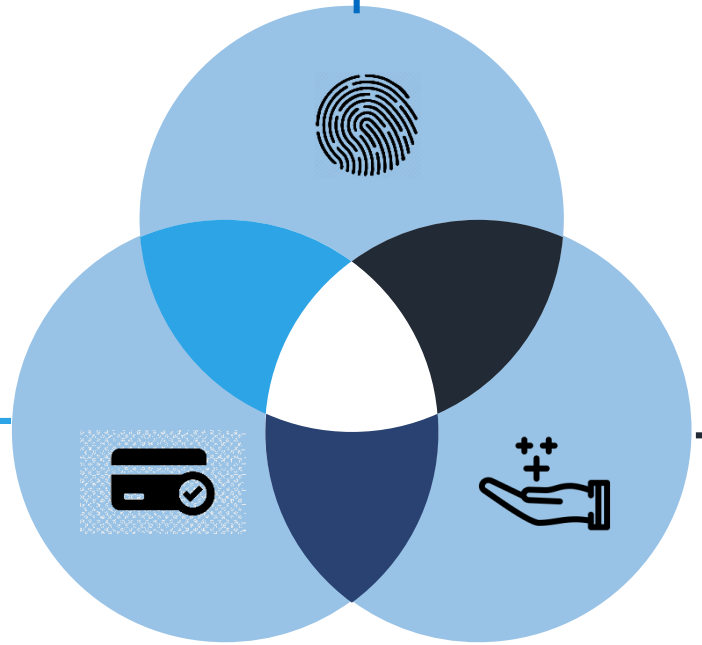
Διαδικασία αυστηρής εξακρίβωσης πελάτη (Strong Customer Authentication- SCA)

Εύη Δημητροπούλου, Δικηγόρος LLM /DEA

Τι είναι η διαδικασία SCA;

Ισχυρή ταυτοποίηση πελάτη σε ηλεκτρονικές πληρωμές- PSD II

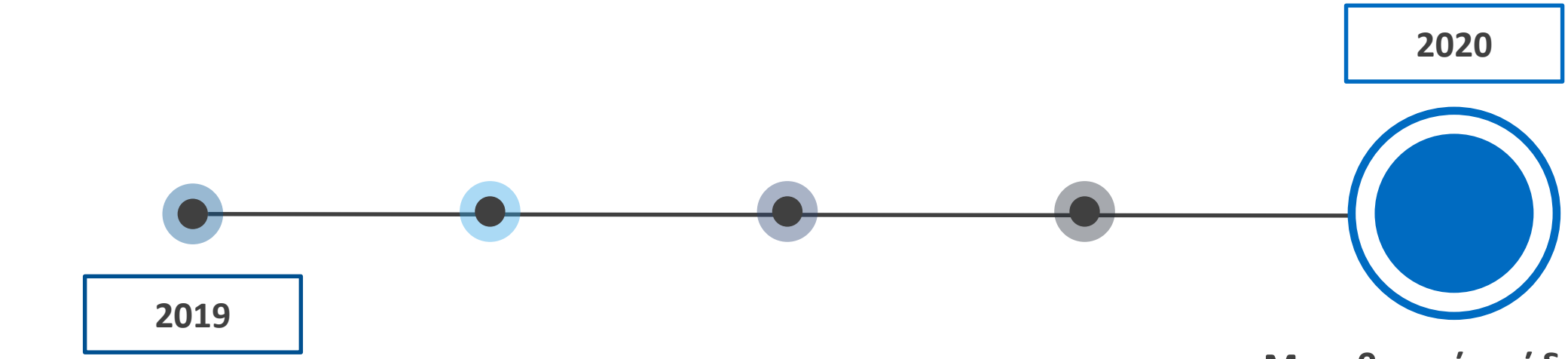


Τράπεζα καταναλωτή και τράπεζα εμπόρου εντός Ε.Ε.

