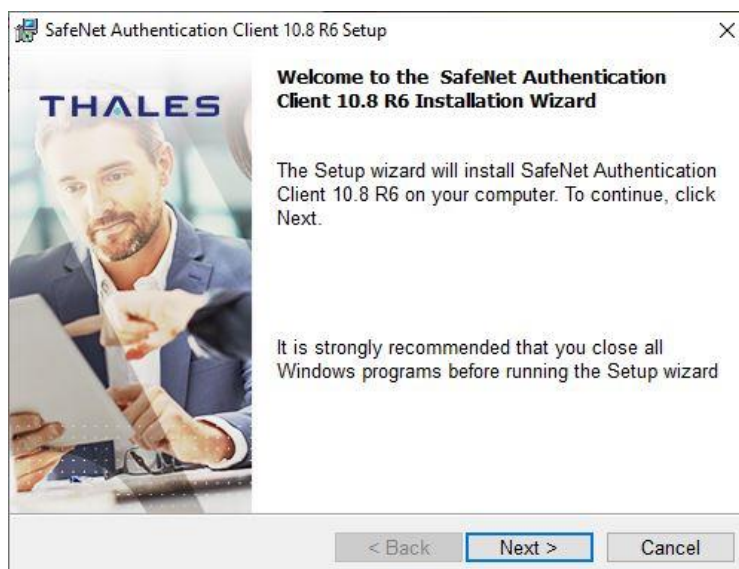
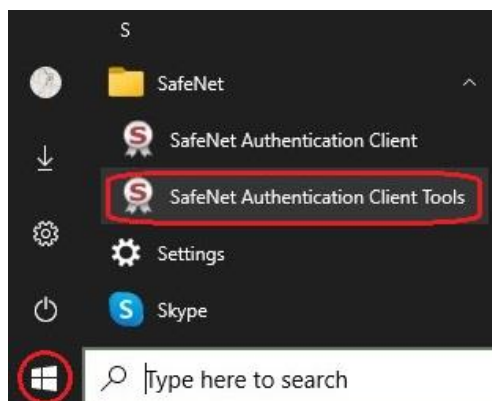


**ΕΓΚΑΤΑΣΤΑΣΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΣΕ WINDOWS – MD940****1. Εγκατάσταση λογισμικού SafeNet Authentication Client**

Προτού χρησιμοποιήσετε το USB token MD940, είναι απαραίτητο να εγκαταστήσετε το λογισμικό SafeNet Authentication Client της Thales, το οποίο μπορείτε να βρείτε στην ιστοσελίδα μας ([www.optis.gr](http://www.optis.gr)). Ξεκινάτε την εγκατάσταση του λογισμικού κάνοντας διπλό κλικ στο αρχείο SafeNetAuthenticationClient-x\*\*-10.8-R6.msi.



- Πατάτε **Next**
- Επιλέγετε γλώσσα
- Διαβάζετε και αποδέχεστε τους όρους χρήσης
- Επιλέγετε τον φάκελο εγκατάστασης (συνιστάται να αφήσετε τον προεπιλεγμένο)
- Επιλέγετε τύπο εγκατάστασης (συνιστάται ο προεπιλεγμένος)
- Πατάτε **Install**
- Πατάτε **Finish**
- Το πρόγραμμα μπορείτε να το βρείτε στο **Start > SafeNet > SafeNet Authentication Client Tools**



## 2. Προεπιλεγμένοι κωδικοί του USB token

Ένα καινούριο usb token ή κάρτα MD940 έχει τους ακόλουθους προεπιλεγμένους (default) κωδικούς:

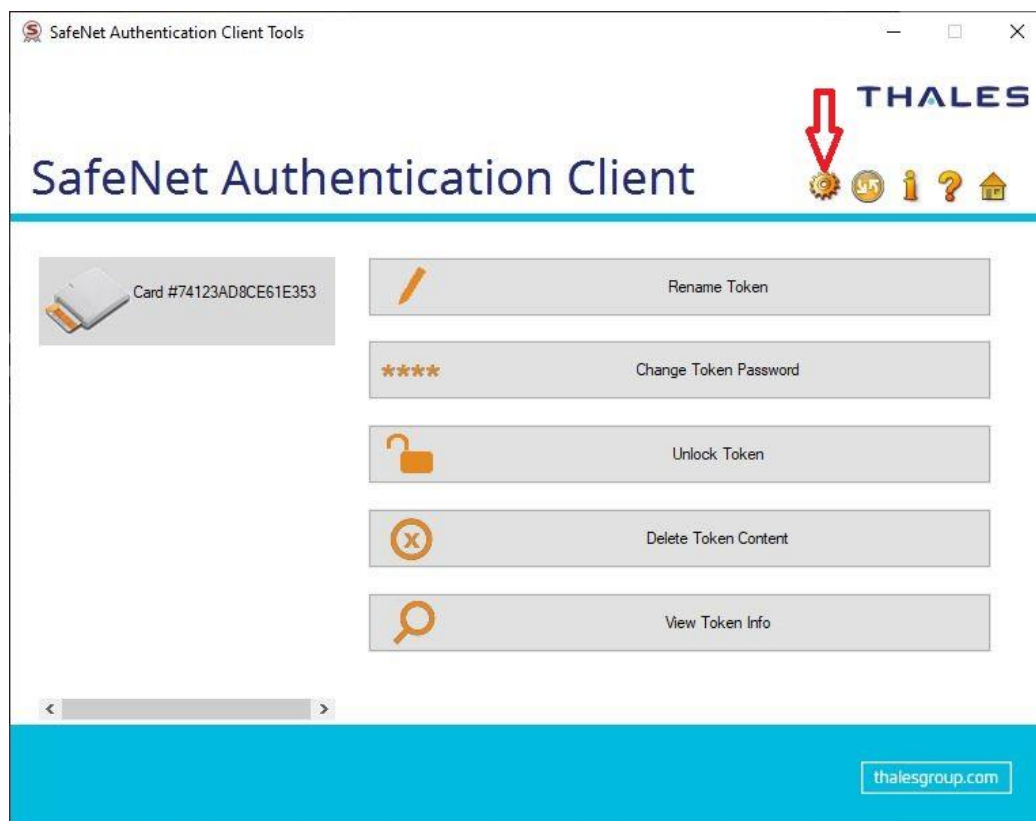
<b>Token Password</b>	0000
<b>Administrator Password</b>	0000000000000000000000000000000000000000000000000000000 (48x0)
<b>Digital Signature PIN</b>	000000
<b>Digital Signature PUK</b>	000000

Οι παραπάνω κωδικοί θα πρέπει να αλλαχθούν για λόγους ασφαλείας. Αφού αλλαχθούν τους γνωρίζει μόνο ο ίδιος ο χρήστης! Παρακάτω περιγράφεται το πώς μπορείτε να ορίσετε τους εν λόγω κωδικούς.

