**Άσκηση**

Θεωρήστε ότι ο διευθυντής ενός μεγάλου οργανισμού θέλει να στείλει στους υπαλλήλους του ένα έγγραφο, το οποίο είναι χωρισμένο σε τμήματα, σε καθένα από τα οποία θα πρέπει να κάνει τροποποιήσεις διαφορετικός υπάλληλος, με βάση τα καθήκοντά του. Καθώς πρόκειται για ευαίσθητο έγγραφο, ο διευθυντής δεν επιθυμεί ο κάθε υπάλληλος να έχει πλήρη εικόνα του, παρά μόνο αυτά που πρέπει να γνωρίζει προκειμένου να κάνει τις απαραίτητες τροποποιήσεις. Στο τέλος αυτής της διαδικασίας, ο κάθε υπάλληλος θα πρέπει να στείλει το έγγραφο πίσω με τις τροποποιήσεις του, επιτρέποντας στο διευθυντή του να επιβεβαιώσει την αυθεντικότητα των τροποποιήσεων.
Περιγράψτε τη διαδικασία που πρέπει να ακολουθηθεί τόσο από το διευθυντή όσο και από τον κάθε υπάλληλο.

**Απάντηση**

Για να εξασφαλίσει ο διευθυντής ότι κάθε υπάλληλός του θα έχει πρόσβαση μόνο σε συγκεκριμένο τμήμα του εγγράφου, θα πρέπει να κρυπτογραφήσει το κάθε τμήμα του με κάποιο κλειδί, ώστε να μπορεί να το αποκρυπτογραφήσει μόνο ο αντίστοιχος υπάλληλος. Καθώς μιλάμε για ένα μεγάλο οργανισμό, θα ήταν ασύμφορο να ακολουθήσουμε ένα σχήμα συμμετρικής κρυπτογραφίας, αφού κάτι τέτοιο θα προαπαιτούσε τη συμφωνία με κάθε υπάλληλο ξεχωριστά για συμμετρικά κλειδιά. Συνεπώς, προτιμάμε τη χρήση ασύμμετρης κρυπτογραφίας.

Βήμα 1
Για να περιορίσει την πρόσβαση κάθε τμήματος του εγγράφου ανά υπάλληλο, ο διευθυντής θα επιλέξει να το κρυτπογραφήσει με το αντίστοιχο δημόσιο κλειδί του καθένα. Με αυτό τον τρόπο εξασφαλίζει ότι μόνο ο κάτοχος του ιδιωτικού κλειδιού (δηλαδή ο κάθε υπάλληλος ξεχωριστά, αφού το ιδιωτικό κλειδί το γνωρίζει μόνο ο κάτοχός του) θα μπορεί να επέμβει στο αντίστοιχο τμήμα του εγγράφου. Έτσι, ο διευθυντής θα κρυπτογραφήσει το κάθε τμήμα που θέλει να προστατέψει με το αντίστοιχο δημόσιο κλειδί του υπαλλήλου στον οποίο θέλει να δώσει πρόσβαση.

Βήμα 2
Στη συνέχεια, θα πρέπει να υπογράψει ψηφιακά το έγγραφο που στέλνει, ώστε οι υπάλληλοι να γνωρίζουν ότι το έγγραφο είναι έγκυρο και στέλνεται όντως από το διευθυντή τους και όχι από κάποιον που προσπαθεί να τους ξεγελάσει για να αποσπάσει πληροφορία. Έτσι, ο διευθυντής θα εφαρμόσει μια συνάρτηση σύνοψης στο έγγραφο και το αποτέλεσμα θα το κρυπτογραφήσει με το ιδιωτικό του κλειδί. Τέλος, επισυνάπτει το κρυπτογράφημα (ψηφιακή υπογραφή) στο έγγραφο που αποστέλει.

Βήμα 3
Κάθε υπάλληλος που παραλαμβάνει το έγγραφο πρώτα επιβεβαιώνει την ψηφιακή υπογραφή. Η διαδικασία που ακολουθεί είναι η εξής:

1. Αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του διευθυντή.
2. Εφαρμόζει τη συνατηση σύνοψης στο υπογεγραμμένο έγγραφο.
3. Συγκρίνει τα αποτελέσματα των δύο προηγούμενων βημάτων. Αν είναι ίδια, τότε έχει επιβεβαιωθεί η γνησιότητα του εγγράφου.

Βήμα 4
Κατόπιν αυτού, ο κάθε υπάλληλος θα αποκρυπτογραφήσει το τμήμα του εγγράφου για το οποίο είναι υπεύθυνος (ο προσδιορισμός αυτού του τμήματος είναι ανεξάρτητος από τις τεχνολογίες ασφάλειας και μπορεί να βασίζεται σε πρότυπα όπως το xml encryption – xenc), θα κάνει τις τροποποιήσεις που χρειάζονται και, στη συνέχεια, θα το κρυπτογραφήσει με το δημόσιο κλειδί του διευθυντή του, ώστε

μόνο ο τελευταίος να είναι σε θέση να το αποκρυπτογραφήσει. Τέλος, με τρόπο αντίστοιχο με το Βήμα 2, ο υπάλληλος θα υπογράψει ψηφιακά το έγγραφο που αποστέλλει στο διευθυντή του.

Βήμα 5
Κάθε μήνυμα που θα λαμβάνει ως απάντηση ο διευθυντής, θα το επιβεβαιώνει ως προς την αυθεντικότητά του κάνοντας χρήση της ψηφιακής υπογραφής (σε αντιστοιχία με το Βήμα 3) και στη συνέχεια θα αποκρυπτογραφεί το τμήμα για το οποίο είναι υπεύθυνος ο αποστολέας κάνοντας χρήση του ιδιωτικού του κλειδιού.