XML Cryptographic Mechanisms

Τεχνολογιες Διαχειρισης Ασφαλειας (ΤεΔΑ) - ΠΜΣ Προηγμενα Συστηματα Πληροφορικης

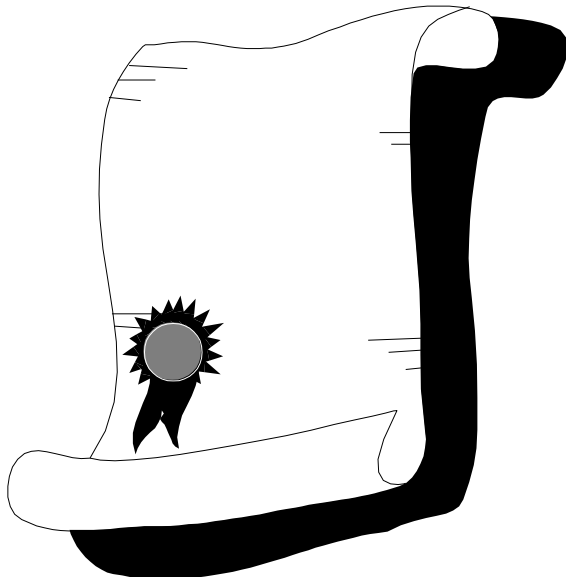
δρ. Καραντζιας Θανος

Περιεχόμενα

- Digital Certificate
- XML Encryption
- XML Digital Signature
- SSL – TLS protocols

Ψηφιακό Πιστοποιητικό

- **Πιστοποιητικό**: ηλεκτρονικό μέσο που διασφαλίζει τη σύνδεση μεταξύ μιας οντότητας και του δημόσιου κλειδιού της
- Είδη Πιστοποιητικών:
  - X.509 Public Key Certificates
    - Identity Certificates
    - S/MIME Certificates
    - Object Signing Certificates
    - SSL Certificates
  - Simple Public Key Infrastructure (SPKI) Certificates



