Παράρτημα Α – Περισσότερα για την Ασφάλεια στο Διαδίκτυο

Α.1 Κρυπτογράφηση Δημόσιου Κλειδιού

Όπως αναφέρθηκε στην παράγραφο 2.3.2, η πιο διαδεδομένη μέθοδος κρυπτογραφίας στο Διαδίκτυο είναι η κρυπτογράφηση με ασυμμετρικό αλγόριθμο, ή αλλιώς Κρυπτογράφηση Δημόσιου Κλειδιού.

Μέσω αυτής λύνεται το παράδοξο της συμμετρικής κρυπτογράφησης ότι αφενός για να υπάρχει ασφαλής επικοινωνία χρειάζεται κρυπτογράφηση, αφετέρου για να είναι ασφαλής η αποστολή του κλειδιού κρυπτογράφησης (στην περίπτωση συμμετρικού αλγόριθμου) στους επιθυμητούς αποδέκτες, χρειάζεται ασφαλής επικοινωνία.

Το σύστημα κρυπτογράφησης δημόσιου κλειδιού είναι εκείνο στο οποίο τα μηνύματα που έχουν κρυπτογραφηθεί με ένα δημόσιο κλειδί, μπορούν να αποκρυπτογραφηθούν μόνο με ένα αντίστοιχο –δεύτερο- ιδιωτικό κλειδί και αντίστροφα. Ένα ισχυρό σύστημα κρυπτογράφησης δημόσιου κλειδιού είναι εκείνο στο οποίο η κατοχή του αλγόριθμου και του δημόσιου κλειδιού δεν δίνει καμία χρήσιμη πληροφορία σε σχέση με το ιδιωτικό κλειδί, άρα και δεν αρκεί για την αποκρυπτογράφηση του μηνύματος.

Το σύστημα παίρνει το όνομά του από το ότι ο χρήστης δημοσιοποιεί το ένα κλειδί, αλλά κρατά το άλλο κρυφό. Ο καθένας μπορεί να χρησιμοποιήσει το δημόσιο κλειδί για να στείλει μηνύματα που μπορεί να διαβάσει μόνο ο κάτοχος του (μυστικού) ιδιωτικού κλειδιού. Αντίστροφα, ο κάτοχος του ιδιωτικού κλειδιού το χρησιμοποιεί για να στείλει μηνύματα που μόνο αυτός μπορεί να έχει στείλει.
Με τη βοήθεια της κρυπτογράφησης δημόσιου κλειδιού είναι δυνατό να εγκατασταθεί μια ασφαλής γραμμή επικοινωνίας μεταξύ χρηστών που χρησιμοποιούν ένα συμβατό πρόγραμμα αποκρυπτογράφησης ή αντίστοιχο ειδικό εξοπλισμό. Ο αποστολέας και ο παραλήπτης δε χρειάζονται πια ένα ασφαλές κανάλι επικοινωνίας και ένα συμφωνημένο κοινό κλειδί, όπως στην κρυπτογράφηση μοναδικού κλειδιού.

Αν η Α θέλει να επικοινωνήσει με τον Β, ένα ξένο με τον οποίο ποτέ δεν έχει επικοινωνήσει ξανά, η Α και ο Β μπορούν αρχικά να ανταλλάξουν τα δημόσια κλειδιά τους, χωρίς να απαιτείται ασφαλής σύνδεση. Μετά, ο καθένας από τους δύο θα κρυπτογραφεί τα μηνύματα που θέλει να στείλει με το δημόσιο κλειδί του άλλου και θα τα στέλνει, και πάλι χωρίς ανάγκη ασφαλούς σύνδεσης. Τέλος, ο καθένας θα αποκρυπτογραφεί τα μηνύματα που λαμβάνει με το δικό του ιδιωτικό κλειδί. Η ασφάλεια του συστήματος δεν κινδυνεύει, όσο τα ιδιωτικά κλειδιά δεν διαρρέουν σε τρίτους.

Η Α, εφόσον έχει το δημόσιο κλειδί του Β και ξέρει ότι είναι πραγματικά το δικό του, μπορεί να το χρησιμοποιεί ώστε να ξέρει ότι μόνο ο Β, και όχι κάποιος τρίτος που ισχυρίζεται ότι είναι ο Β, θα μπορεί να αποκρυπτογραφήσει τα μηνύματά της.

