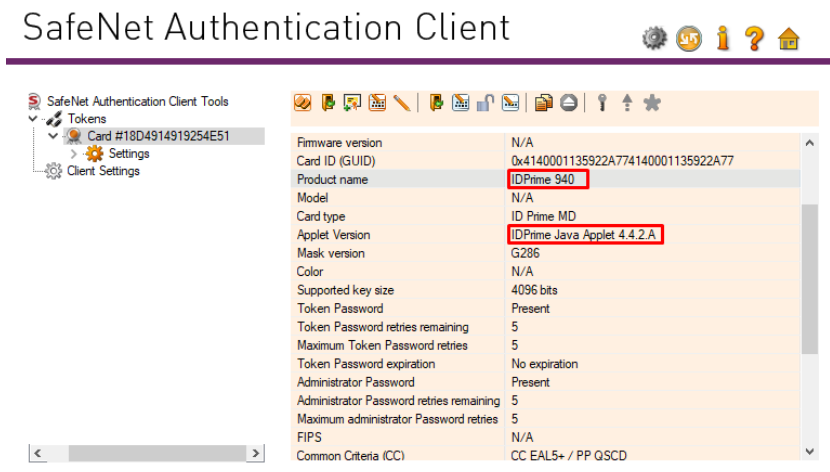
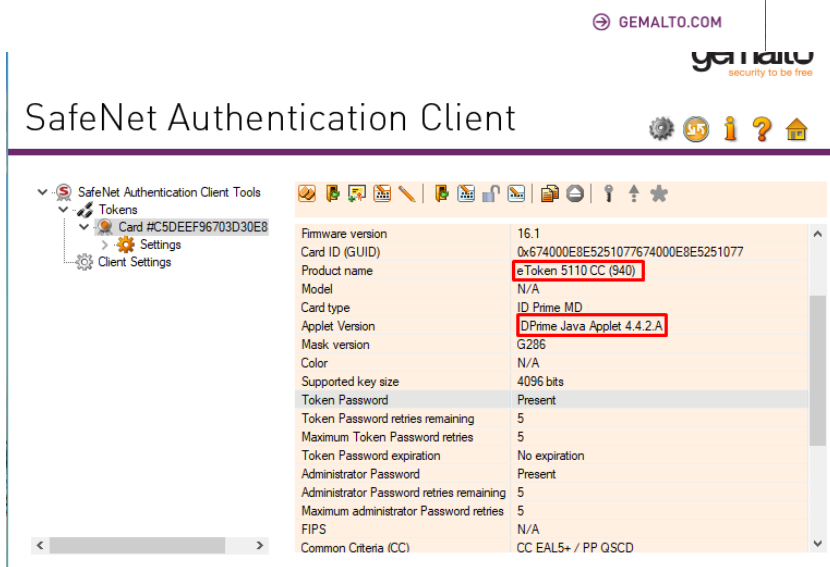
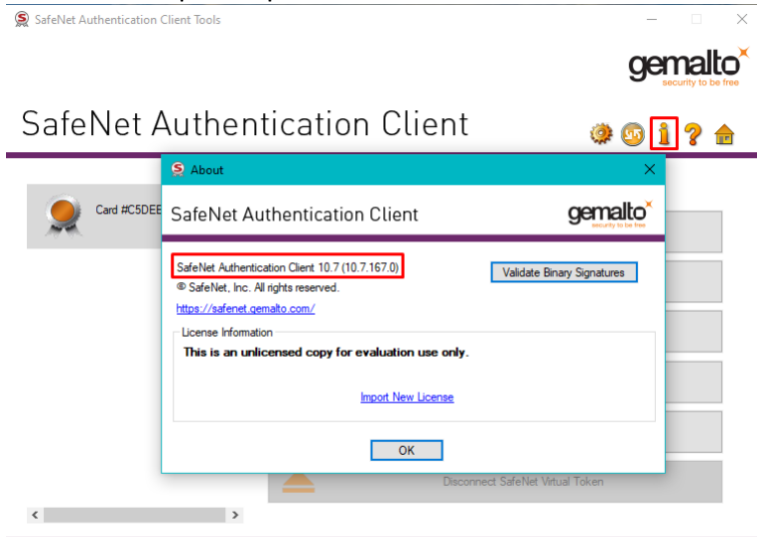