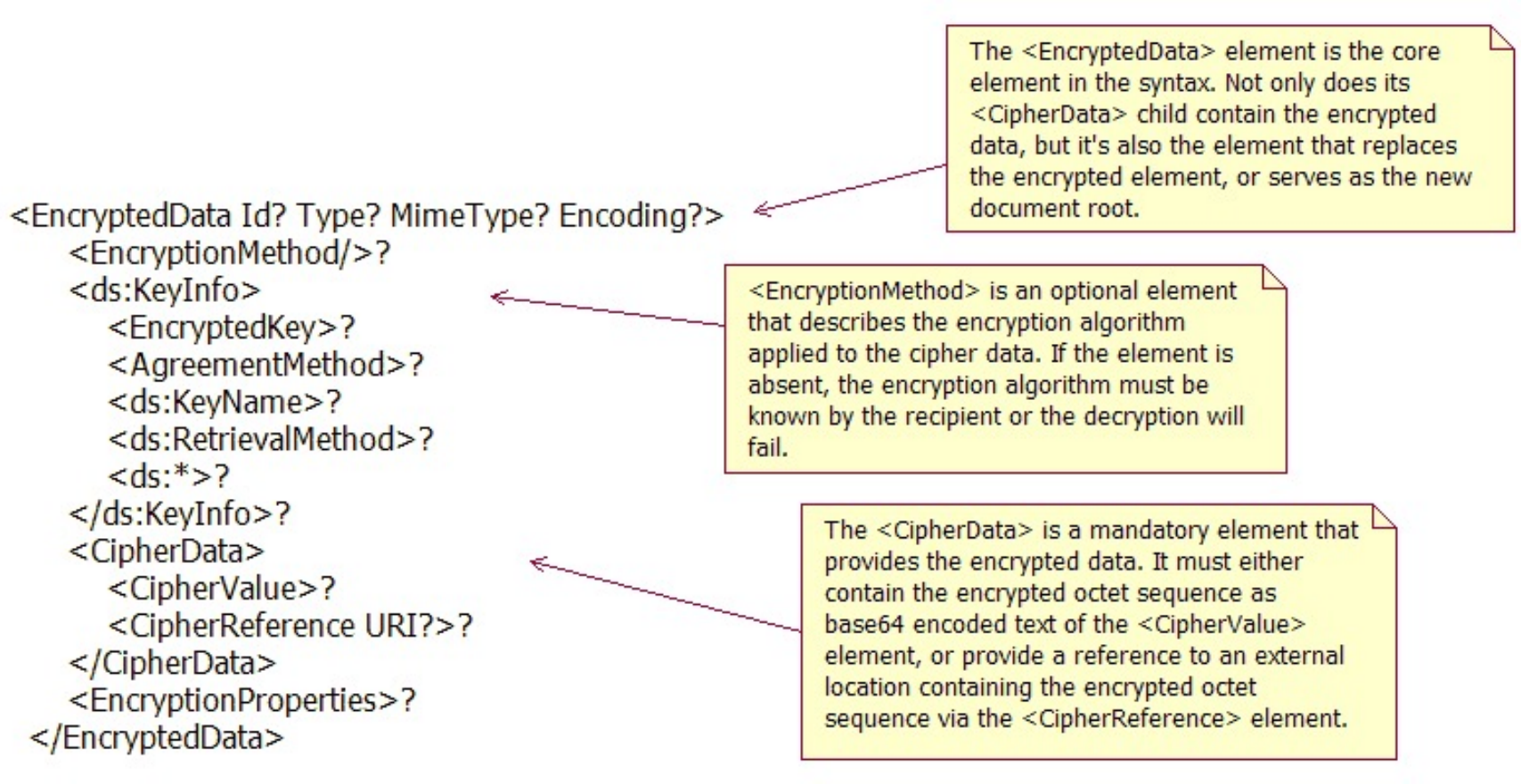
Παράδειγμα X.509

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 2 (0x0)
Signature Algorithm: sha1withRSAEncryption
Issuer: C=GR, SP=ATTIKH, L=Athens, O=Expertnet S.A.,
OU=Security Dept., CN=DemoCA,
Validity
Not Before: Nov 14 17:15:25 2001 GMT
Not After : Dec 14 17:15:25 2001 GMT
Issuer: C=GR, SP=ATTIKH, L=Athens, O=Expertnet S.A.,
OU=Security Dept., CN=Panagiotis D. Sklavos,
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Modulus:
00:9a: …… :8a:67
Exponent: 65537 (0x10001)
Signature Algorithm: sha1withRSAEncryption
0e:28:……70:e3

Plain XML Text

```
<?xml version='1.0'?>

<PaymentInfo xmlns='http://example.org/paymentv2'>
        <Name>John Smith</Name>

        <CreditCard Limit='5,000' Currency='USD'>
                <Number>4019 2445 0277 5567</Number>
                <Issuer>Example Bank</Issuer>
                <Expiration>04/02</Expiration>
        </CreditCard>

</PaymentInfo>
```

Μορφή – Δομή Κρυπτογράφησης



Μορφή - Δομή

- Τα κρυπτογραφημένα δεδομένα περιέχονται στο στοιχείο (element) ***EncryptedData***
- Η δομή του βασίζεται στο σχήμα του ***EncryptedType***
- Το ***EncryptedData*** αποτελείται από τα κρυπτογραφημένα δεδομένα εντός ενός στοιχείου ***CipherData*** (required)
- Το στοιχείο ***CipherData*** μπορεί να αναπαρασταθεί:
  - Να περιέχει το ίδιο το κρυπτογραφημένο κείμενο ως XML (κρυπτογραφημένο σε μορφή base64)
  - Να περιέχει μια *αναφορά (reference)* στο κρυπτογραφημένο αντικείμενο και όχι το ίδιο το αντικείμενο
- Μπορεί να περιλαμβάνει τα στοιχεία ***EncryptionMethod***, ***KeyInfo*** και ***EncryptionProperties*** (optional)
- Το στοιχείο ***EncryptionMethod*** περιέχει τον αλγόριθμο κρυπτογράφησης και το μέγεθος του κλειδιού
- Το στοιχείο ***KeyInfo*** παρέχει την πληροφορία που απαιτείται από την εφαρμογή του παραλήπτη προκειμένου να αποκρυπτογραφήσει τα δεδομένα (Εάν παραλείπεται, αναμένεται από την εφαρμογή να γνωρίζει πώς θα υλοποιήσει την αποκρυπτογράφηση, συμπεριλαμβανομένου της επιλογής του κλειδιού που θα χρησιμοποιήσει)
- Το στοιχείο ***EncryptionProperties*** περιέχει επιπρόσθετες πληροφορίες σχετικές με την διαδικασία

Encrypted Text

ENCRYPT ENTIRE CreditCard ELEMENT

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
        <Name>John Smith</Name>
        <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
                       xmlns='http://www.w3.org/2001/04/xmlenc#'>
              <CipherData>
                    <CipherValue>A23B45C56</CipherValue>
              </CipherData>
         </EncryptedData>
</PaymentInfo>
```

Encrypted Text

ENCRYPT CreditCard ELEMENT CONTENT

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
      <Name>John Smith</Name>
      <CreditCard Limit='5,000' Currency='USD'>
      <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Element'
                     xmlns='http://www.w3.org/2001/04/xmlenc#'>
            <CipherData>
                  <CipherValue>A23B45C56</CipherValue>
            </CipherData>
       </EncryptedData>
</PaymentInfo>
```

Encrypted Text

ENCRYPT ENTIRE XML DOCUMENT

```
<?xml version='1.0'?>
<EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
                        MimeType='text/xml'>
      <CipherData>
            <CipherValue>A23B45C56</CipherValue>
      </CipherData>
</EncryptedData>
```

Encrypted Text

ENCRYPT TWO TIMES

```
<pay:PaymentInfo xmlns:pay='http://example.org/paymentv2'>
        <EncryptedData Id='ED1'
                       xmlns='http://www.w3.org/2001/04/xmlenc#'
                       Type='http://www.w3.org/2001/04/xmlenc#Element'>
                <CipherData>
                        <CipherValue>originalEncryptedData</CipherValue>
                </CipherData>
        </EncryptedData>
</pay:PaymentInfo>
```

```
<pay:PaymentInfo xmlns:pay='http://example.org/paymentv2'>
        <EncryptedData Id='ED2'
                       xmlns='http://www.w3.org/2001/04/xmlenc#'
                       Type='http://www.w3.org/2001/04/xmlenc#Element'>
                <CipherData>
                        <CipherValue>newEncryptedData</CipherValue>
                </CipherData>
        </EncryptedData>
</pay:PaymentInfo>
```