Το πρόβλημα που αντιμετωπίζει η Α είναι ότι, λαμβάνοντας το αρχικό μήνυμα από τον Β όπου εκείνος της γνωστοποιεί το δημόσιο κλειδί του, δεν γνωρίζει αν πρόκειται πραγματικά για τον Β ή κάποιον κακόπιστο τρίτο που της δίνει το δικό του δημόσιο κλειδί δηλώνοντας ότι είναι ο Β (το ίδιο ακριβώς πρόβλημα θα αντιμετωπίσει και ο Β ως προς την Α). Κάποιος κακόπιστος Κ μπορεί να στείλει στην Α το δικό του δημόσιο κλειδί δηλώνοντας ότι είναι ο Β και η Α δεν έχει τρόπο να γνωρίζει αν ο άλλος (και το δημόσιο κλειδί του) είναι πραγματικά ο Β ή κάποιος άλλος. Ο μοναδικός τρόπος εξασφάλισης της πραγματικής ταυτότητας του άλλου μέρους είναι μια φυσική επικοινωνία εκτός δικτύου ή η επιβεβαίωση από κάποια τρίτη πηγή (μια Έμπιστη Τρίτη Οντότητα). Βέβαια, αν η Α και ο Β ήδη γνωρίζονται, το ίδιο το μήνυμα μπορεί να αποδεικνύει την ταυτότητα του αποστολέα, αναφέροντας στοιχεία ή γεγονότα γνωστά και στους δύο.

Μια ανεξάρτητη βάση δεδομένων δημόσιων κλειδιών δεν λύνει το πρόβλημα αν δεν πιστοποιεί και την ακρίβεια της πληροφορίας που παρέχει. Ας υποθέσουμε ότι η Γ διατηρεί μια δικτυακή βάση με ονόματα, ηλεκτρονικές διευθύνσεις και δημόσια κλειδιά. Η Γ επιτρέπει σε όλους να καταχωρηθούν στη βάση της χωρίς χρέωση και χωρίς εκείνη να ελέγχει την ακρίβεια των δεδομένων που καταχωρούνται. Έτσι, ο κακόπιστος Κ μπορεί να δημιουργήσει μια καταχώρηση με τα στοιχεία του Β αλλά το δικό του δημόσιο κλειδί. Η Α δεν έχει τρόπο να

γνωρίζει αν η καταχώρηση που βλέπει στη βάση με τα στοιχεία του Β έγινε πραγματικά από τον Β ή από τον Κ και αν το δημόσιο κλειδί που βλέπει αντιστοιχεί στον Β ή στον Κ. Είναι φανερό ότι μια τέτοια βάση δεδομένων δεν είναι σε θέση να προσφέρει ουσιαστική πιστοποίηση. Το πρόβλημα αυτό λύνεται με την ύπαρξη εγκεκριμένων Φορέων Πιστοποίησης, που αναλαμβάνουν –εκτός από την τήρηση των σχετικών βάσεων δεδομένων- και την εξακρίβωση των στοιχείων που είναι καταχωρημένα σε αυτές.

Α.2 Ψηφιακά Πιστοποιητικά

Πιστοποιητικό είναι μια ψηφιακά υπογεγραμμένη βεβαίωση από έναν Φορέα Πιστοποίησης που παρέχει ανεξάρτητη διαβεβαίωση για μια σειρά από ιδιότητες ενός προσώπου, που εμφανίζονται στην ψηφιακή υπογραφή ενός εγγράφου. Η ηλεκτρονική υπογραφή ενός προσώπου μπορεί να είναι ένα τέτοιο πιστοποιητικό.

Πιο αναλυτικά, ένα πιστοποιητικό είναι μια ηλεκτρονική εγγραφή η οποία:

1. Προσδιορίζει τον ΦΠ που το εκδίδει
2. Αναφέρει ή περιγράφει μια ή περισσότερες ιδιότητες του συνδρομητή
3. Περιλαμβάνει το δημόσιο κλειδί του συνδρομητή
4. Είναι ψηφιακά υπογεγραμμένη από τον ΦΠ που το εκδίδει

Τυπικά, η παροχή τέτοιων πιστοποιητικών δεν είναι απαραίτητο να συνοδεύεται από περιγραφή του βαθμού ελέγχου που διεξήχθη προκειμένου να ελεγχθεί η ακρίβεια των δεδομένων που πιστοποιούνται. Παρ' όλ' αυτά, η έλλειψη καταγεγραμμένων διαδικασιών ελέγχου της ακρίβειας των δεδομένων από τους φορείς πιστοποίησης, μειώνει σαφώς το κύρος των τελευταίων.