Διαδικασία έκδοσης Class A πιστοποιητικού HARICA σε υπολογιστή με εγκατεστημένο το SafeNet Authentication Client (SAC) 10.6 - 10.7

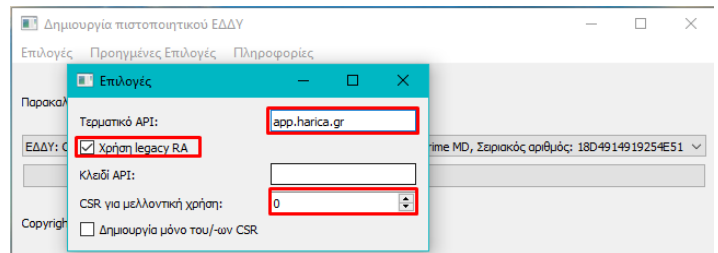
Η διαδικασία έκδοσης Class A πιστοποιητικού HARICA στις νέες ΕΔΔΥ *SafeNet eToken 5110CC* και *Gemalto IDPrime 940*, απαιτεί την εγκατάσταση του SafeNet Authentication Client έκδοση 10.6 ή 10.7.



Η διαδικασία που ακολουθεί περιγράφει τον τρόπο έκδοσης πιστοποιητικών σε αυτές τις συσκευές ή οποιαδήποτε άλλη που χρησιμοποιεί τις συγκεκριμένες εκδόσεις του SafeNet Authentication Client (π.χ. SafeNet eToken 5100 - 5110)

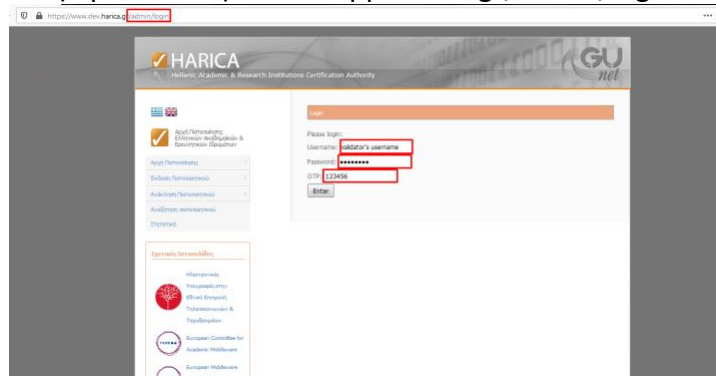
Στον υπολογιστή του validator θα πρέπει να προηγηθεί η λήψη του προγράμματος **pkcs11-enroll** που έχει δημιουργήσει η HARICA και από τις επιλογές να γίνουν οι παρακάτω ρυθμίσεις. ([Windows x64](#), [Windows x32](#), [Linux](#))

Τερματικό API: ο custom ιστοχώρος του Φορέα (π.χ. ca.uoa.gr) αν υπάρχει, διαφορετικά app.harica.gr
Χρήση legacy RA -> επιλεγμένο
CSR για μελλοντική χρήση: 0