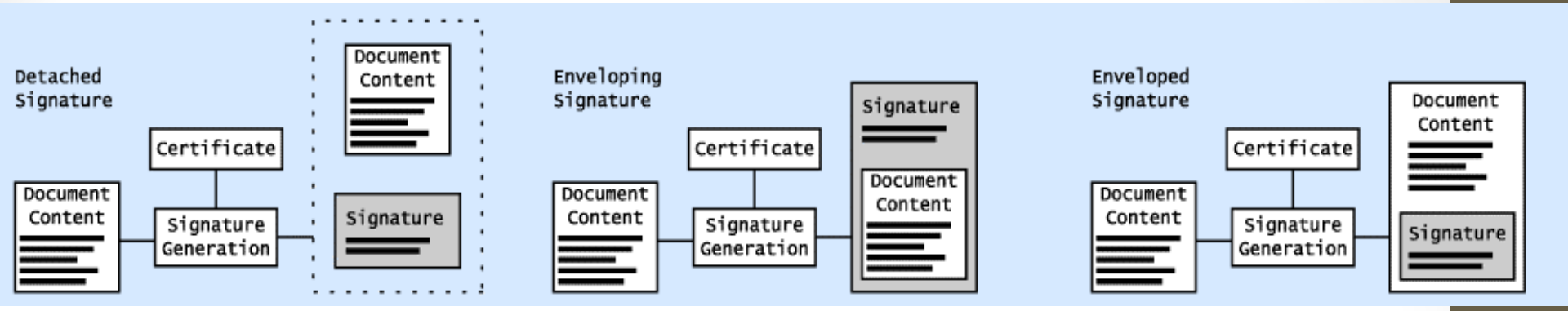
XML Ψηφιακή Υπογραφή

- ***XML Digital Signature (XML-DSig):*** καθορίζει πώς ψηφιακά δεδομένα υπογράφονται και πως το αποτέλεσμα της υπογραφής μπορεί να αναπαρασταθεί σε XML
- Προορίζεται κυρίως για δεδομένα XML, αλλά μπορεί να εφαρμοστεί και γενικότερα με όλες τις μορφές ψηφιακών δεδομένων
- Υπογράφει ένα ολόκληρο έγγραφο XML ή επιλεγμένα κομμάτια του
- Καθορίζει την διαδικασία δημιουργίας και αναπαράσταση μιας υπογραφής XML, καθώς και την επαλήθευση της εγκυρότητάς της
- Βασίζεται σε υπάρχοντες αλγορίθμους
- Μπορεί επίσης να χρησιμοποιηθεί χωρίς πιστοποιητικά
- Κάνει αναφορά σε άλλα πρότυπα για μετασχηματισμούς όπως είναι η *κανονικοποίηση*, η οποία φέρνει τα δεδομένα σε μια πρότυπη μορφή που εξαλείφει οποιεσδήποτε δευτερεύουσες και ασήμαντες διαφορές στην αναπαράσταση και κωδικοποίηση

XML Ψηφιακή Υπογραφή

- Είναι αρκετά πιο πολύπλοκες στην υλοποίηση από την κρυπτογράφηση
- Είναι άρρηκτα δεμένες με την αναπαράσταση των δεδομένων που υπογράφονται
- Η αναπαράσταση των υπογεγραμμένων δεδομένων και των δεδομένων που διαβάζονται προκειμένου να επαληθευτεί η υπογραφή πρέπει να είναι συνεπείς
- Ακόμη και αν υπογραφή ήταν έγκυρη τη στιγμή της δημιουργίας της, υπάρχει το ενδεχόμενο να μη μπορεί να επαληθευτεί στη συνέχεια από τον παραλήπτη, λόγω αλλαγών που συνέβησαν κατά τη μεταφορά ενός μηνύματος

Είδη Ψηφιακών Υπογραφών



- Τρία ισότιμα σχήματα:
  - ***Περικλειόμενες (enveloped) υπογραφές*** - Το έγγραφο παραμένει στην μορφή που ήταν και πριν και μπορεί να υποστεί επεξεργασία
  - ***Περικλείουσες (enveloping) υπογραφές*** - Τα υπογεγραμμένα δεδομένα πρέπει να εξαχθούν πριν γίνει η επεξεργασία τους από μια εφαρμογή.
  - ***Αποσπασμένες (detached) υπογραφές*** - Αυξάνει την πολυπλοκότητα της ενσωμάτωσης της ασφάλειας που προσφέρει στο σύστημα λόγω του ότι πρέπει κάθε στιγμή να μεταφέρονται δύο διαφορετικά αρχεία

Enveloped DSig

```
<doc Id="myID">
      <myElement>
                  ...
      </myElement>

      <Signature> ...
            <Reference URI="#myID"/> ...
      </Signature>
</doc>
```

Enveloping DSig

```
<Signature>
        ...
        <Reference URI="#myRefObjectID">
                        ...
        </Reference>
        <Object Id="myRefObjectID">
                <doc>
                        <myElement>
                                        ...
                        </myElement>
                        ...
                </doc>
        </Object>
</Signature>
```