Πρακτικά, οι ΦΠ παρέχουν πιστοποιητικά διαφόρων βαθμίδων, ανάλογα με το επίπεδο ελέγχου που προηγήθηκε προκειμένου να επιβεβαιωθεί η ορθότητα των πιστοποιούμενων ιδιοτήτων. Για παράδειγμα, η VeriSign, μια από τις πρώτες εταιρίες που ασχολήθηκαν με την έκδοση πιστοποιητικών ταυτοποίησης προτείνει τέσσερις διαφορετικές βαθμίδες πιστοποιητικών:

1. Πιστοποιητικά πρώτης βαθμίδας, που προορίζονται μόνο για απλή πλοήγηση στο Διαδίκτυο και ασφαλές ηλεκτρονικό ταχυδρομείο, ενώ πιστοποιούν μόνο τη μοναδικότητα του ονόματος ή της ηλεκτρονικής διεύθυνσης. Για την έκδοση τους αρκεί μια αίτηση του ενδιαφερόμενου με συμπλήρωση των στοιχείων του μέσω ηλεκτρονικού ταχυδρομείου.
2. Η δεύτερη βαθμίδα απαιτεί το όνομα, η διεύθυνση και άλλα προσωπικά στοιχεία να αποδεικνύονται και με σχετικά έγγραφα, πχ με αποστολή μιας φωτοτυπίας της αστυνομικής ταυτότητας.
3. Για την έκδοση πιστοποιητικού τρίτης βαθμίδας απαιτείται επιπλέον προσωπική παρουσία του ενδιαφερόμενου στα γραφεία του φορέα πιστοποίησης.
4. Τέλος, το πιστοποιητικό τέταρτης βαθμίδας εκδίδεται μετά από εις βάθος έρευνα.

Ανάλογα με τη βαθμίδα του πιστοποιητικού, αυξάνει και το κόστος έκδοσης.

Η ηλεκτρονική υπογραφή είναι ένα από τα διαθέσιμα είδη πιστοποιητικών. Ανάλογα με το περιεχόμενο, οι ΦΠ εκδίδουν επίσης πιστοποιητικά εξουσιοδότησης, συναλλαγών και «σφραγίδες χρονοσήμανσης».

Α.2.1 Πιστοποιητικά Ταυτοποίησης

Ένα Πιστοποιητικό Ταυτοποίησης, συνδέει ένα όνομα με ένα δημόσιο κλειδί. Ο έλεγχος από το ΦΠ ότι το όνομα αντιστοιχεί σε ένα υπαρκτό πρόσωπο συσχετίζει το όνομα με μια ταυτότητα. Η προσεκτική και ακριβής ταυτοποίηση είναι αντικείμενο σοβαρό και σημαντικό: Το κόστος ταυτοποίησης όλων των κατόχων Κάρτας Κοινωνικής Ασφάλισης των ΗΠΑ θα ξεπερνούσε το 1,5 δισ δολάρια.

Πέρα από την αποθήκευση των πιστοποιητικών ταυτοποίησης σε υπολογιστές συνδεδεμένους με το Διαδίκτυο, αυτά θα μπορούσαν να περιλαμβάνονται και σε προσωπικές κάρτες για χρήση σε υπηρεσίες ή στη διεξαγωγή τραπεζικών ή εμπορικών συναλλαγών.

Ο ΦΠ, προκειμένου να εκδώσει ένα πιστοποιητικό για να βεβαιώσει ότι ένα δημόσιο κλειδί ανήκει σε ένα πρόσωπο, παράγει ένα ηλεκτρονικό μήνυμα που περιλαμβάνει το όνομα του προσώπου, μια βεβαίωση -ανάλογα με το επίπεδο ελέγχου που έγινε- ότι το πρόσωπο είναι όντως αυτό και, τέλος, το δημόσιο

κλειδί του. Ο ΦΠ υπογράφει το μήνυμα με το δικό του δημόσιο κλειδί. Το τι συμβαίνει μετά εξαρτάται από τις υπηρεσίες που προσφέρει ο ίδιος ο ΦΠ. Το πιστοποιητικό μπορεί να είναι διαθέσιμο δημόσια σε μια ιστοσελίδα, προσβάσιμο από όλους τους ενδιαφερόμενους, ή μπορεί να παραδοθεί στον ενδιαφερόμενο, ή μπορεί ακόμη και να συμφωνηθεί ότι ο ΦΠ θα παρέχει αντίγραφο του πιστοποιητικού σε όλους όσους το ζητήσουν. Φυσικά, οι διαθέσιμες επιλογές σχετίζονται και με το νομικό καθεστώς στο οποίο υπόκειται ο ΦΠ.