Σκοπιμότητα:

- Μείωση απάτης
- Ασφάλεια στις συναλλαγές
- Εναρμόνιση διαδικασιών

Χρονοδιάγραμμα εφαρμογής



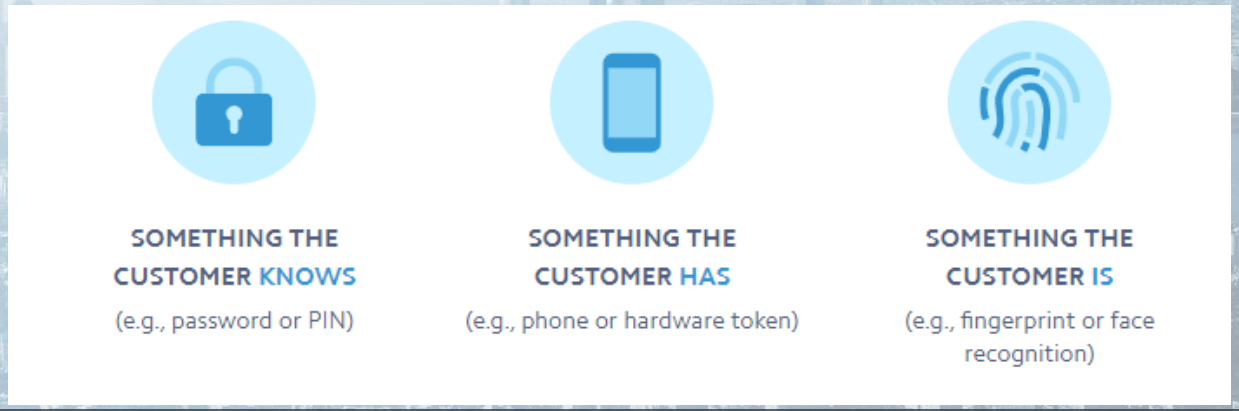
Θέση σε ισχύ στις
14 Σεπτεμβρίου 2019

Μεταβατικό στάδιο:
Ανοχή από τις εποπτικές αρχές μέχρι τις
31 Δεκεμβρίου 2020

Τα τεχνικά πρότυπα της SCA

Συνδυασμός δύο στοιχείων από δύο διαφορετικές κατηγορίες

- ✓ Κάτι που πληρωτής γνωρίζει
- ✓ Κάτι που ο πληρωτής κατέχει
- ✓ Κάτι που συνδέεται με φυσικά χαρακτηριστικά του πληρωτή



Ανεξαρτησία στοιχείων

Δυναμική σύνδεση με συναλλαγή

Κάτι που ο πληρωτής γνωρίζει

K G Law Firm

two factor authentication - Αγγλ | EBA publishes an Opinion on the | BoS 2019 XX (EBA Opinion on SC