Detached DSig

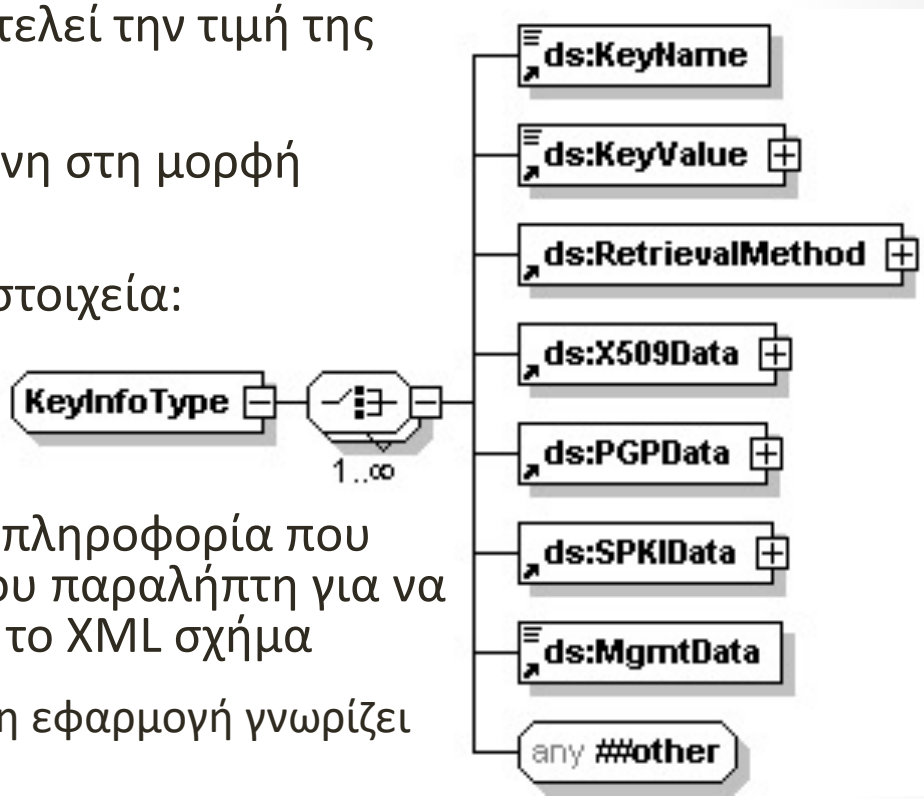
```
<Signature>
                ...
        <Reference URI="http://www.buy.com/books/purchaseWS"/>
                ...
</Signature>
```

Μορφή - Δομή

- Αποτελείται από δυο απαραίτητα στοιχεία XML:
  - Το στοιχείο ***SignedInfo***
  - Το στοιχείο ***SignatureValue***
- Το ***SignedInfo*** περιλαμβάνει το στοιχείο ***CanonicalizationMethod***, που είναι η μέθοδος κανονικοποίησης που θα εφαρμοστεί:
  - Στο ίδιο το στοιχείο ***SignedInfo***
  - Στους αλγορίθμους που χρησιμοποιούνται για την παραγωγή της υπογραφής
  - Σε μια ή περισσότερες αναφορές στα δεδομένα που υπογράφονται
- Κάθε στοιχείο ***Reference*** περιλαμβάνει ένα ***URI*** που αναγνωρίζει:
  - Τα δεδομένα που υπογράφονται
  - Τους μετασχηματισμούς που αυτά υπόκεινται
  - Ένα αναγνωριστικό του αλγορίθμου μετασχηματισμού που θα χρησιμοποιηθεί στα προς μετασχηματισμό δεδομένα
  - Την τιμή του αποτελέσματος της συνάρτησης κατακερματισμού

Μορφή - Δομή

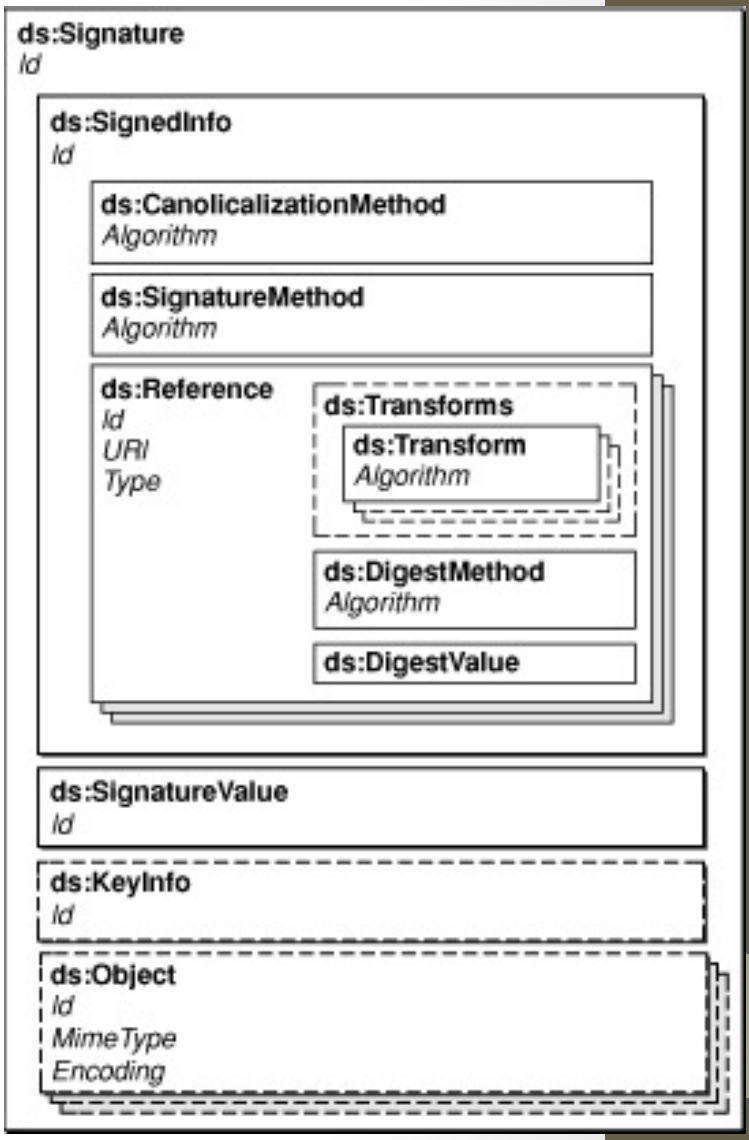
- Το στοιχείο ***SignatureValue*** αποτελεί την τιμή της ψηφιακής υπογραφής
- Η τιμή αυτή είναι κωδικοποιημένη στη μορφή ***base64***
- Υπάρχουν και δυο προαιρετικά στοιχεία:
  - Το στοιχείο ***KeyInfo***
  - Το στοιχείο ***Object***