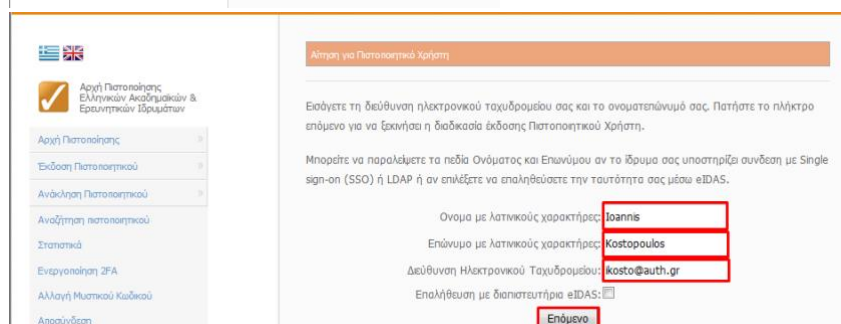
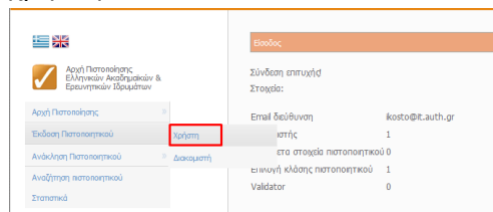
Βήμα 1

Με χρήση οποιουδήποτε πλοηγού (Firefox, Chrome, Edge) **εκτός** Internet Explorer, συνδεόμαστε στον ιστοχώρο του Φορέα εφόσον υπάρχει (π.χ. ca.uoa.gr/admin/login), διαφορετικά στη σελίδα app.harica.gr/admin/login.



Βήμα 2

Από τον **ίδιο πλοηγό** γίνεται το authentication (e-mail, sso) για την έκδοση πιστοποιητικού χρήστη.



Σε περίπτωση e-mail authentication, το όνομα και το επίθετο του χρήστη πρέπει να είναι ίδια με αυτά που αναγράφονται στο έγγραφο ταυτοπροσωπίας του.



Αρχή Πιστοποίησης
Ελληνικών Ακαδημαϊκών &
Ερευνητικών Ίδρυμάτων

- Αρχή Πιστοποίησης
- Έκδοση Πιστοποιητικού
- Ανάκληση Πιστοποιητικού
- Αναζήτηση πιστοποιητικού

Αίτηση για Πιστοποιητικό Χρήστη

Για να συνεχίσετε με το αίτημα για ψηφιακό πιστοποιητικό από την HARICA, παρακαλώ διαβάστε το μήνυμα στη θυρίδα ηλεκτρονικού ταχυδρομείου σας στον φορέα **Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (ΔΟΚΙΜΑΣΤΙΚΟ)** και ακολουθείστε τις εσώκλειστες οδηγίες.

Αν δεν λάβατε το μήνυμά ή συνέβη κάποιο σφάλμα, παρακαλώ επικοινωνήστε με το support@harica.gr.

Βήμα 3 (μόνο για Φορείς με e-mail authentication)

Ο χρήστης λαμβάνει μήνυμα στο ηλεκτρονικό του ταχυδρομείο, με το σύνδεσμο επιβεβαίωσης πρόσβασης. Ο σύνδεσμος πρέπει να ανοίξει στον **ίδιο πλοηγό** που έχει χρησιμοποιηθεί μέχρι στιγμής.

From: HARICA Helpdesk <help@harica.gr>
Subject: E-mail confirmation for HARICA User Certificate Request
To: ikosto@auth.gr

Αγαπητέ Κύριε/Κυρία,

Παρακαλώ ακολουθήστε τον παρακάτω σύνδεσμο με τον πλοηγό σας (συνιστούμε Chrome, Edge, Firefox, Safari) για να συνεχίσετε με το αίτημα πιστοποιητικού.

- [Σύνδεσμος επιβεβαίωσης πρόσβασης](#)

Αν δεν αιτηθήκατε εσείς την έκδοση ψηφιακού πιστοποιητικού, παρακαλώ να αναφέρετε το συμβάν στο validators-dev@harica.gr

Παρακαλώ μην απαντάτε σε αυτό το μήνυμα. Για οποιοδήποτε απορία, παρακαλώ επικοινωνήστε με το validators-dev@harica.gr.