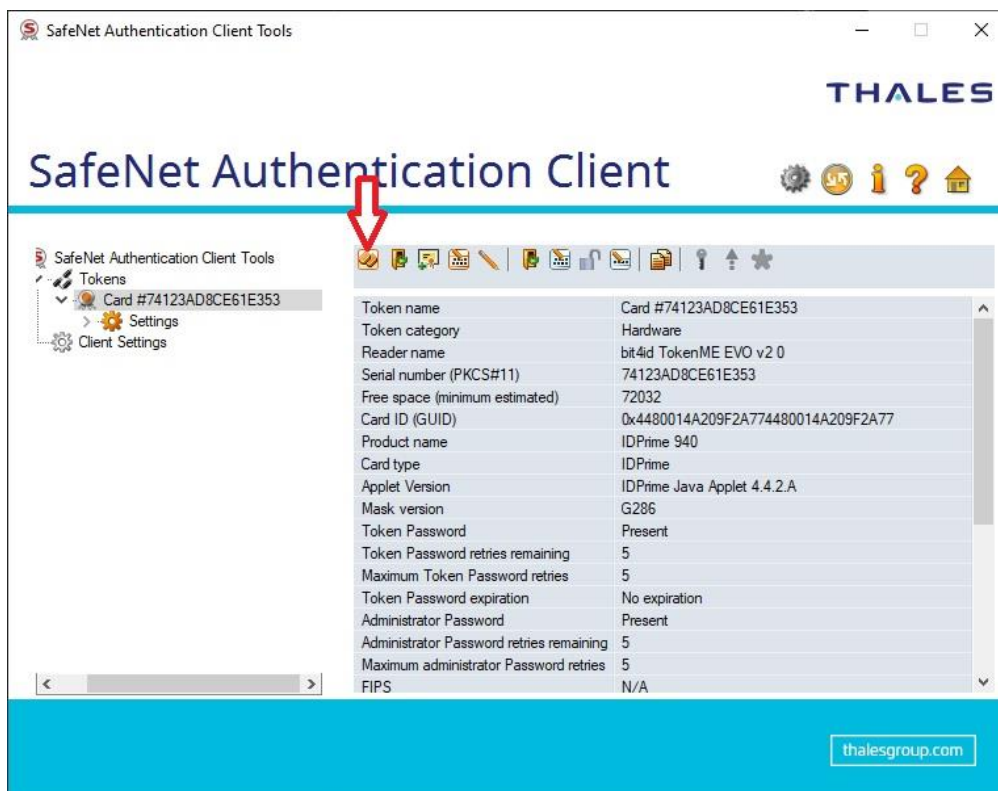
## 3. Αρχικοποίηση του USB token

Στην αρχή συιστάται να κάνετε Αρχικοποίηση (Initialize) του USB token, για να ορίσετε τους απαραίτητους κωδικούς ασφαλείας.

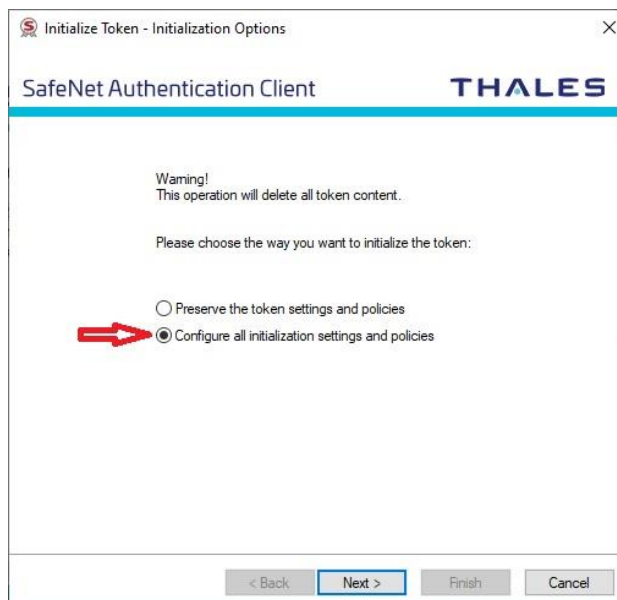
- Συνδέετε το USB token στον σταθμό εργασίας
- Ανοίγετε το πρόγραμμα **SafeNet Authentication Client Tools**
- Από το παράθυρο που εμφανίζεται, επιλέξετε **Advanced View**



