Mladenoc, V., Rohlmann, S., & Schwenk, J. (2020). *Attacks bypassing the signature validation in PDF*. (https://www.pdf-insecurity.org/)

Είναι φανερό ότι το πρόγραμμα αναγνωρίζει πλέον την τροποποίηση και για το λόγο αυτό εμφανίζει ότι υπάρχει πρόβλημα στην υπογραφή. Αυτό δεν συνέβαινε με την έκδοση του προγράμματος που ήταν διαθέσιμη όταν οι ερευνητές έκαναν τη σχετική έρευνα.

Η προτεινόμενη από την ΕΕΤΤ διαδικασία παρέχει μεγαλύτερη ασφάλεια και αναμένεται να καλύπτει επαρκώς και την περίπτωση άλλων κενών που, ενδεχομένως, υπάρχουν στους αλγόριθμους επικύρωσης υπογραφών των προγραμμάτων ανάγνωσης εγγράφων PDF.