Ο κίνδυνος ότι οι πληροφορίες που δίνει το πιστοποιητικό δεν είναι πλέον ακριβείς μπορεί να μειωθεί, αλλά όχι να εξαλειφθεί. Θα πρέπει τα πιστοποιητικά να περιλαμβάνουν ημερομηνία έκδοσης και να έχουν συγκεκριμένη διάρκεια ισχύος ή να απαιτούν περιοδική επιβεβαίωση από την ΑΠ και περιοδικό έλεγχο από το χρήστη των «πινάκων ανάκλησης πιστοποιητικών» που δημοσιοποιεί η ΑΠ με τα πιστοποιητικά που δεν ισχύουν πλέον.

Από τη στιγμή που δεν υπάρχει κάποιο άλλο σύστημα ή διαδικασία που να ορίζει ποιος θα ελέγχει κάθε μέρα και θα βεβαιώνει ότι τα στοιχεία των πιστοποιητικών εξακολουθούν να είναι ακριβή, κάθε χρήστης, πέρα από το συστηματικό έλεγχο των πινάκων ανάκλησης, πρέπει να γνωρίζει ότι πάντα εκτίθεται σε κάποιο μεγαλύτερο ή μικρότερο κίνδυνο. Αν θέλει να μειώσει αυτόν τον κίνδυνο, μπορεί να αποφασίσει ότι θα δέχεται μόνο πιστοποιητικά με γνωστή ημερομηνία έκδοσης και σχετικά πρόσφατα (όσο πιο πρόσφατα έχουν εκδοθεί, τόσο μειώνεται ο κίνδυνος). Μπορεί επίσης να αποφασίσει ποιων εταιριών ΑΠ τα πιστοποιητικά θα εμπιστεύεται και ποιων όχι. Τέλος, μπορεί να κρίνει με βάση το επίπεδο ελέγχου π.χ. να δέχεται μόνο πιστοποιητικά δεύτερης και πάνω βαθμίδας και να απορρίπτει εκείνα της πρώτης βαθμίδας.

Σε κάθε περίπτωση ο κίνδυνος, όσο και αν μειώνεται, είναι πάντα υπαρκτός, όπως συμβαίνει και σε κάθε παραδοσιακή - φυσική συναλλαγή, αφού άλλωστε η πλαστογραφία ανακαλύφθηκε πολύ νωρίτερα από το διαδύκτυο.

Α.2.2 Πιστοποιητικά Εξουσιοδότησης

Αν και τα πιστοποιητικά ταυτοποίησης είναι μάλλον τα πιο δημοφιλή αυτή τη στιγμή, μεσοπρόθεσμα οι ΦΠ αναμένεται να πιστοποιούν περισσότερο ιδιότητες παρά ταυτότητα. Ένα Πιστοποιητικό Εξουσιοδότησης μπορεί να βεβαιώνει που μένει ο συνδρομητής, ποια είναι η ηλικία του, ότι ανήκει σε κάποια οργάνωση, ότι καταναλώνει συστηματικά ένα προϊόν κλπ. Τέτοια πιστοποιητικά μπορεί να χρησιμοποιηθούν με πολλούς διαφορετικούς τρόπους.

Ένα πιστοποιητικό που συνδέει τον τόπο κατοικίας, την ηλικία ή άλλη ιδιότητα με το δημόσιο κλειδί μπορεί να περιλαμβάνει και το όνομα του κατόχου. Δεν είναι όμως απαραίτητο, το ίδιο το κλειδί είναι αρκετό, φτάνει να είναι αρκετά μεγάλο ώστε να είναι μοναδικό και αν έχει παραχθεί με ασφαλή τρόπο. Ανώνυμα πιστοποιητικά εξυπηρετούν ιδιαίτερα σε κάποιες συγκεκριμένες διαδικτυακές συναλλαγές. Για παράδειγμα η είσοδος σε ιστοσελίδες με ενήλικο περιεχόμενο μπορεί να απαιτεί πιστοποιητικό ηλικίας άνω των 18 ετών, αλλά οι χρήστες δεν θα ήθελαν να δηλώσουν το όνομά τους. Επίσης, τράπεζες θα μπορούσαν να χορηγούν πιστοποιητικά που συνδέουν απλά ένα λογαριασμό με ένα κλειδί, χωρίς να εμφανίζεται το όνομα του δικαιούχου.