- Επιλέγετε **Initialize Token**



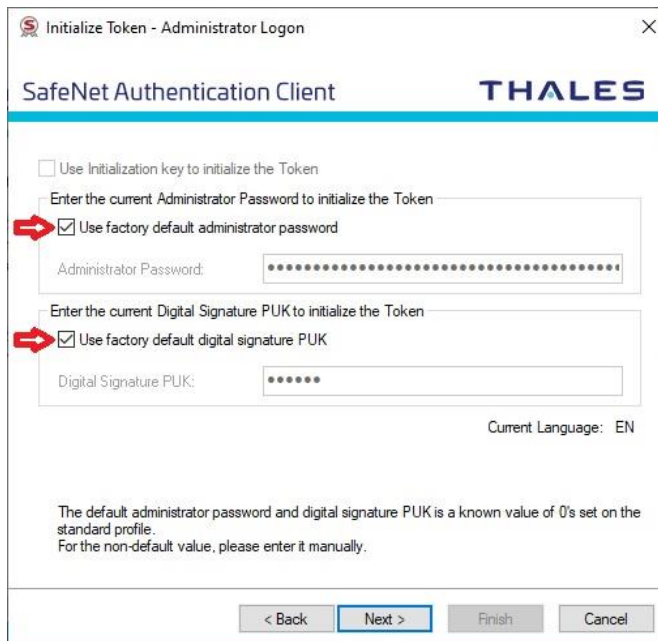
- Επιλέγετε **Configure all initialization settings and polices** και πατάτε **Next**



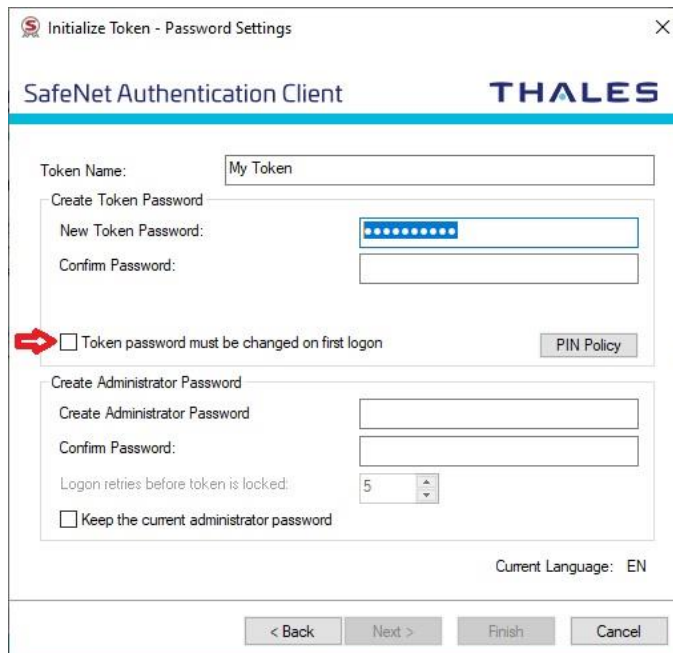
**Προσοχή!**

Κάνοντας Αρχικοποίηση του token, διαγράφονται όλα τα περιεχόμενα που έχουν περαστεί στο USB token.

- Επιλέγοντας τα **2 Checkboxes** γίνεται χρήση των προεπιλεγμένων κωδικών (Αν έχετε αλλάξει τους κωδικούς στο παρελθόν, πληκτρολογήστε τους κωδικούς που έχετε θέσει!)
- Πατάτε **Next**



- Ορίζετε:
  - το όνομα του Token
  - το **Token Password** (ζητείται και επιβεβαίωση)
  - το **Administrator Password** (ζητείται και επιβεβαίωση)
- Αφαιρείτε την επιλογή **Token password must be changed on first logon** και πατάτε **Next**



#### Σημειώσεις:

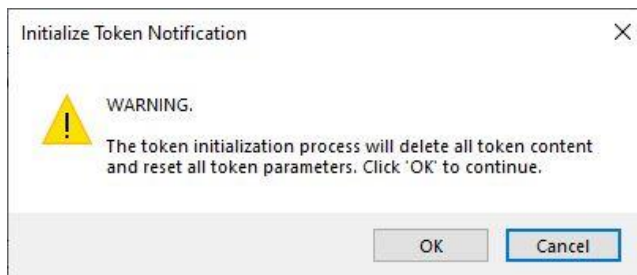
- Ένας κωδικός πρέπει να αποτελείται από 6 έως 8 χαρακτήρες και να περιέχει συνδυασμό από κεφαλαία γράμματα, πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες (όπως !, \$, #, %)
- Προσέχετε να έχει επιλεγθεί Current Language: EN
- Οι κωδικοί που ορίζετε είναι προσωπικοί. Δεν καταχωρούνται κάπου. Μην τους ανακοινώσετε σε άλλα άτομα και αν υποψιάζεστε ότι έχουν διαρρεύσει, συστήνεται να τους αλλάξετε.