- Το στοιχείο ***KeyInfo*** παρέχει την πληροφορία που χρειάζεται από την εφαρμογή του παραλήπτη για να επαληθεύσει την υπογραφή και το XML σχήμα
  - Εάν παραληφθεί, θεωρείται ότι η εφαρμογή γνωρίζει τον τρόπο για την επαλήθευση
- Το στοιχείο ***Object*** είναι μια δομή που μπορεί να περιέχει οποιασδήποτε άλλης μορφής πληροφορία για την υποστήριξη της υπογραφής

Μορφή - Δομή

```
<Signature ID?>
        <SignedInfo>
                <CanonicalizationMethod/>
                <SignatureMethod/>
                (<Reference URI? >
                        (<Transforms>)?
                        <DigestMethod>
                        <DigestValue>
                </Reference>)+
        </SignedInfo>
        <SignatureValue>
        (<KeyInfo>)?
        (<Object ID?>)*
</Signature>
```



Digital Signed Text

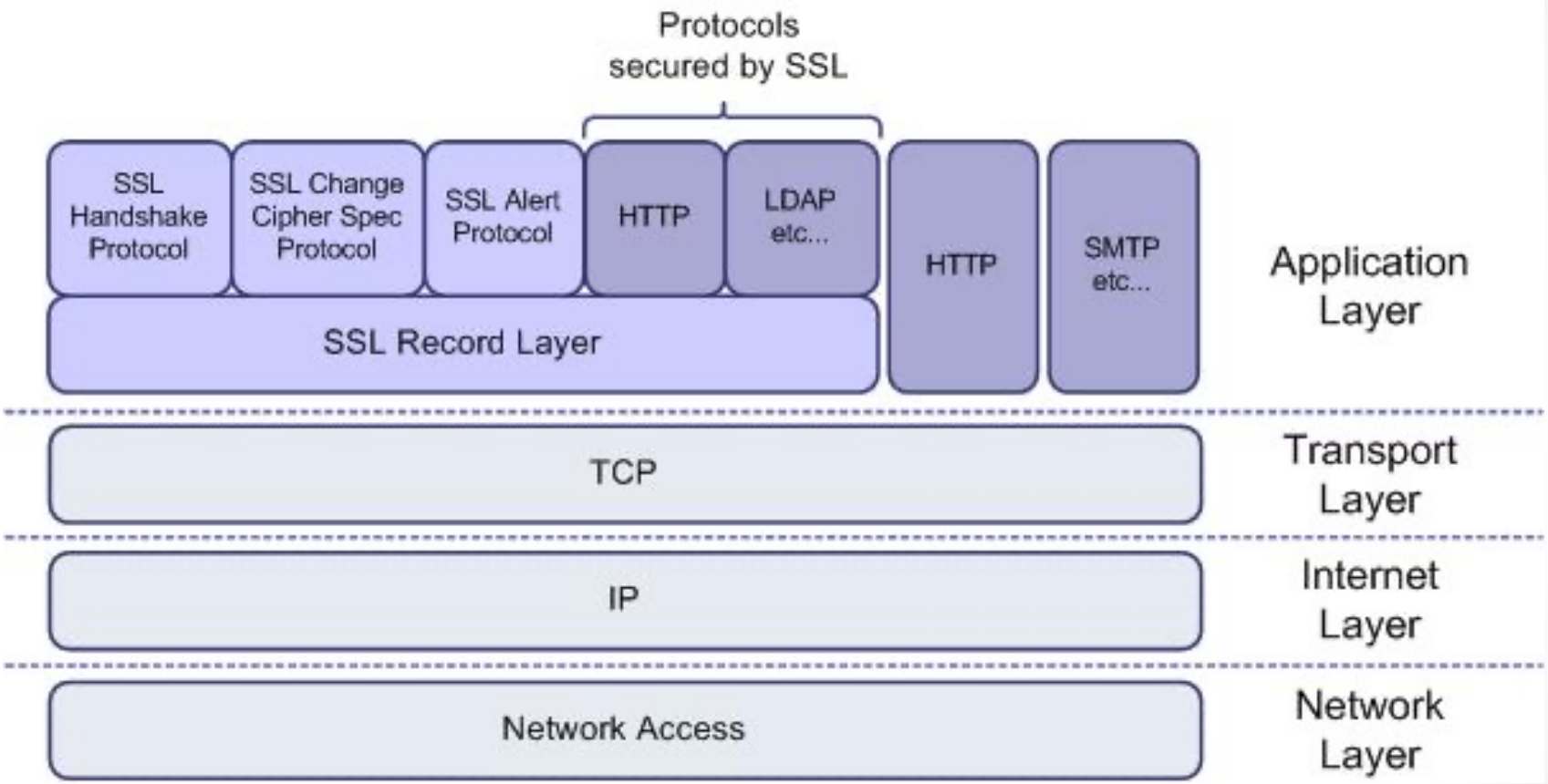
```
<Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
                <CanonicalizationMethod
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                <SignatureMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
                <Reference
        URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
                        <Transforms>
                                <Transform
        Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                                </Transforms>
                        <DigestMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <DigestValue> j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
                </Reference>
        </SignedInfo>
        <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
        <KeyInfo>
                <KeyValue>
                        <DSAKeyValue> <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
                        </DSAKeyValue>
                </KeyValue>
        </KeyInfo>
</Signature>
```

```
- <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  - <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    - <Reference URI="">
      - <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>m1KaNnwzBBRn3hiDhNuQlBw0Leo=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue />
  - <KeyInfo>
    - <KeyValue>
      - <RSAKeyValue>

            <Modulus>g2WWzC+rCLBQ4KZlGLyBu9Yfdh7OunFGVSQ7JvrBT+4/6rBbBr7HuCj1T5aXFO71shOHmoQS1FcddN0lm1Nz
          <Exponent>AQAB</Exponent>
        </RSAKeyValue>
      </KeyValue>
    - <X509Data>
      - <X509IssuerSerial>
          <X509IssuerName>C=DE,O=Fraunhofer Institut FOKUS,CN=SWEB Server CA</X509IssuerName>
          <X509SerialNumber>7685174419968916376</X509SerialNumber>
        </X509IssuerSerial>
        <X509SKI>FOP56rDta0x5jje6F4g+v3GGbjw=</X509SKI>
        <X509SubjectName>C=GR,L=Piraeus,O=University of Piraeus Research
          Centre,T=Server,SERIALNUMBER=sts0000,CN=STS,EMAILADDRESS=muster@musterdomain.com</X509SubjectName>

          <X509Certificate>MIIC+zCCAmSgAwIBAgIIaqc5assqe5gwDQYJKoZIhvcNAQEFBQAwSjEXMBUGA1UEAwwOU1dFQiBTZXJ
      </X509Data>
    </KeyInfo>
  </Signature>
```

