ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΤΜΗΜΑ: ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧ/ΚΩΝ & ΜΗΧ/ΚΩΝ Η/Υ
ΜΑΘΗΜΑ: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Διδακτικό έτος: 2019 -2020

Εργασία για το μάθημα «Ασφάλεια Υπολογιστικών Συστημάτων»

1. Αντικείμενο της εργασίας:

Απόκτηση προσωπικού ψηφιακού πιστοποιητικού (digital certificate), εξέταση του περιεχομένου του και χρήση του για την ψηφιακή υπογραφή (digital signature) και κρυπτογράφηση (encryption) αρχείων και email.

2. Βήματα που πρέπει να ακολουθήσετε:

Ι. ΕΚΔΟΣΗ ΠΡΟΣΩΠΙΚΟΥ ΨΗΦΙΑΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ (ΨΠ)

α) Από τη σελίδα του ΚΗΔ (βλ. http://it.auth.gr/el/security/personalCert) σύμφωνα με τις οδηγίες βγάλτε προσωπικό ψηφιακό πιστοποιητικό[1] *(για online αίτηση βλ. https://pki.auth.gr/issue).*
Αποθηκεύστε το πιστοποιητικό σας σε αρχείο σε format base-64 (π.χ. ***username*-cert.pem**)
(το αρχείο αυτό σας παρέχεται κατά την έκδοση του πιστοποιητικού σας ή εναλλακτικά εξάγοντάς το από τον browser σας ή ακόμα αναζητώντας το από τη σελίδα https://pki.auth.gr/search.php).

ΙΙ. ΕΞΕΤΑΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΨΗΦΙΑΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

β) Με την κατάλληλη εντολή openssl[2] εμφανίστε σε αναγνώσιμη μορφή το περιεχόμενο και τη δομή του πιστοποιητικού σας και αποθηκεύστε το περιεχόμενο αυτό σε ένα αρχείο κειμένου (π.χ. ***username*_AEM.docx**) μαζί με την εντολή openssl που τρέξατε.
Επίσης στην αρχή του κειμένου προσθέστε τα στοιχεία σας (Ονοματεπώνυμο, ΑΕΜ και ιδρυματικό email).

γ) Μέσα στο ίδιο αρχείο κειμένου εντοπίστε και επισημάνετε τα παρακάτω στοιχεία του πιστοποιητικού σας *(όπου είναι δυνατό ως inline κείμενο στο text output του πιστοποιητικού σας)*:

1. Το Common Name (CN) του πιστοποιητικού σας και η ημερομηνία λήξης του.
2. Τα Common-Names της ιεραρχίας της υποδομής δημοσίου κλειδιού (ΥΔΚ) που εξέδωσε το πιστοποιητικό σας.
3. Το url που περιγράφει τις πολιτικές και διαδικασίες πιστοποίησης της ΥΔΚ.
4. Το url του CRL που δημοσιοποιεί τα πιστοποιητικά που ανακαλούνται (CRL: λίστα ανάκλησης πιστοποιητικών).
5. Το όνομα του μη-συμμετρικού αλγόριθμου που χρησιμοποιήθηκε και το μέγεθος των κλειδιών σε bits.
6. Το modulus n.
7. Το δημόσιο κλειδί σας e.

---

[1] Η εργασία προϋποθέτει να χρησιμοποιήσετε το ιδρυματικό σας email (π.χ. *username*@ece.auth.gr)
[2] Στα windows το openssl διατίθεται από τη σελίδα: https://slproweb.com/products/Win32OpenSSL.html

III. ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΑΡΧΕΙΟΥ

δ) Μετατρέψτε το παραπάνω αρχείο κειμένου σε pdf (π.χ. ***username*_AEM.pdf**).

ε) Υπογράψτε με το ΨΠ σας το αρχείο pdf σύμφωνα με τις οδηγίες της σελίδας του ΚΗΔ.