Α.2.3 Πιστοποιητικά Συναλλαγών

Τα Πιστοποιητικά Συναλλαγών επικυρώνουν δεδομένα συναλλαγών. Σε αντίθεση με τα πιστοποιητικά Ταυτοποίησης ή Εξουσιοδότησης, αυτά δεν προορίζονται για πολλές χρήσεις ή για τη σύνδεση δεδομένου με κλειδί. Αντίθετα, επικυρώνουν ότι κάποιο γεγονός ή διατύπωση βεβαιώνεται από κάποιον τρίτο παρατηρητή. Για παράδειγμα, μπορεί ένας συμβολαιογράφος να εκδώσει ένα τέτοιο πιστοποιητικό βεβαιώνοντας ότι ο πελάτης του υπέγραψε ψηφιακά ένα ψηφιακό συμβόλαιο. Το πιστοποιητικό μπορεί να περιλαμβάνει το κείμενο του συμβολαίου, την ψηφιακή υπογραφή του πελάτη, το δημόσιο κλειδί του πελάτη, και όλα αυτά να είναι υπογεγραμμένα με το μυστικό κλειδί του συμβολαιογράφου.

Από τεχνικής σκοπιάς, η διαφορά του πιστοποιητικού συναλλαγής με ένα απλό ηλεκτρονικό κείμενο ψηφιακά υπογεγραμμένο με το δημόσιο κλειδί της ΑΠ είναι μάλλον μικρή. Η διαφοροποίηση είναι περισσότερο νομική παρά τεχνική.

Οι νομικές διαφορές είναι αρκετές:

- Πρώτον, η ενσωμάτωση της ψηφιακής υπογραφής κατά κάποιο τρόπο προσθέτει επισημότητα και εγκυρότητα.
- Δεύτερον, ένα τέτοιο πιστοποιητικό τυπικά περιλαμβάνει δέσμευση της ΑΠ σε σχέση με το επίπεδο ελέγχου που έχει διενεργήσει, σε αντίθεση με μια απλή ψηφιακή υπογραφή που δεν προσθέτει περιεχόμενο στο υπογραφόμενο κείμενο.
- Τρίτον, η ΑΠ μπορεί να ενσωματώσει στο υπογραφόμενο έγγραφο επιπλέον πληροφορίες, όπως μια ασφαλή σφραγίδα χρονοσήμανσης από μια αξιόπιστη πηγή παροχής σχετικών υπηρεσιών.
- Τέταρτον, η ΑΠ εκδίδοντας ένα πιστοποιητικό συναλλαγής υπάγεται σε ένα εντελώς διαφορετικό καθεστώς ευθύνης σε σχέση με την έκδοση ενός πιστοποιητικού ταυτοποίησης.
- Το πιστοποιητικό συναλλαγής έχει από τη φύση του ένα μοναδικό και πολύ συγκεκριμένο σκοπό.
- Από τη στιγμή που ένας απεριόριστος και άγνωστος αριθμός τρίτων προσώπων μπορεί να στηριχτούν σε αυτό, η εμπιστοσύνη τους είναι σε μεγάλο βαθμό ή και απόλυτα εξαρτώμενη από την ΑΠ.

Α.2.4 Ψηφιακή Σφραγίδα Χρόνου

Η σφραγίδα χρονοσήμανσης είναι μια κρυπτογραφική ψηφιακή απόδειξη, που δεν μπορεί να πλαστογραφηθεί και που βεβαιώνει ότι το έγγραφο που την περιλαμβάνει δημιουργήθηκε σε δεδομένη χρονική στιγμή.

Είναι σχετικά απλό να αποδείξει κανείς ότι το έγγραφο γράφτηκε μετά από μια συγκεκριμένη ημερομηνία, αν το συνδέσει με κάποιο γεγονός που δεν είχε συμβεί πριν από αυτήν και δεν μπορούσε να προβλεφθεί. Αν για παράδειγμα το κείμενο περιλάμβανε μια αναφορά σε κάποιο άρθρο εφημερίδας συγκεκριμένης μέρας, αυτό θα αποδείκνυε ότι το κείμενο δεν θα μπορούσε να έχει γραφτεί πριν την κυκλοφορία της εφημερίδας. Αυτό όμως δεν εξασφαλίζει ότι το κείμενο δεν γράφτηκε οποιαδήποτε στιγμή μετά την κυκλοφορία της εφημερίδας. Για να εξασφαλίσουμε και αυτό, θα μπορούσαμε να δημοσιεύσουμε το κείμενο στην εφημερίδα της επόμενης ημέρας. Αλλά, μια τέτοια μέθοδος θα ήταν δύσκολη, ακριβή και θα καταργούσε το απόρρητο του κειμένου.