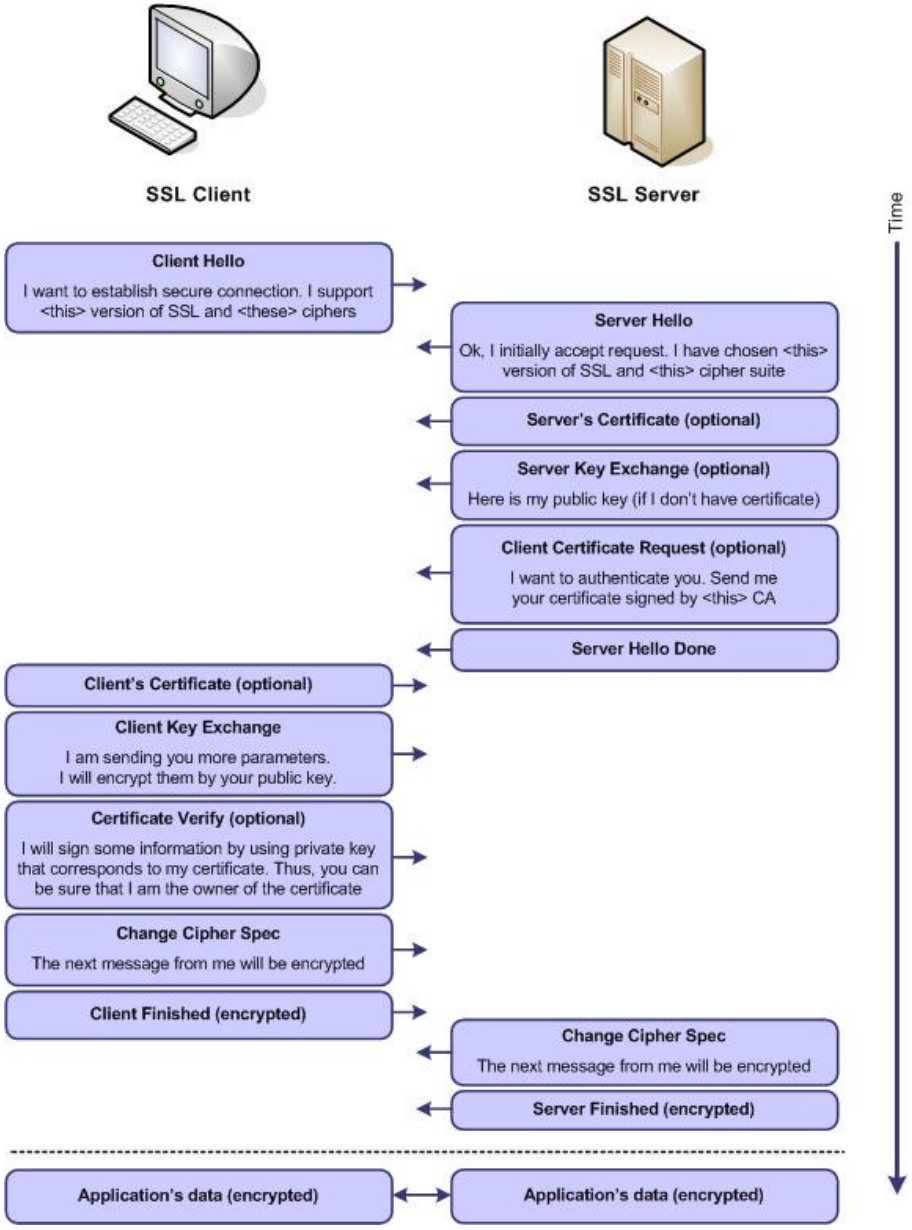
Secure Sockets Layer - SSL

- IP (Internet Protocol): Το πρωτόκολλο που είναι υπεύθυνο για την δρομολόγηση των μηνυμάτων διαμέσου των δικτύων από την πηγή στον προορισμό
- Το TCP (Transmission Control Protocol): Στηρίζεται στις υπηρεσίες του IP και βεβαιώνει ότι η επικοινωνία είναι αξιόπιστη
- HTTP (Hypertext Transfer Protocol): Κατανοεί τις λεπτομέρειες της διεπαφής ανάμεσα στους φυλλομετρητές Ιστού και τους εξυπηρετητές
- Το SSL (Secure Socket Layer) πρωτόκολλο παρουσιάζει τα εξής χαρακτηριστικά:
  - Προσθέτει ένα στρώμα στην αρχιτεκτονική του IP πρωτοκόλλου.
  - Βρίσκεται ανάμεσα στην HTTP εφαρμογή και στο TCP, ενεργώντας σαν ένα ξεχωριστό πρωτόκολλο ασφαλείας.
  - Τρέχει πάνω από το TCP/IP και κάτω από την διεπαφή μεταξύ του στρώματος Δικτύου (Network Layer) και του στρώματος Εφαρμογής (Application Layer)

