Πρόταση διαδικασίας - δημιουργία και επιβεβαίωση ψηφιακής υπογραφής

Έκδοση 1.5 - 29/03/2024

Προαπαιτούμενα

Η προδιαγραφή της ΑΑΔΕ θετει τα παρακάτω προαπαιτούμενα για την ψηφιακή υπογραφή

1. Η ψηφιακή υπογραφή θα γίνεται με χρήση ECC (Elliptic Curve Cryptography)
2. Το μήκος κλειδιού θα είναι 256bits
3. Οι παραγόμενες υπογραφές θα είναι μήκους 64 bytes
4. Η είσοδος της υπογραφής θα περιέχει τα παρακάτω:
   α. Αναγνωριστικό παραστατικου (UID)
   β. MAPK σε περίπτωση ετεροχρονισμένης πληρωμής
   γ. Ημερομηνία και ώρα υπογραφής
   δ. Πληρωτέο ποσό
   ε. Καθαρή αξία
   στ. ΦΠΑ
   ζ. Συνολικό ποσό παραστατικού
   η. Terminal ID του μέσου πληρωμών

Προτάσεις

Οι προτάσεις μας σε σχέση με την τεχνική υλοποίηση των προαπαιτούμενων είναι οι παρακάτω:

Τυποποίηση του προς υπογραφή κειμένου

Για την δημιουργία ενός κειμένου το οποίο μπορεί να ανασκευάζεται ανεξάρτητα από την ΥΠΑΗΕΣ και το μέσο πληρωμής, προτείνεται η παρακάτω τυποποίηση.

Η καθαρή μορφή του προς υπογραφή κειμένου θα είναι text σε μορφή US-ASCII. Τα προαπαιτούμενα πεδία θα μπαίνουν στο κείμενο με την παρακάτω σειρά, σε μεταβλητού μήκους πεδία με την χρήση του χαρακτήρα ';' σαν field seperator.

Πεδία προς υπογραφή:

Πεδίο	**Υποχρεωτικό**	**Σχόλια**
UID	Ναί	
MAPK	Όχι	
Ημερομηνία/ώρα υπογραφής	Ναί	Η μορφή πρέπει να είναι YYYYMMDDhhmmss. Η ώρα θα είναι πάντα τοπική ώρα Ελλάδος
Καθαρή αξία	Ναί	
ΦΠΑ	Ναί	
Συνολικό ποσό παραστατικού	Ναί	
Πληρωτέο ποσό	Ναί	

Πεδίο	Υποχρεωτικό	Σχόλια
Terminal ID	Ναί	

Παράδειγμα ενός κειμένου προς υπογραφή, το οποίο περιέχει τις παρακάτω τιμές:

Πεδίο	Τιμή	Μορφοποιημένη τιμή
UID	D4F6A5F5C6123658F78369E5191ED5C9D73CB7AC	D4F6A5F5C6123658F78369E5191ED5C9D73CB7AC
MAPK	400013293980417	400013293980417
Ημερομηνία	2023/11/14 10:00:00 EEST	20231114100000
Καθαρή αξία	1.00	100
ΦΠΑ	0.24	24
Συνολικό ποσό	1.24	124
Πληρωτέο ποσό	1.24	124
Terminal ID	01234567	01234567

```
D4F6A5F5C6123658F78369E5191ED5C9D73CB7AC;400013293980417;20231114100000;100;24;124;124;012
34567
```

Σε περίπτωση που κάποιο πεδίο (όπως το MAPK) είναι κενό, αποτυπώνεται με πεδίο μηδενικού μήκους όπως παρακάτω:

```
D4F6A5F5C6123658F78369E5191ED5C9D73CB7AC;;20231114100000;100;24;124;124;01234567
```

ECC prime curve

Η τεχνολογία ECC έχει την απαίτηση επιλογής ενός prime curve κατά την υλοποίηση μιας λύσης. Η πρόταση μας είναι η χρήση του prime curve με όνομα prime256v1 το οποίο είναι τυποποιημένο σύμφωνα με τον οργανισμό NIST.

Παρακάτω ακολουθεί ένα παράδειγμα δημιουργίας ενός ζεύγους κλειδιών σύμφωνα με αυτό το curve με την βοήθεια της εφαρμογής openssl

```
openssl ecparam -name prime256v1 -genkey -out private_key.pem
openssl ec -in private_key.pem -pubout -out public_key.pem
```

Το αποτέλεσμα των εντολών είναι όπως παρακάτω

Private key:

```

```

```
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIAm8LOPlxVl8yQlflu5hRnNWN75yhfr7jJ1S3ZBfSiiKoAoGCCqGSM49
AwEHoUQDQgAEpzk6G8Y2bV3n539vK/+y7n4wZjD5fmhCXuTSxo+bg8t4NEqy8WHW
zF9SmHC7HnarnJ8p3gukw8Noxmavs7hPSw==
-----END EC PRIVATE KEY-----
```

Public key:

```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEpzk6G8Y2bV3n539vK/+y7n4wZjD5
fmhCXuTSxo+bg8t4NEqy8WHWzF9SmHC7HnarnJ8p3gukw8Noxmavs7hPSw==
-----END PUBLIC KEY-----
```

Αλγόριθμος υπογραφής

Για την δημιουργία ψηφιακής υπογραφής με χρήση κλειδιών ECC, προτείνεται ο αλγόριθμος ECDSA (Elliptic Curve Digital Signature Algorithm). Ο αλγόριθμος αυτός είναι επί του παρόντος ο πιο διαδεομένος αλγόριθμος ψηφιακών υπογραφών ECC και χρησιμοποιείται σε εφαρμογές όπως SSL/TLS.

Στις περιπτώσεις ψηφιακής υπογραφής με ECC κλειδιά, για λόγους ασφαλείας είναι συνήθης πρακτική η δημιουργία ενός hash από το αρχικό κείμενο και η κρυπτογράφηση του hash. Η πρόταση είναι η χρήση της hash function sha256

Η τελική υπογραφή έχει ονομαστικό μήκος 64 bytes σύμφωνα με τα προαπαιτούμενα, αλλά λόγω της φύσης του αλγορίθμου μπορεί να έχει διαφοροποιήσεις στο μέγεθος και μπορεί να είναι έως 71 με 72 bytes.

Ολοκληρωμένο παράδειγμα:

Καθαρό κείμενο σε μορφή US-ASCII:

```
D4F6A5F5C6123658F78369E5191ED5C9D73CB7AC;400013293980417;20231114100000;100;24;124;124;012
34567
```

Hashed Κείμενο (sha256) σε μορφή HEX:

```
ADB9C55E1D866CE742CDF7A7EA35268E766B5984EAEB5DEF65F76A1DC7631A89
```

Υπογραφή σε μορφή HEX

```
3046022100DC4350AD0ABB451701C9592D07A06EA7FB3DB021786BA72755E41D9452562833022100CE112AF425
2C606862F2CB9FC1AC86FD47D2CC94DFFFFAF6CCD2FD699705E323
```

Η μορφή της υπογραφής του παραδείγματος είναι σε τυποποίηση ASN.1