Η λύση βρίσκεται στη λεγόμενη «μυστική τιμή» του κειμένου. Πρόκειται για ένα μεγάλο αριθμό που παράγεται από μια μυστική συνάρτηση χρησιμοποιώντας

σαν δεδομένο όλο το κείμενο. Οι μυστικές συναρτήσεις που χρησιμοποιούνται για αυτό το σκοπό έχουν τρεις βασικές ιδιότητες που τους επιτρέπουν να λειτουργούν σαν δακτυλικό αποτύπωμα ενός κειμένου:

Πρώτον είναι διαθέσιμες σε όλους, όλοι μπορούν να τις χρησιμοποιήσουν για να υπολογίσουν τη μυστική τιμή του κειμένου, αρκεί να το έχουν στα χέρια τους.

Δεύτερον, είναι συνάρτηση «μίας κατεύθυνσης». Καθένας μπορεί να υπολογίσει τη μυστική τιμή ενός κειμένου που έχει, αλλά αν έχει μόνο τη μυστική τιμή δεν μπορεί να τη χρησιμοποιήσει για να αναπαράγει το κείμενο από το οποίο αυτή προήλθε.

Τρίτον, αν και θεωρητικά δύο κείμενα θα μπορούσαν να δώσουν την ίδια μυστική τιμή, στην πράξη η πιθανότητα για κάτι τέτοιο τείνει στο 0.

Η παραμικρή αλλαγή στο κείμενο θα αλλάξει αυτόματα και τη μυστική τιμή του. Ακόμη και αν ζητούσαμε από έναν υπερ-υπολογιστή να παράγει ένα κείμενο με δεδομένη μυστική τιμή (ίδια με κάποιο άλλο κείμενο), το αποτέλεσμα θα ήταν ένα σύνολο χαρακτήρων που σε καμία περίπτωση δεν θα είχαν κάποια λογική σειρά και, συνεπώς, δεν θα ήταν αναγνώσιμο.

Η πιστοποίηση του χρόνου γίνεται από τις εταιρίες ΑΠ. Αυτές μπορούν εύκολα να παρέχουν μια σφραγίδα χρονοσήμανσης, πιστοποιώντας ότι έλαβαν από κάποιο συνδρομητή μια συγκεκριμένη μυστική τιμή σε μια συγκεκριμένη χρονική στιγμή. Με αυτό τον τρόπο εξαλείφεται μεγάλο μέρος του κινδύνου, αφήνοντας μόνο την περίπτωση κακοπιστίας από πλευράς της ΑΠ και παροχής, ίσως μετά από συνεννόηση με το συνδρομητή, σφραγίδας προχρονολογημένης. Όμως, και αυτή η περίπτωση μπορεί να αντιμετωπιστεί με μια παραλλαγή της μεθόδου: Η ΑΠ, όταν λαμβάνει την μυστική τιμή από το συνδρομητή, αντί να επιστρέψει απλά τη μυστική τιμή και μια σφραγίδα χρονοσήμανσης, επιστρέφει μαζί και τις μυστικές τιμές μαζί με τις αντίστοιχες ηλεκτρονικές διευθύνσεις των -μερικών - άλλων τελευταίων συνδρομητών που ζήτησαν πιστοποίηση. Έτσι, η κακοπιστία γίνεται φοβερά δύσκολή, αφού θα απαιτούσε συνεννόηση όχι μόνο με την ΑΠ αλλά και με όλους τους πρόσφατους χρήστες του συστήματος.

Α.3 Ψηφιακές Υπογραφές

Τα συστήματα Δημοσίου Κλειδιού, επιτρέπουν στο χρήστη να προσθέτει στα κρυπτογραφημένα του μηνύματα και μια ψηφιακή υπογραφή. Μια ψηφιακή

υπογραφή κρυπτογραφημένη με ένα μυστικό κλειδί προσδιορίζει με τρόπο μοναδικό τον αποστολέα του μηνύματος. Εάν χρησιμοποιηθεί επιπλέον και μια ψηφιακή «σφραγίδα χρονοσήμανσης», μπορεί να αποδειχτεί και η ακριβής ώρα αποστολής του μηνύματος. Οποιοσδήποτε κατέχει το δημόσιο κλειδί του αποστολέα, μπορεί και να πιστοποιήσει την γνησιότητα της ψηφιακής υπογραφής του. Επειδή η ψηφιακή υπογραφή χρησιμοποιεί το κείμενο του μηνύματος για την παραγωγή του αλγορίθμου κρυπτογράφησης, αν το μήνυμα τροποποιηθεί έστω και στο ελάχιστο, η υπογραφή δεν θα αποκρυπτογραφείται σωστά δείχνοντας ότι το μήνυμα τροποποιήθηκε καθ' οδόν ή ακόμα ότι η υπογραφή είναι πλαστογραφημένη, όπως για παράδειγμα αν έχει αντιγραφεί από άλλο μήνυμα. Στην περίπτωση αντιγραφής της υπογραφής και μεταφοράς της από μήνυμα σε μήνυμα η πιθανότητα σωστής αντιστοίχισής της με το νέο μήνυμα, ώστε να δείχνει αυθεντική, τείνει στο μηδέν.