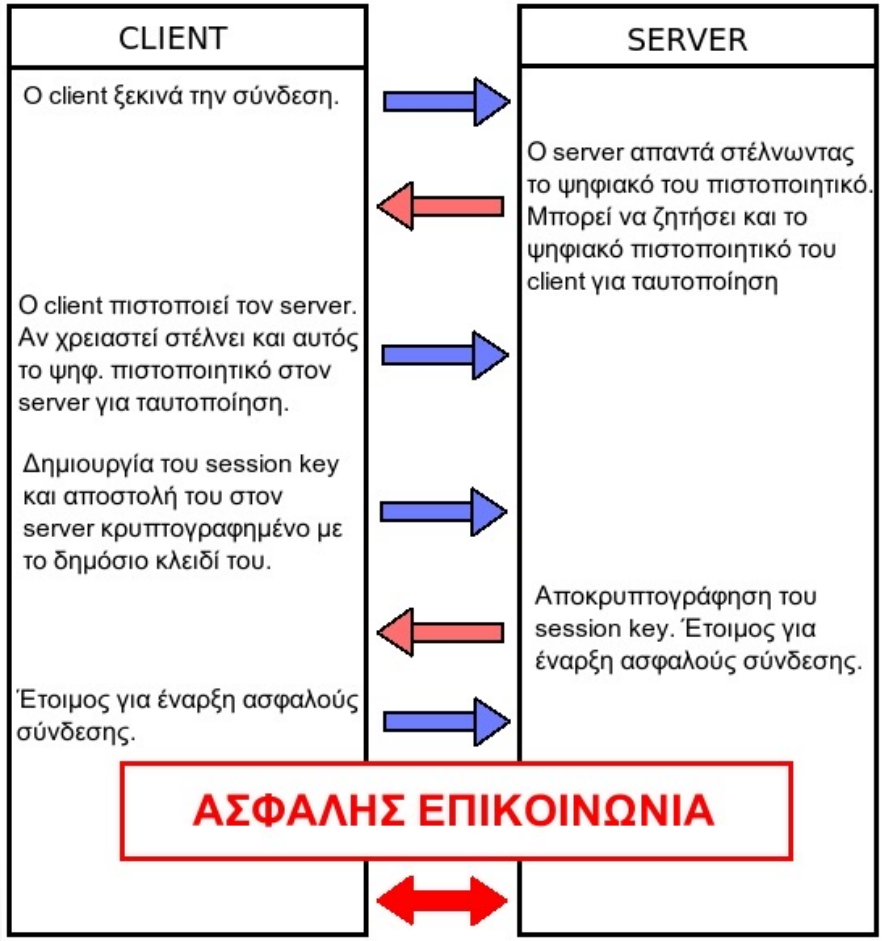
Secure Sockets Layer - SSL

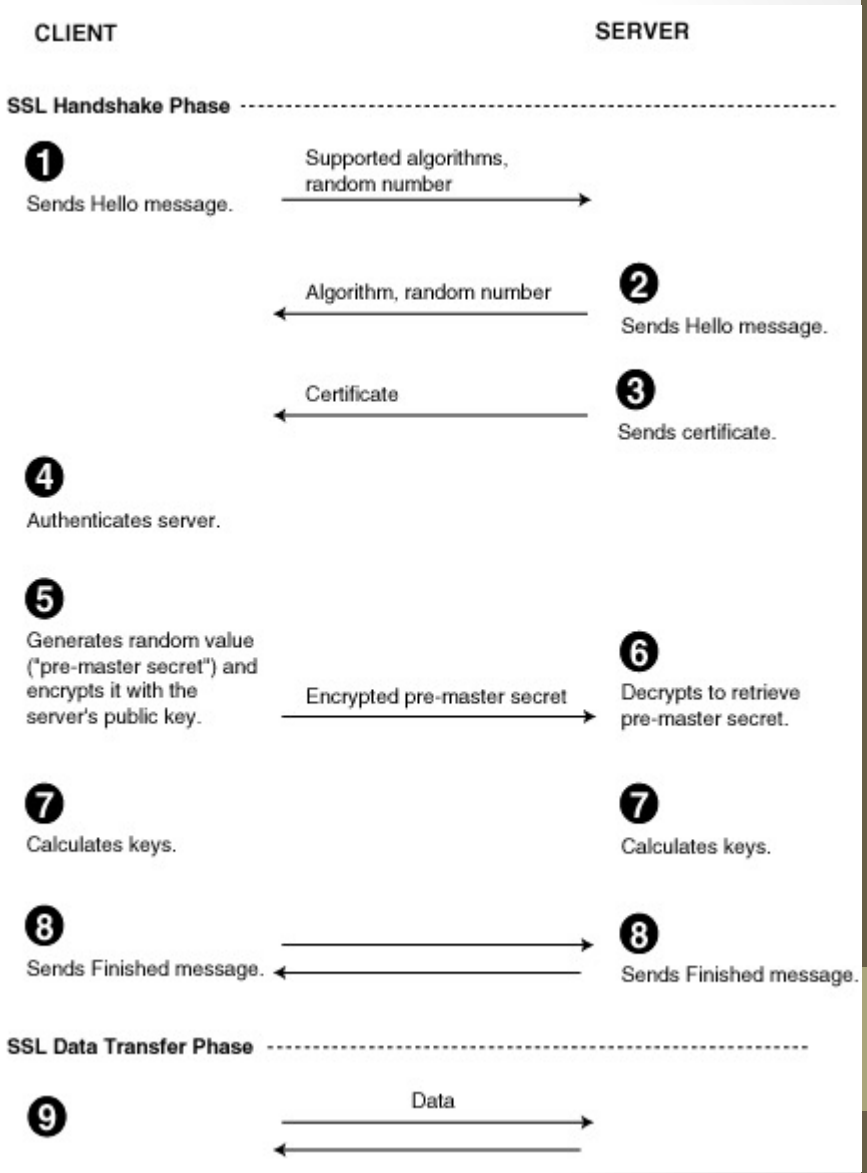


Secure Sockets Layer - SSL



Secure Sockets Layer - SSL





Secure Sockets Layer - SSL

- Το πρωτόκολλο SSL εμπεριέχει δύο υπό-πρωτόκολλα:
  - Το Πρωτόκολλο Καταγραφής SSL (*SSL record protocol*): Καθορίζει τη μορφή με την οποία αναμεταδίδονται τα δεδομένα
  - Το Πρωτόκολλο Χειραψίας SSL (*SSL Handshake protocol*): Χρησιμοποιεί το πρωτόκολλο καταγραφής για την ανταλλαγή μιας σειράς μηνυμάτων μεταξύ του εξυπηρετητή και του πελάτη όταν ο πρώτος δημιουργεί μια σύνδεση SSL μεταξύ τους
- Στόχοι των κρυπτογραφημένων μηνυμάτων είναι:
  - Η αυθεντικοποίηση του εξυπηρετητή στον εξυπηρετούμενο πελάτη.
  - Το να επιτρέπει στον εξυπηρετητή και στον εξυπηρετούμενο να επιλέξουν τον κρυπτογραφικό αλγόριθμο που θα χρησιμοποιήσουν βάσει αυτών που υποστηρίζουν.
  - Η προαιρετική αυθεντικοποίηση του πελάτη στον εξυπηρετητή.
