

Το ψηφιακό πιστοποιητικό είναι για τον ηλεκτρονικό κόσμο το αντίστοιχο του διαβατηρίου για τον φυσικό κόσμο. Εκδίδεται από έναν Πάροχο Υπηρεσιών Πιστοποίησης (Αρχή Ψηφιακής Πιστοποίησης) που εγγυάται για τα στοιχεία του κατόχου του, ακριβώς όπως η αρμόδια κρατική αρχή εγγυάται για την έκδοση του διαβατηρίου.

Η κατοχή του ψηφιακού πιστοποιητικού διασφαλίζεται από την αποκλειστική κατοχή συγκεκριμένων ψηφιακών δεδομένων (ιδιωτικό κλειδί) από το φυσικό πρόσωπο. Ο Πάροχος δημοσιεύει ψηφιακά δεδομένα σχετικά με την επαλήθευση της κατοχής του πιστοποιητικού (δημόσιο κλειδί) και εγγυάται για τα στοιχεία του φυσικού προσώπου.

Η ηλεκτρονική υπογραφή δημιουργείται με βάση τα δεδομένα αποκλειστικής κατοχής (ιδιωτικό κλειδί) και τα προς υπογραφή δεδομένα και αποτελεί μια ψηφιακή "ετικέτα" η οποία επισυνάπτεται στα προς υπογραφή δεδομένα. Σκοπός είναι:

- α) η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση της ηλεκτρονικής συναλλαγής με το φυσικό πρόσωπο που υπογράφει,
- β) η εγγύηση της γνησιότητας των ψηφιακών δεδομένων και
- γ) η δέσμευση του υπογράφοντος ως προς την ηλεκτρονική συναλλαγή, δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί την συμβολή του στην εν λόγω συναλλαγή.

Σε αντιδιαστολή με την ιδιόχειρη υπογραφή, το ακριβές περιεχόμενο της ηλεκτρονικής υπογραφής διαφοροποιείται ανάλογα με τα προς υπογραφή δεδομένα αφού προκύπτει με βάση και αυτά.