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

Η διαδικασία έκδοσης Class Α 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.

Client έκδοση 10.6 ή	10.7.	
SafeNet Authentication Client Tools		- ○ × gemalto [×]
SafeNet Authent	ication Client	🚳 🖓 🚺 🤉 🌧
S About		× • • • • •
Card #C5DEE SafeNet Aut	hentication Client	
SafeNet Authenticati © SafeNet. Inc. All ri	on Client 10.7 (10.7.167.0) ahts reserved.	Validate Binary Signatures
https://safenet.gema	ito.com/	
This is an unlice	nsed copy for evaluation use only.	
	Import New License	
	ОК	
	Disconnec	t SafeNet Virtual Token
< >		
		→ GEMALTO.COM
I		yanalu
		security to be free
SafeNet Auther	ntication Clier	nt 🛛 🐲 😳 🧯 🥐 🎰
SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools	🥺 🖗 🖾 🖼 🖊 🦉 🖬 🚽	『▶』 🗃 🖨 ¥ 🛧 🛠
> Settings	Firmware version Card ID (GUID)	16.1 0x674000E8E5251077674000E8E5251077
8 -	Model	N/A
	Applet Version	DPrime Java Applet 4.4.2.A
	Color Supported key size	N/A 4096 bits
	Token Password	Present 5
	Maximum Token Password expiration	5 5 No expiration
	Administrator Password extrine remain	Present
	Maximum administrator Password retri	es 5
< >	Common Criteria (CC)	CC EAL5+ / PP QSCD
SafaNlat Author	tication Clion	st and a
		n 🎯 😳 1 ? 🔒
SafeNet Authentication Client Tools	● ● □ □	` ⊳ ₽
 Card #18D4914919254E51 Settings 	Firmware version Card ID (GUID)	N/A 0x4140001135922A774140001135922A77
ଲ୍ଲୁର୍ବୁ Ulient Settings	Product name Model	IDPrime 940 N/A
	Card type Applet Version	ID Prime MD
	Mask version	G286
	Supported key size	4096 bits Breast
	Token Password	Fresent

Token Password retries remaining Maximum Token Password retries

Administrator Password retries remaining 5 Maximum administrator Password retries 5

Token Password expiration Administrator Password

Common Criteria (CC)

FIPS

< >

5

No expi Present

N/A

CC EAL5+ / PP QSCD

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. (<u>Windows x64</u>, <u>Windows x32</u>, <u>Linux</u>)

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

🔳 Δημι	ουργία πιστοποιητικού ΕΔΔΥ					-		\times
Επιλογές	; Προηγμένες Επιλογές Πληρ	οφορίες						
	💽 Επιλογές	-		×				
Παρακαλ	Τερματικό API:	app.harica	.gr					
ΕΔΔΥ: Ο	🗹 Χρήση legacy RA				rime MD, Σειριακός	αριθμός: 18D493	14919254	E51 ~
	Κλειδί ΑΡΙ:							
	CSR για μελλοντική χρήση:	0		\$				
Copyrigh	Δημιουργία μόνο του/-ων CSR							

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.

MARICA	Etutions Certification Authority	I I I I I I I I I I I I I I I I I I I	GU
Constraints Constrain	sar Pixot lipti: Usaranci Addizi'y semane Pasiodi 01P (12365 Ether		-
Paradic transable Warawaii, Warawaii, Warawaii (t Topiani Topiani Adamsmid Adamsmid Topiani Adamsmid Adamsmid Topiani			