Πάντως, και εδώ ισχύει το πρόβλημα που αναφέρθηκε παραπάνω: Η δυνατότητα για τον παραλήπτη να πιστοποιήσει με απόλυτο τρόπο την ταυτότητα του αποστολέα βάσει της ψηφιακής υπογραφής εξαρτάται από το κατά πόσο ο παραλήπτης είναι σίγουρος ότι το δημόσιο κλειδί του αποστολέα το οποίο έχει στα χέρια του είναι πραγματικά αυθεντικό.

Εφόσον τα δύο μέρη που επιθυμούν να επικοινωνήσουν δεν γνωρίζονται ήδη και δεν έχουν φυσική, εκτός δικτύου, επικοινωνία ώστε να μπορούν εύκολα να πιστοποιήσουν ο ένας την ταυτότητα του άλλου, δεν μπορούν να αποκλείσουν την περίπτωση παρεμβολής κάποιου κακόβουλου και της αποστολής από αυτόν του δικού του δημόσιου κλειδιού, ακόμα και αν χρησιμοποιούν συστήματα κρυπτογράφησης και ψηφιακές υπογραφές.

Η μοναδική λύση στο πρόβλημα είναι η χρήση κάποιας τρίτης, ανεξάρτητης, έμπιστης πηγής που θα συνέδεε την πραγματική ταυτότητα του καθενός και το δημόσιο κλειδί του. Για παράδειγμα, μια τηλεφωνική εταιρία θα μπορούσε να γνωστοποιεί το δημόσιο κλειδί της πάνω στους μηνιαίους λογαριασμούς της, ή μια ιδιωτική εταιρία θα μπορούσε να δημοσιεύει το δικό της στις εφημερίδες.

Τέλος, στην περίπτωση των δύο χρηστών που προσπαθούν να επικοινωνήσουν, θα μπορούσε να παίξει το ρόλο της τρίτης, έμπιστης πηγής πιστοποίησης της σχέσης ταυτοτήτων και δημοσίων κλειδιών ένας κοινός φίλος,

ένας δημόσιος οργανισμός ή μια ειδικευμένη εταιρία παροχής υπηρεσιών πιστοποίησης.

Α.4 Φορείς Πιστοποίησης

Φορέας Πιστοποίησης (ΦΠ) είναι κάθε φορέας, δημόσιος ή ιδιωτικός, που προορίζεται να καλύψει την ανάγκη για ανεξάρτητες, έμπιστες υπηρεσίες πιστοποίησης στο ηλεκτρονικό εμπόριο, εκδίδοντας ψηφιακά πιστοποιητικά που επικυρώνουν κάποια στοιχεία σχετικά με το αντικείμενο του πιστοποιητικού.

Στο παράδειγμα που χρησιμοποιήθηκε παραπάνω, προκειμένου η Α και ο Β να εμπιστευτούν τα πιστοποιητικά μιας Αρχής Πιστοποίησης ΑΠ1 θα πρέπει πρώτα να εμπιστεύονται την αυθεντικότητα του κλειδιού της ίδιας της ΑΠ1. Και αν αυτή πιστοποιηθεί από μια άλλη Αρχής Πιστοποίησης ΑΠ2, το πρόβλημα μεταφέρεται στην αυθεντικότητα του κλειδιού πλέον της ΑΠ2 και ούτω καθ΄ εξής. Δημιουργείται δηλαδή ένα δέντρο από Φορείς Πιστοποίησης, όπου το πρόβλημα της ανασφάλειας μεταφέρεται απλά από τη μία στην άλλη.

Μια λύση σε αυτό το πρόβλημα θα ήταν η εμπλοκή κάποιου δημόσιου φορέα που θα βρισκόταν στην κορυφή του δέντρου και πιστοποιούσε τα κλειδιά των Αρχών Πιστοποίησης. Σε αυτή την περίπτωση, αυτός ο δημόσιος φορέας θα έλεγχε κάθε Φορέας Πιστοποίησης, θα επέλεγε εκείνες που πληρούν τις απαραίτητες προϋποθέσεις και θα πιστοποιούσε ο ίδιος τα κλειδιά τους. Αυτές οι, πιστοποιημένες από το κράτος, Φορείς Πιστοποίησης θα πιστοποιούσαν, με τη σειρά τους, τα κλειδιά οργανισμών που θα ήθελαν να διαχειριστούν δικά τους πιστοποιητικά.