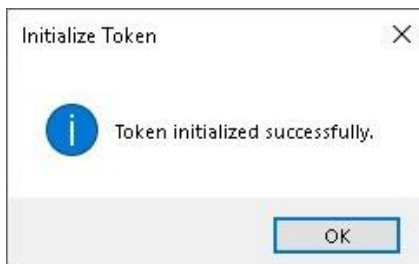
- Ορίζετε:
  - το **Digital Signature PIN** (ζητείται και επιβεβαίωση)
  - το **Digital Signature PUK** (ζητείται και επιβεβαίωση)
- Πατάτε **Finish**



- Πατάτε **OK**



- Η Αρχικοποίηση ολοκληρώθηκε επιτυχώς, πατάτε **OK**



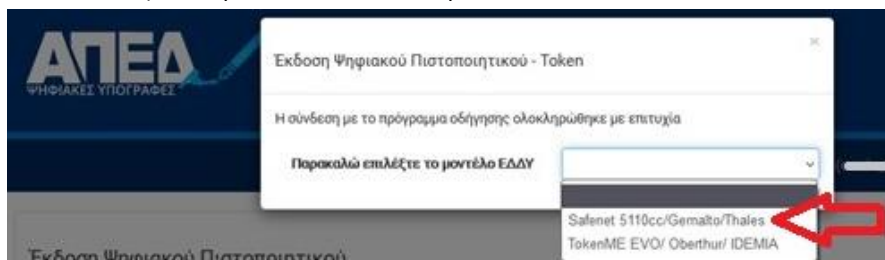
#### 4. Απόκτηση ψηφιακής υπογραφής (ΟΔΗΓΙΕΣ ΑΠΕΔ)

Για τη λήψη ψηφιακής υπογραφής, απαιτείται η παραμετροποίηση του σταθμού εργασίας βάσει των οδηγιών της Αρχής Πιστοποίησης Ελληνικού Δημοσίου. Ακολουθήστε τις οδηγίες που βρίσκονται στα παρακάτω links:

[Απόκτηση ψηφιακής υπογραφής](#)

[Οδηγίες υπογραφής μέσω JSigndf](#)


- Όταν κληθείτε να επιλέξετε το μοντέλο ΕΔΔΥ, επιλέγετε: **Safenet 5110cc/Gemalto/Thales**