Υποδομή Δημοσίου Κλειδιού HARICA


Βήμα 4


Γίνεται μεταφόρτωση του εγγράφου ταυτοπροσωπίας και επιλέγουμε **Κλάση A**.
Επιλέγουμε για χρήση πιστοποιητικού το **S/MIME + eSignature** και στη συνέχεια **Αιτούμαι**.


Αποσύνδεση

Σχετικές Ιστοσελίδες

- 

Ηλεκτρονικές Υπογραφές στην Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
- 

European Committee for Academic Middleware
- 

European Middleware Coordination and Collaboration
- 

Υποδομή Δημοσίου Κλειδιού ΑΠΘ

Υπεύθυνη Δήλωση Ταυτότητας

Δηλώνω υπεύθυνα με την υποβολή της αίτησης για ψηφιακό πιστοποιητικό ότι το πλήρες όνομά μου είναι **Ioannis Kostopoulos**, η διεύθυνση ηλεκτρονικού ταχυδρομείου **ikosto@auth.gr** μου ανήκει και ότι τα στοιχεία που περιέχονται στο πιστοποιητικό μου **Email=ikosto@auth.gr, serialNumber=2229570965, CN=Ioannis Kostopoulos, GivenName=Ioannis, Surname=Kostopoulos, O=Aristotle University of Thessaloniki, L=Thessaloniki, C=GR** είναι αληθινά.

Απαιτείται να ανεβάσετε ένα αρχείο που περιέχει ένα επίσημο έγγραφο ταυτοποίησης (Διαβατήριο/Ταυτότητα). Στο έγγραφο πρέπει να φαίνονται με ευκρίνεια το πλήρες όνομα (στα Λατινικά) και η εικόνα του/-ης Απών/-ούσας και να μην ξεπερνά το 2ΜΒ. **Ταυτότητες χωρίς το πλήρες όνομα στα Λατινικά δεν θα γίνουν δεκτές και το αίτημα θα απορριφθεί.**

Προσοχή: Η μεταφόρτωση της ταυτότητας είναι **υποχρεωτική** για την αίτηση του πιστοποιητικού.


Μεταφορά αντιγράφου ταυτότητας: Αναζήτηση αρχείου


Παρακαλώ επιλέξτε τον τύπο πιστοποιητικού που επιθυμείτε.


Κλάση A
Κλάση B


Αποσύνδεση

Σχετικές Ιστοσελίδες

- 

Ηλεκτρονικές Υπογραφές στην Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
- 

European Committee for Academic Middleware
- 

European Middleware Coordination and Collaboration
- 

Υποδομή Δημοσίου Κλειδιού ΑΠΘ

Υπεύθυνη Δήλωση Ταυτότητας

Δηλώνω υπεύθυνα με την υποβολή της αίτησης για ψηφιακό πιστοποιητικό ότι το πλήρες όνομά μου είναι **Ioannis Kostopoulos**, η διεύθυνση ηλεκτρονικού ταχυδρομείου **ikosto@auth.gr** μου ανήκει και ότι τα στοιχεία που περιέχονται στο πιστοποιητικό μου **Email=ikosto@auth.gr, serialNumber=2229570965, CN=Ioannis Kostopoulos, GivenName=Ioannis, Surname=Kostopoulos, O=Aristotle University of Thessaloniki, L=Thessaloniki, C=GR** είναι αληθινά.

Απαιτείται να ανεβάσετε ένα αρχείο που περιέχει ένα επίσημο έγγραφο ταυτοποίησης (Διαβατήριο/Ταυτότητα). Στο έγγραφο πρέπει να φαίνονται με ευκρίνεια το πλήρες όνομα (στα Λατινικά) και η εικόνα του/-ης Απών/-ούσας και να μην ξεπερνά τα 2ΜΒ. **Ταυτότητες χωρίς το πλήρες όνομα στα Λατινικά δεν θα γίνουν δεκτές και το αίτημα θα απορριφθεί.**

Προσοχή: Η μεταφόρτωση της ταυτότητας είναι **υποχρεωτική** για την αίτηση του πιστοποιητικού.