Βήμα 2

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

Anych Percensinger, Behryneiter Adorgeniatie & Behryneiter Adorgeniatie & Edelant Percensinger, Edelant Percensinger, Anderson Percensinger, Anderson Percensinger, Anderson Percensinger, Anderson Percensinger, Anderson Percensinger, Ziernemad Dataset Adorgeniatie (Comparison)	Elsoloc Závědaní smundrů Zřeváda: Ernal Šelidivon, kosto@it.auth.gr erna fosgla natronotitekoù 0 ersvný kládar (natronotitekoù 0 Validator 0	
	Αίτηση για Πατοιοιητικά Χρήστη Εισάγετε τη διεύθυνση ηλοκτρονικού τοχυδρομείου σας και το σνοματειτώνυμό σας. Πατήστε το πλήκτρο επόμεινο για να ξισκιήσια η διαδικασία έκδοσης Πιστοποητικού Χρήστη. Μποράτε να παραλάψετε τα πεδία Ονόματος και Επωνύμου αν το ίδρυμα σος υποστηρίζα συνδεση με Single sign-on (SSO) ή LDAP ή αν επιλέξατε να επαληθιεύσετε την ταυτότητα σος μέσω «IDAS. Ονομα με λατινικούς χαρακτήρες Toannis Επώνυμο με λατινικούς χαρακτήρες Kostopoulos Διεύθυνση Ηλικτρονικού Ταχυδρομείου: Kosto@auth.gr Επαλήθευση με διοποτευτήρια «IDAS:	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 Ακαδημ Ερευνητικών Ιδρυμ	αϊκών & άτων
Αρχή Πιστοποίησης	
Έκδοση Πιστοποιητικού	
Ανάκληση Πιστοποιητικού	
Αναζάτηση αστοποιητικού	

Για να συνοχίσετε με το αίτημα για ψηφιακό πιστοποιητικό από την ΗΑΡΙCΑ, παρακαλώ δαβάστε το μήνυμα στη θυρίδα ηλεκτρονικού τοχυδρομείου σας στον φορέα **Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης** (ΔΟΚΙΜΑΣΤΙΚΟ) και σκολουθείστε τις εσώκλεστες οδηγίες.

Αν δεν λάβατε το μήνυμα ή συνέβη κάποιο σφαλμα, παρακαλώ επικοινωνήστε με το support at 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 <noreply@harica.gr> 🏠</noreply@harica.gr>	* Reply	* Reply All V	+ Forward	Archive	ð Junk
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, Saf	fari) για να συνεχίσετε	με το <mark>αίτημα</mark> π	ιιστοποιητι	κού.	
 Σύνδεσμος επιβεβαίωσης πρόσβασης. 					
Αν δεν αιτηθήκατε εσείς την έκδοση ψηφιακού πιστοποιητικού, παρακαλώ να αναφέρετε το συμβάν στο <u>vali</u>	dators-dev@harica.gr.				
Παρακαλώ μην απαντάτε σε αυτό το μήνυμα. Για οποιεσδήποτε απορίες, παρακαλώ επικοινωνήστε με το 🔬	lidators-dev@harica.gr				

Βήμα 4

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





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 pkcs11-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).

🔳 Δημιουργία πιστοποιητικού ΕΔΔΥ	🗈 Δημιουργία πιστοποιητικού ΕΔΔΥ
Επιλογές Προηγμένες Επιλογές Πληροφορίες	Επιλογές Προηγμένες Επιλογές Πληροφορίες
Παρακολώ επλέξτε ΕΔΔΥ:	Σύνδεση στην ΕΔΔΥ
ΕΔΔΥ: Card #18D4914919254E51, Κατασκευαστής: Gemalto, Μοντέλο: ID Prime MD, Σεριακός αριθμός: 18D4914919254E51 🔻	ΕΔΔΥ: Card #18D4914919254E51, Κατασ
Εκκάνηση	OK Cancel
Copyright © 2017-2020 HARICA	Copyright © 2017-2020 HARICA
Δημιουργία πιστοποιητικού ΕΔΔΥ	🗈 Δημιουργία πιστοποιητικού ΈΔΔΥ
Επιλογές Προηγμένες Επιλογές Πληροφορίες	Επιλογές Προηγμένες Επιλογές Πληροφορίες
Ynoβoλή artiµaroc moronomie Authorization Code P Ynoβoλή artiµaroc moronomie Παριακλώ ασογάγετε το authorization code του artiµaroc ΕΔΔΥ: Card # 180/#914919254 Παριακλώ ασογάγετε το authorization code του artiµaroc ΕΔΔΥ: Card # 180/#914919254 TSISOPDTWRYCZΣΗΤΥΠΤΥΥΡΓΟΚΑΤΕΡΕΙΟΣΕΙΟΟΡΓΑΧΙ OK Cancel Copyright © 2017-2020 HARICA	Σ Υποβολή αιτήματος πιστοποιητικού Υποβολή αιτήματος πιστοποιητικού ΕΔΔΥ: Card #1804914919 Οκ Copyright © 2017-2020 HARICA