στ) Στείλτε το τελικό ψηφιακά υπογεγραμμένο pdf αρχείο με email στο: asiach@ece.auth.gr
Το θέμα (subject) του email θα πρέπει να είναι της μορφής: «*ΑΕΜ,* εργασία ασφάλειας **μέρος Α**».
Στο κείμενο του email να βάλετε τα στοιχεία σας, δηλ. Ονοματεπώνυμο, ΑΕΜ και ιδρυματικό email.

IV. ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΟΥ

ζ) Χρησιμοποιώντας το OpenSSL κρυπτογραφήστε το αρχείο του πιστοποιητικού σας (δηλ. του ***username*-cert.pem**) με συμμετρικό αλγόριθμο AES (256 bits CBC mode) χρησιμοποιώντας για password το ΑΕΜ σας και αποθηκεύστε το σε ένα νέο αρχείο με όνομα της μορφής**:**
***username*-cert-encr.txt**

V. ΑΠΟΣΤΟΛΗ ΚΡΥΠΤΟΓΡΑΦΗΜΕΝΟΥ ΨΗΦΙΑΚΑ ΥΠΟΓΕΓΡΑΜΜΕΝΟΥ email

η) Ρυθμίστε τον email client σας (π.χ. Thunderbird, Outlook, κλπ) ή το AUTH webmail (webmail.auth.gr) ώστε να χρησιμοποιεί το πιστοποιητικό σας.

θ) Στη συνέχεια στείλτε με κρυπτογραφημένο ΚΑΙ ψηφιακά υπογεγραμμένο email το πιο πάνω AES-encrypted κρυπτογραφημένο αρχείο (δηλ. ***username*-cert-encr.txt**), καθώς και την εντολή που απαιτείται για την αποκρυπτογράφηση του αρχείου αυτού, στο email asiach@ece.auth.gr

Σημειώνεται ότι η κρυπτογράφηση του email προϋποθέτει να έχετε το πιστοποιητικό του παραλήπτη, το οποίο μπορείτε να βρείτε από τη σελίδα: https://pki.auth.gr/search.php *(**προσοχή** επιλέξτε το πιστοποιητικό του παραλήπτη τύπου **Class B)***

Το θέμα (subject) του email θα πρέπει να είναι της μορφής: «*ΑΕΜ,* εργασία ασφάλειας **μέρος Β**».

3. *Επισημάνσεις:*

- *Για όλα τα παραπάνω μπορείτε να βρείτε αναλυτικές οδηγίες στα εγχειρίδια που βρίσκονται στη σελίδα http://it.auth.gr/el/security/personalCert*
- *Στο κείμενο του κάθε email να βάλετε τα στοιχεία σας, δηλ. Ονοματεπώνυμο, ΑΕΜ και ιδρυματικό email καθώς και το κατάλληλο subject (όπως ορίζεται στις παραπάνω εκφωνήσεις)*
- *Στο τέλος θα πρέπει να στείλετε **μόνο μέχρι δύο emails** στο asiach@ece.auth.gr. Το 1ο email (μέρος Α) θα αφορά τα ερωτήματα I, II και III και το 2ο email (μέρος Β) τα ερωτήματα IV και V.*
  Αν αποστείλετε περισσότερα emails θα εξεταστούν μόνο τα 2 πρώτα. Σε κάθε ένα από τα 2 emails θα σας αποσταλεί σύντομη απάντηση που να επιβεβαιώνει τη λήψη τους.
- *Η ολοκλήρωση των I, II και III θα προσδίδει βαθμολογικό bonus, και η ολοκλήρωση των IV και V θα προσδίδει κάποιο επιπλέον bonus. Το μέγιστο βαθμολογικό bonus είναι 2 μονάδες στον τελικό βαθμό του μαθήματος, και θα προσμετράται μόνο εφόσον ο βαθμός της τελικής εξέτασης είναι πάνω από 5.*
- *Προθεσμία ολοκλήρωσης της εργασίας και αποστολής των δύο emails είναι η Παρασκευή 10 Ιανουαρίου 2020*