Μεταφορά αντιγράφου ταυτότητας: Αναζήτηση αρχείου

Χρήση πιστοποιητικού:

S/MIME
 S/MIME + eSignature

Αποδέχομαι τους Όρους Χρήσης, υπογράφω τις δηλώσεις και Αιτούμαι την έκδοση του Πιστοποιητικού.

Βήμα 5

Η αίτηση για την έκδοση πιστοποιητικού έχει υποβληθεί χωρίς CSR. Για την δημιουργία ζεύγους κλειδιών αντιγράφουμε το authorization code (χωρίς τα κενά στην αρχή και στο τέλος).

Βήμα 6

Τρέχουμε το πρόγραμμα rkcs11-enroll ενώ έχουμε συνδεδεμένη την ΕΔΔΥ στον υπολογιστή και πατάμε *Εκκίνηση*. Εισάγουμε το pin της συσκευής και στη συνέχεια μας ζητείται το authorization code από το προηγούμενο βήμα. Στο συγκεκριμένο βήμα δημιουργείται το ιδιωτικό κλειδί του χρήστη στη συσκευή και υποβάλλεται το αρχείο αιτήματος έκδοσης πιστοποιητικού (CSR).

Βήμα 7

Λαμβάνουμε μήνυμα ηλεκτρονικού ταχυδρομείου στο validators alias του Φορέα (π.χ. validators@harica.gr) με το σύνδεσμο επιβεβαίωσης στοιχείων. Πατώντας το σύνδεσμο, μεταφερόμαστε στη σελίδα όπου πρέπει να επαληθεύσουμε τα στοιχεία χρήστη (όνομα, επίθετο) βάσει του εγγράφου ταυτοπροσωπίας που έχει γίνει μεταφόρτωση.

Επιλέγουμε ότι τα στοιχεία είναι Σωστά και πατάμε Υποβολή.

Βήμα 8

Ο χρήστης λαμβάνει μήνυμα στο ηλεκτρονικό του ταχυδρομείο, με το σύνδεσμο παραλαβής πιστοποιητικού. Στη συνέχεια επιλέγει *Αποδέχομαι και επιθυμώ να παραλάβω το πιστοποιητικό μου (Χειροκίνητη εισαγωγή σε ΕΔΔΥ)* και *Παραλαβή πιστοποιητικού σε Δυαδική μορφή*. Η παραλαβή του πιστοποιητικού θα γίνει σε μορφή .cer την οποία αναγνωρίζει ο SafeNet Authentication Client.

From: HARICA PKI Administrator <noreply@harica.gr>
Subject: Your HARICA Digital Certificate request has been approved
To: ikosto@auth.gr

Αγαπητέ Κύριε/Κυρία,

Το πιστοποιητικό σας για την συνύληξη με διακεκριμένο όνομα Email=ikosto@auth.gr, serialNumber=2229570965, CN=Ioannis Kostopoulos, OU=Class A - Private Key created and stored in hardware CSP, GivenName=Ioannis, Surname=Kostopoulos, O=Aristotle University of Thessaloniki, L=Thessaloniki, C=GR έχει εκδοθεί από τον διαχειριστή της Αρχής Πιστοποίησης.