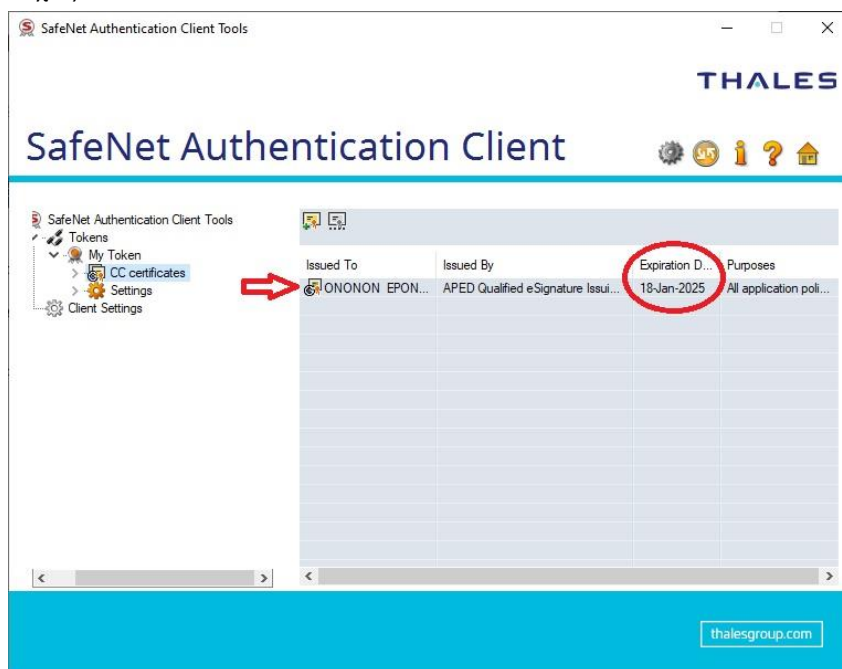


- Αρχικά θα σας ζητηθεί το Token Password και έπειτα το Digital Signature PIN

#### 5. Έλεγχος πιστοποιητικών

Όταν ολοκληρώσετε τη διαδικασία λήψης του πιστοποιητικού από την ΑΠΕΔ, για να βεβαιωθείτε ότι το πιστοποιητικό έχει εγκατασταθεί σωστά, μπορείτε να ακολουθήσετε τα παρακάτω βήματα:



- Με συνδεδεμένο το USB token, ανοίγετε το πρόγραμμα **SafeNet Authentication Client Tools**
- Επιλέγετε **Advanced View** 
- Από την αριστερή στήλη επιλέγετε **CC certificates**
- Αν εμφανίζεται το πιστοποιητικό με το Όνομα και το Επώνυμό σας, όπως φαίνονται παρακάτω, η έκδοση ολοκληρώθηκε επιτυχώς

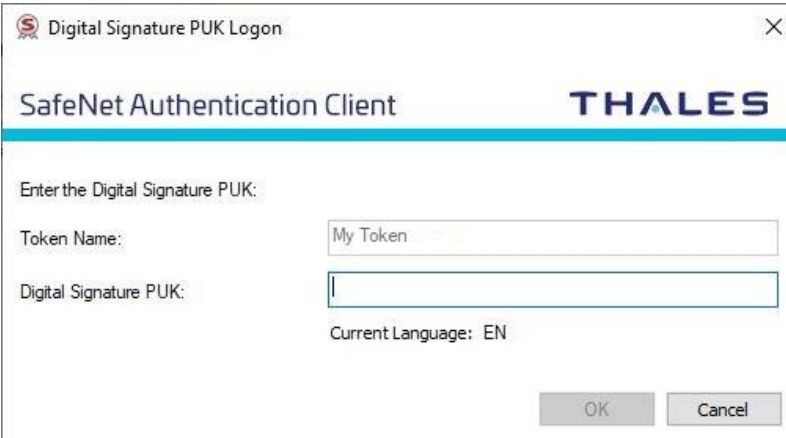


- Στην τρίτη στήλη βλέπετε την ημερομηνία λήξης του πιστοποιητικού σας

**ΠΡΟΣΘΕΤΕΣ ΟΔΗΓΙΕΣ****1. Ξεκλείδωμα Digital Signature PIN με χρήση του Digital Signature PUK**

Σε περίπτωση που ο χρήστης ξεχάσει το Digital Signature PIN ή το κλειδώσει μετά από επιλαμβανόμενη λανθασμένη εισαγωγή, παρέχεται η δυνατότητα να το ορίσει εκ νέου κάνοντας χρήση του Digital Signature PUK:

- Με συνδεδεμένο το USB token, ανοίγεται το πρόγραμμα **SafeNet Authentication Client Tools**
- Επιλέγεται **Advanced View** 
- Επιλέγεται **Set Digital Signature PIN** 
- Πληκτρολογείται το **Digital Signature PUK** και πατάτε **OK**



- Πληκτρολογείται το νέο επιθυμητό **Digital Signature PIN** (ζητείται και επιβεβαίωση) και πατάτε **OK**



- Το Digital Signature PIN ορίστηκε επιτυχώς