  - Τη χρησιμοποίηση κρυπτογράφησης δημοσίου κλειδιού για την δημιουργία κοινών μυστικών.
  - Τη δημιουργία μιας κρυπτογραφημένης σύνδεσης SSL.

Secure Sockets Layer - SSL

Η ασφάλεια στην επικοινωνία επιτυγχάνεται εφόσον:

- **Το κανάλι είναι ιδιωτικό**: η κρυπτογράφηση χρησιμοποιείται για όλα τα μηνύματα αφότου μια απλή ανταλλαγή μηνυμάτων χρησιμοποιηθεί για να καθορίσει ένα μυστικό κλειδί.
- **Το κανάλι επικυρώνεται**: το σημείο εξυπηρέτησης της συνομιλίας επικυρώνεται πάντα, ενώ το σημείο τέλους πελατών επικυρώνεται προαιρετικά.
- **Το κανάλι είναι αξιόπιστο**: η μεταφορά μηνυμάτων περιλαμβάνει έναν έλεγχο ακεραιότητας μηνυμάτων (που χρησιμοποιεί έναν MAC).

Οι αλγόριθμοι που χρησιμοποιούνται:

- DES, DSA, KEA, MD5, RC2 & RC4, RSA, SHA-1, SKIPJACK, Triple DES

Ευχαριστώ
για την προσοχή σας!!

Επικοινωνία: karant@unipi.gr

Ενημέρωση: http://athina.cs.unipi.gr/site-ergastirio/asfaleia/index.html