Έτσι, για παράδειγμα, μια Φορέας Πιστοποίησης θα πιστοποιούσε το κλειδί της εταιρίας ΑΒΓ, αυτή με τη σειρά της θα πιστοποιούσε τα κλειδιά των τμημάτων της και αυτά θα έκαναν το ίδιο για τα προσωπικά κλειδιά των στελεχών και του προσωπικού τους.

Σε όσο περισσότερα επίπεδα είναι ανεπτυγμένο το δέντρο πιστοποίησης, τόσο περισσότερα πιστοποιητικά θα χρειαστεί να ελέγξει η Α προκειμένου να σιγουρευτεί ότι το πιστοποιητικό του Β παραμένει σε ισχύ.

Ας υποθέσουμε ότι η ψηφιακή υπογραφή του Β είναι πιστοποιημένη από την ΑΠ1, της οποίας το δημόσιο κλειδί είναι πιστοποιημένο από την ΑΠ2, και αυτής

από την ΑΠ3, και αυτής από ένα δημόσιο οργανισμό. Εάν ο δημόσιος οργανισμός εκδώσει μια ανακοίνωση ανάκλησης του πιστοποιητικού της ΑΠ3 επειδή διαπιστώθηκε υπεξαίρεση του δημόσιου κλειδιού της από κάποιον τρίτο, όλα τα πιστοποιητικά που έχει εκδώσει η ΑΠ3 είναι πλέον ύποπτα. Αν, από την άλλη, η ΑΠ3 μπορούσε να διαβεβαιώσει ότι το κλειδί της ήταν ασφαλές τουλάχιστον μέχρι κάποια συγκεκριμένη ημερομηνία, τότε τα πιστοποιητικά που συνοδεύονταν από μια ασφαλή σφραγίδα χρόνου που δείχνει ότι αυτά εκδόθηκαν πριν από αυτή την ημερομηνία θα παρέμεναν αξιόπιστα. Η Α θα μπορούσε να ακολουθήσει όλη αυτή τη διαδικασία ελέγχου, αλλά αυτό θα απαιτούσε αρκετό χρόνο και πρόσβαση σε τόσες διαφορετικές βάσεις δεδομένων όσες είναι και οι ΦΠ που εμπλέκονται. Κάτι τέτοιο θα ήταν ιδιαίτερα άβολο και χρονοβόρο.

Για την ώρα, οι λίγες Φορείς Πιστοποίησης που λειτουργούν αντιμετωπίζουν την έλλειψη κεντρικής ΦΠ - φορέα στην κορυφή του δέντρου, πιστοποιώντας οι ίδιες το κλειδί τους και απλά δημοσιεύοντας τα πιστοποιητικά τους, που οι ίδιες έχουν εγκρίνει, στις ιστοσελίδες τους.

Το σύστημα της «αυτο-πιστοποίησης», κατά το οποίο η ΦΠ βασίζεται στη φήμη και το κύρος της που προκύπτει από το παρελθόν και την παρουσία της στην αγορά, σχηματοποιεί ένα μοντέλο σχετικά επίπεδης ιεραρχίας πιστοποίησης.

Κατά τους ειδικούς, η μελλοντική τάση παραμένει στην σχετικά επίπεδη ιεραρχία πιστοποίησης, όπου οι οργανισμοί θα έχουν ένα κεντρικό πιστοποιητικό για εσωτερική χρήση, πιστοποιημένο από άλλη μία, το πολύ, Φορέας Πιστοποίησης. Είναι ακόμη πολύ νωρίς για να πει κανείς με σιγουριά ποιο μοντέλο πιστοποίησης θα επικρατήσει τελικά, αλλά είναι ενδιαφέρον το γεγονός ότι σήμερα ο βασικός παράγοντας εξασφάλισης της αυθεντικότητας των περισσότερων, για παράδειγμα, επιστολών με συμβουλές από λογιστές ή δικηγόρους προς πελάτες τους, είναι απλά το λογότυπό τους (που μπορεί να πλαστογραφηθεί με χαρακτηριστική ευκολία) και η σχετική διαβεβαίωση εκείνου που παραδίδει την επιστολή.