Βήμα 7

Λαμβάνουμε μήνυμα ηλεκτρονικού ταχυδρομείου στο validators alias του Φορέα (π.χ. <u>validators@harica.gr</u>) με το σύνδεσμο επιβεβαίωσης στοιχείων. Πατώντας το σύνδεσμο, μεταφερόμαστε στη σελίδα όπου πρέπει να επαληθεύσουμε τα

From HARICA Helpdesk < noreply@	harica.gr> 🏠			Reply	* Reply All V	→ Forward	Archive 🗠	👌 Junk	Delete	More *
Subject Validator confirmation for H	ARICA User Certificate Reques	t								8:36 π.,
To validators-dev@harica.gr✿										
Ος επίσρυος εκποόσωπος το	υ φορέα Αριστοτέλειο Π	ανεπιστήμιο Θεσσαλογίκης (Δ	ΟΚΙΜΑΣΤΙΚΟ) παρακαλώ ακολομθά	OTE TON BO	ιοσκάτω σύνδι		emBeBouid	ναετε ή γι	a aounflein	e ón
χρήστης loannis Kostopoulo	s, ο οποίος αιτήθηκε ένα	ψηφιακό πιστοποιητικό με το α	ικόλουθο Διακεκριμένο όνομα Email	=ikosto@	auth.gr. serial	Number=22	29570965.	CN=loar	inis Kostor	oulo
OU=Class A - Private Key cre	ated and stored in hardw	vare CSP, GivenName=Ioannis,	Surname=Kostopoulos, O=Aristotle	University	of Thessaloni	ki, L=Thessa	loniki, C=0	GR, είναι	μέλος του	φορι
σας και ότι, με βάση την κρία	η σας, η ηλεκτρονική διε	ύθυνση ikosto@auth.gr του αν	ńKEL.							
			-pase -							
ΣΗΜΕΙΩΣΗ: Ο χρήστης αιτήθ	ηκε εγκεκριμένο πιστοπο	οιητικό.	- 1							
ΣΗΜΕΙΩΣΗ: Ο χρήστης αιτήθ • Σύνδεσμος επιβεβαίως	ηκε εγκεκριμένο πιστοπο <u>τος στοιχείων</u>	υητικό.								
ΣΗΜΕΙΩΣΗ: Ο χρήστης αιτήθ • <u>Σύνδεσμος επιβεβαίως</u> Παρακαλούμε επισκευθείτε	ηκε εγκεκριμένο πιστοπο <u>της στοιχείων</u> τη σελίδα το συντομότερ	νιητικό. ο δυνατό, διότι εκκρεμεί η αίτη	ση του χρήστη του φορέα σας.							
ΣΗΜΕΙΩΣΗ: Ο χρήστης αιτήθ • Σύνδεσμος επιβεβαίως Παρακαλούμε επισκευθείτε	ηκε εγκεκριμένο πιστοπο <u>της στοιχείων</u> τη σελίδα το συντομότερ	νιητικό. ο δυνατό, διότι εκκρεμεί η αίτη	ση του χρήστη του φορέα σας.							
ΣΗΜΕΙΩΣΗ: Ο χρήστης αιτήθ • <u>Σύνδεομος επιβεβαίως</u> <u>Παρακαλούμε επισκευθείτε</u>	ηκε εγκεκριμένο πιστοπο <u>ης στοιχείων</u> τη σελίδα το συντομότερ	νιητικό. ο δυνατό, διότι εκκρεμεί η αίτη	ση του χρήστη του φορέα σας.							

