**ΤΜΗΜΑ 1ο**

**Προμήθεια ΑΔΔΥ (Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής) τύπου usb tokens με το απαραίτητο συνοδευτικό λογισμικό**

**“Διεπαφές καθολικού σειριακού αγωγού (USB)” - CPV: 30237132-3,**

**ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Α/Α** | **ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΞΟΠΛΙΣΜΟΥ** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
|  | **ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ** |  |  |  |
| 1 | Αριθμός προσφερόμενων USB Tokens. Να αναφερθεί το μοντέλο για το προσφερόμενο τύπο USB Token. | 83 |  |  |
| 2 | Πιστοποίηση ασφάλειας | >= FIPS 140-1 level 2, CCEAL 4+ |  |  |
| 3 | Υποστήριξη PKCS #11 middleware  | >= v.2.01 |  |  |
| 4 | Συμβατό με USB  | >= 2.0 |  |  |
| 5 | **Υποστήριξη των ακόλουθων:** |  |  |  |
| 5.1. | * Ψηφιακές υπογραφές RSA με μήκος κλείδας μέχρι 2048 bits.
 | ΝΑΙ |  |  |
| 5.2. | * Δημιουργία ζευγών κλειδιών RSA μήκους μέχρι 2048 (μέγιστος αποδεκτός χρόνος δημιουργίας 30 sec) με γεννήτορα πραγματικών τυχαίων αριθμών
 | ΝΑΙ |  |  |
| 5.3. | * Κρυπτογράφηση /αποκρυπτογράφηση με τον αλγόριθμο 3DES.
 | ΝΑΙ |  |  |
| 5.4. | * Υποστήριξη του αλγορίθμου SHA-1
 | ΝΑΙ |  |  |
| 5.5. | * Padding PKCS#1 and ISO9796-2, which offer standard signature and message wrapping.
 | ΝΑΙ |  |  |
| 5.6. | * Συμμετρική κρυπτογραφία DES and Triple DES (56, 112 and 168 bit key length)
 | ΝΑΙ |  |  |
| 5.7. | * On board key generation, data signing, encryption On-card 512-2048 768 RSA, On-card 56-168 DESή ΑΕS
 | ΝΑΙ |  |  |
| 6 | EEPROM  | >= 64 kbytes |  |  |
| 7 | Να περιγραφεί η εγγύηση | ΝΑΙ |  |  |
| 8 | Διάρκεια εγγύησης | >= 1 |  |  |
|  | **ΣΥΝΟΔΕΥΤΙΚΟ ΛΟΓΙΣΜΙΚΟ** |  |  |  |
| 9 | Να περιγραφεί το λογισμικό | ΝΑΙ |  |  |
| 10 | Συμβατό με λειτουργικό Microsoft Windows 10 Professional GR, MS Windows XP/Vista/7 ή νεότερη | NAI |  |  |
| 11 | Συμβατό με λειτουργικό Linux | NAI |  |  |
| 12 | Συμβατό με λειτουργικό MAC-OS | NAI |  |  |
| 13 | Να περιγραφεί η υποστήριξη του λογισμικού (νεότερες εκδόσεις, bug fixes, κ.α.) | NAI |  |  |
| 14 | Διάρκεια υποστήριξης λογισμικού (χρόνια) | >= 3 |  |  |