Ακολουθήστε τον παρακάτω σύνδεσμο χρησιμοποιώντας τον πλοηγό και τον υπολογιστή με τον οποίο υποβάλατε την αίτηση για να παραλάβετε το πιστοποιητικό σας:

- [Παραλαβή του πιστοποιητικού μου](#)

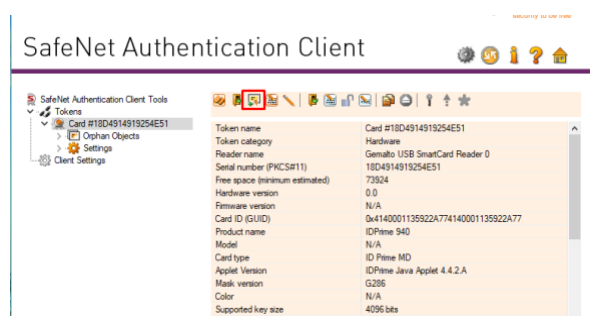
Στην περίπτωση που δεν παραλάβετε το πιστοποιητικό σας εντός 30 ημερών, αυτό θα ανακληθεί αυτόματα.

Παρακαλώ μην απαντήσετε σε αυτό ο e-mail. Για οτιδήποτε περαιτέρω παρακαλώ επικοινωνήστε με το support@harica.gr

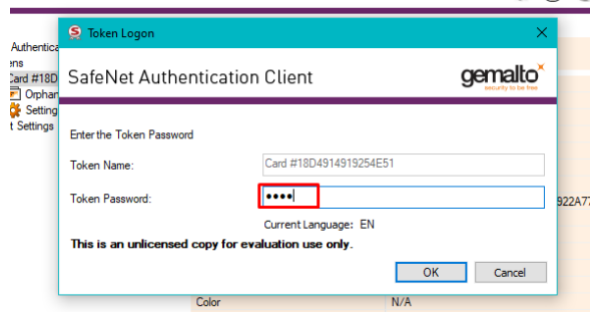
Υποδομή Δημοσίου Κλειδιού HARICA

Βήμα 9

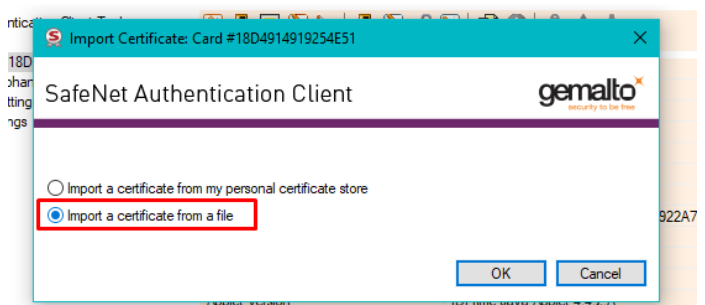
Ανοίγουμε το SafeNet Authentication Client Tools, επιλέγουμε *Advanced View* και στη συνέχεια *Import Certificate*.



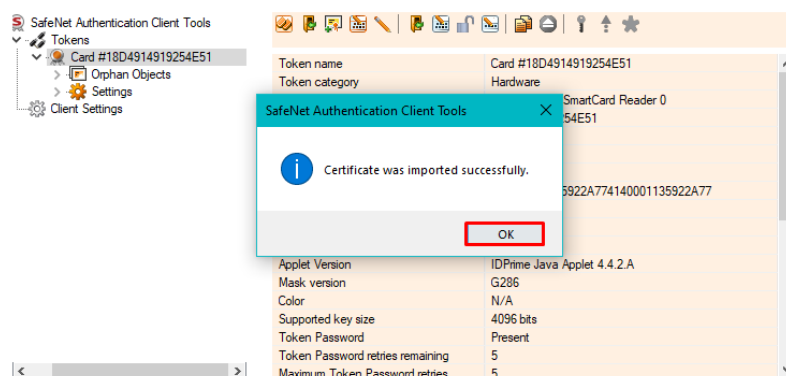
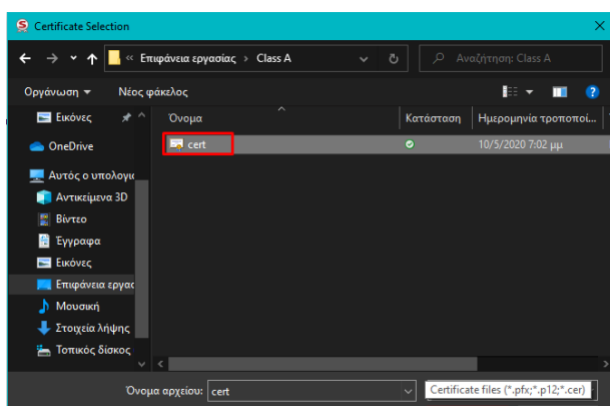
Δίνουμε το pin της συσκευής (*Token Password*)