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.



Βήμα 9

Password)

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

SafeN	let Authentication Client Tools okens (Card #18D4914919254E51	🥹 🖟 🗊 🗟 🔪 🖟 🗟 Token name	IP ≥ ≥ ○ ? * * Card #18D4914919254E51	•
>	IF Orphan Objects	Token category	Hardware Generate USP SmootCovel Reader 0	
;iji Cl	ient Settings	Serial number (PKCS#11)	18D4914919254E51	
		Free space (minimum estimated)	73924	
		Hardware version	0.0	
		Card ID (GUID)	Dx4140001135922A774140001135922A77	
		Product name	IDPrime 940	
		Card type	ID Prime MD	
		Applet Version	IDPrime Java Applet 4.4.2.A	
		Mask version	G286	
		Supported key size	4096 bits	
	🤶 Token Logon		×	-
entica			comalta	
#18D Inphan	SafeNet Authe	ntication Client	Generation Recurity to be free	
etting tings	Enter the Token Passwor	d		
	Token Name:	Card #18D4914	919254E51	
	Token Password:	••••		922A77
	This is an unlicensed	Current Langua copy for evaluation use on	ge: EN Iy.	
			OK Cancel	
		Color	N/A	
S In	nport Certificate: Ca	ard #18D4914919254E51	8 10 0 00 00 00 00 00	×
Safe	eNet Authen	tication Client	ge	malto

OK Cancel

Επιλέγουμε Import a certificate from a file

Δίνουμε το pin της συσκευής (Token

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



Βήμα 10

μετονομασία σε .cer

Κατεβάζουμε την Αρχή Πιστοποίησης του Φορέα μας, που εξέδωσε το πιστοποιητικό από τη σελίδα <u>https://repo.harica.gr/</u> Επιλέγουμε το αρχείο σε μορφή .der, το οποίο αποθηκεύουμε τοπικά στον υπολογιστή και το κάνουμε

itti piki		-	
	L	¥	Trylenconservice Trylenconservice Togolgesetlev
	L	0	Furspean Committee for Academic Middleware
	L	0	European Middleware Coordination and Colleboration
	L	0	Visideori depension Khadaoj AND
	L		
	L		
	L		

Jaienet Authentication Glent

A https: tert 20 too

Control Contel Control Control Control Control Control Control Control Co







🧼 🗐 🧵 🥐 🎰

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.

SafeNet Authentication Client Tools 🛒 🔜 📦 - 🎸 Tokens 👷 Card #18D4914919254E51 Certificate: . User certificates Serial number 7A 36 AD 2D 95 78 CE C3 48 75 B2 3A 23 78 B1 FC 🔄 Ioannis Kostopoulos Ioannis Kostopoulos Issued to CA certificates Aristotle University of Thessaloniki Central CA R5 - Test 🔄 Aristotle University of Thessaloniki Central CA R5 - Test 10-May-2020 🔆 Settings 10-May-2022 Valid to Client Settings Intended purposes Client Authentication, Secure Email, Document Signing, Smartcard Lo. <None> Friendly name < Private key: Cryptographic Provider eToken Base Cryptographic Provider p11#f495fd51fc969103 Container name Modulus 8F 22 F1 81 31 CD 32 8F 63 0B 3D 5D C0 03 92 E9 38 DD B3 3E 40 Key size 2048 bits Key specification AT_KEYEXCHANGE Default key container Yes Auxiliary key container Yes < >