Επιλέγουμε *Import a certificate from a file*



Επιλέγουμε το πιστοποιητικό του χρήστη που κάναμε λήψη από το προηγούμενο βήμα.

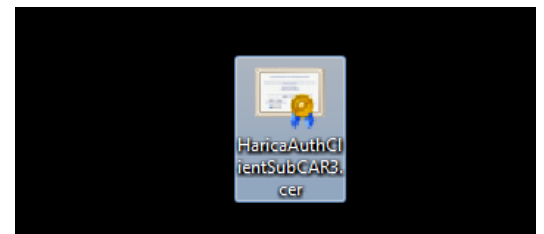
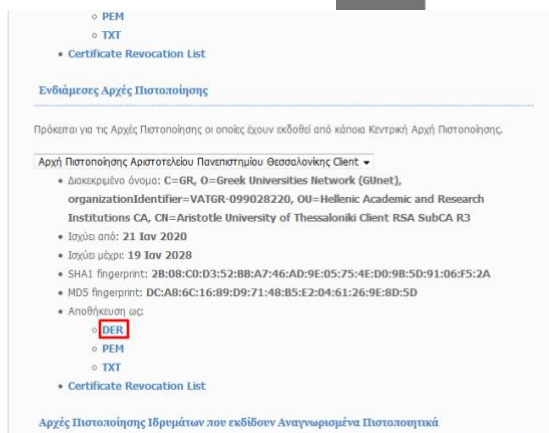
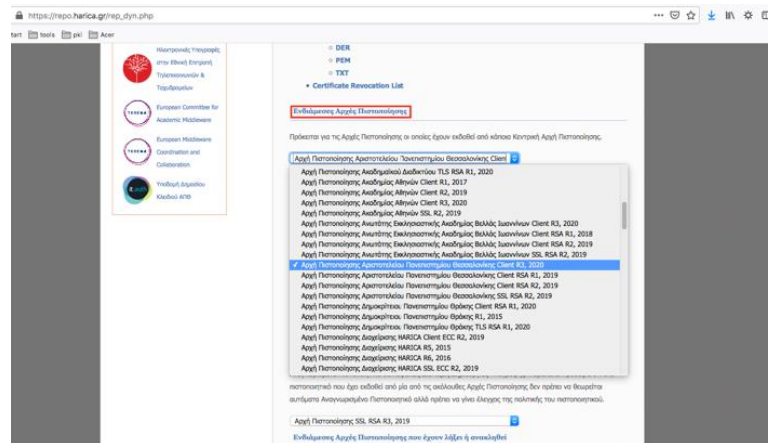


Βήμα 10

Κατεβάζουμε την Αρχή Πιστοποίησης του Φορέα μας, που εξέδωσε το πιστοποιητικό από τη σελίδα

<https://repo.harica.gr/>

Επιλέγουμε το αρχείο σε μορφή .der, το οποίο αποθηκεύουμε τοπικά στον υπολογιστή και το κάνουμε μετονομασία σε .cer



Ακολουθούμε την ίδια διαδικασία με το Βήμα 9 και προσθέτουμε την Αρχή Πιστοποίησης του Φορέα μας στην ΕΔΔΥ, ώστε να υπάρχει όλη η αλυσίδα πιστοποιητικών και να εισάγεται στην υπογραφή του χρήστη.

SAFE NET AUTHENTICATION CLIENT