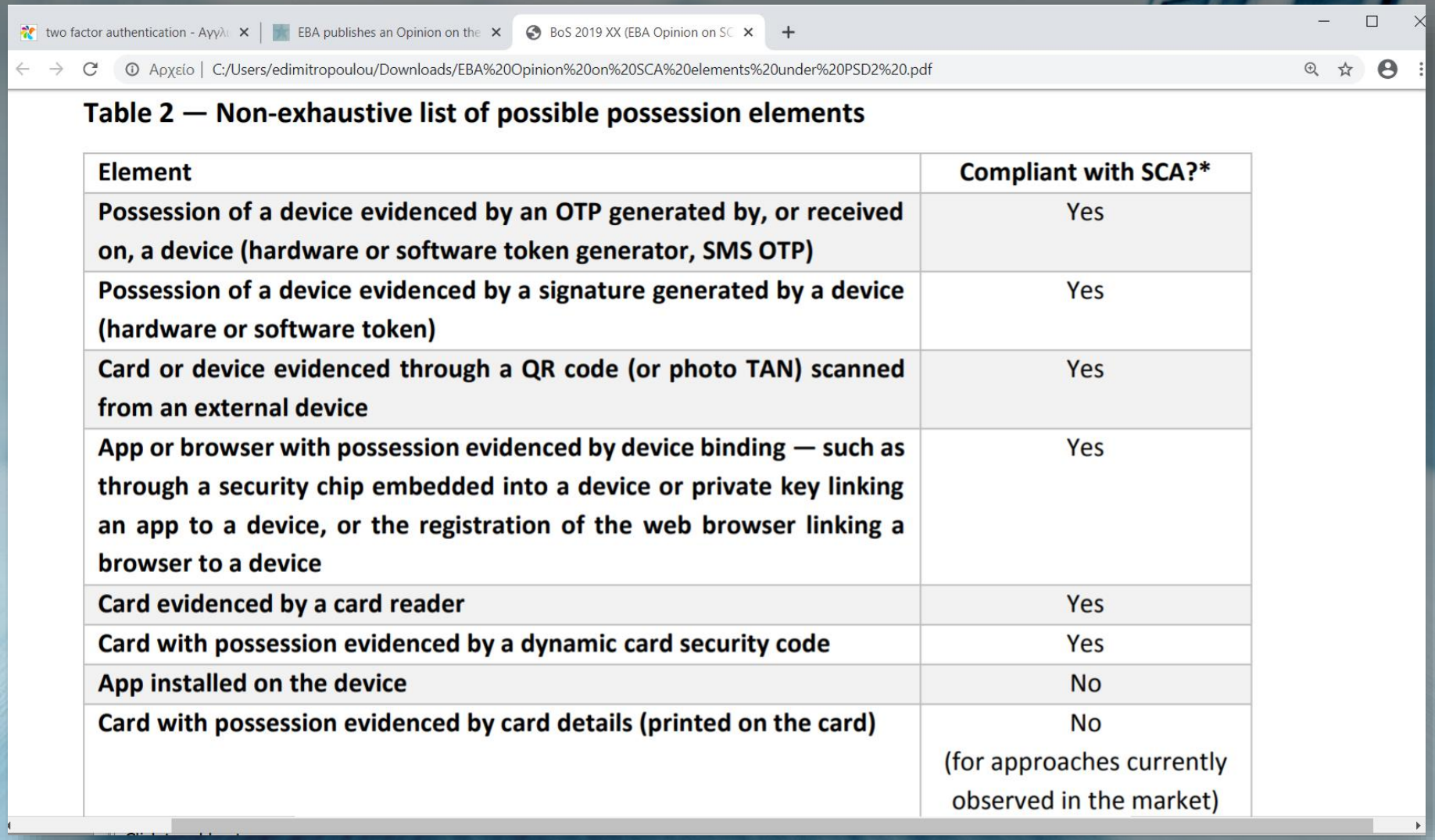
Αρχείο | C:/Users/edimitropoulou/Downloads/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

Table 3 — Non-exhaustive list of possible knowledge elements

Element	Compliant with SCA?*
Password	Yes
PIN	Yes
Knowledge-based challenge questions	Yes
Passphrase	Yes
Memorised swiping path	Yes
Email address or user name	No
Card details (printed on the card)	No
OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	No (for approaches currently observed in the market)

Click to add notes

Κάτι που ο πληρωτής κατέχει


two factor authentication - Αγγλι | EBA publishes an Opinion on the | BoS 2019 XX (EBA Opinion on SC

Αρχείο | C:/Users/edimitropoulou/Downloads/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

Table 2 — Non-exhaustive list of possible possession elements

Element	Compliant with SCA?*
Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	Yes
Possession of a device evidenced by a signature generated by a device (hardware or software token)	Yes
Card or device evidenced through a QR code (or photo TAN) scanned from an external device	Yes
App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device	Yes
Card evidenced by a card reader	Yes
Card with possession evidenced by a dynamic card security code	Yes
App installed on the device	No
Card with possession evidenced by card details (printed on the card)	No (for approaches currently observed in the market)

Κάτι που συνδέεται με φυσικά χαρακτηριστικά του πληρωτή

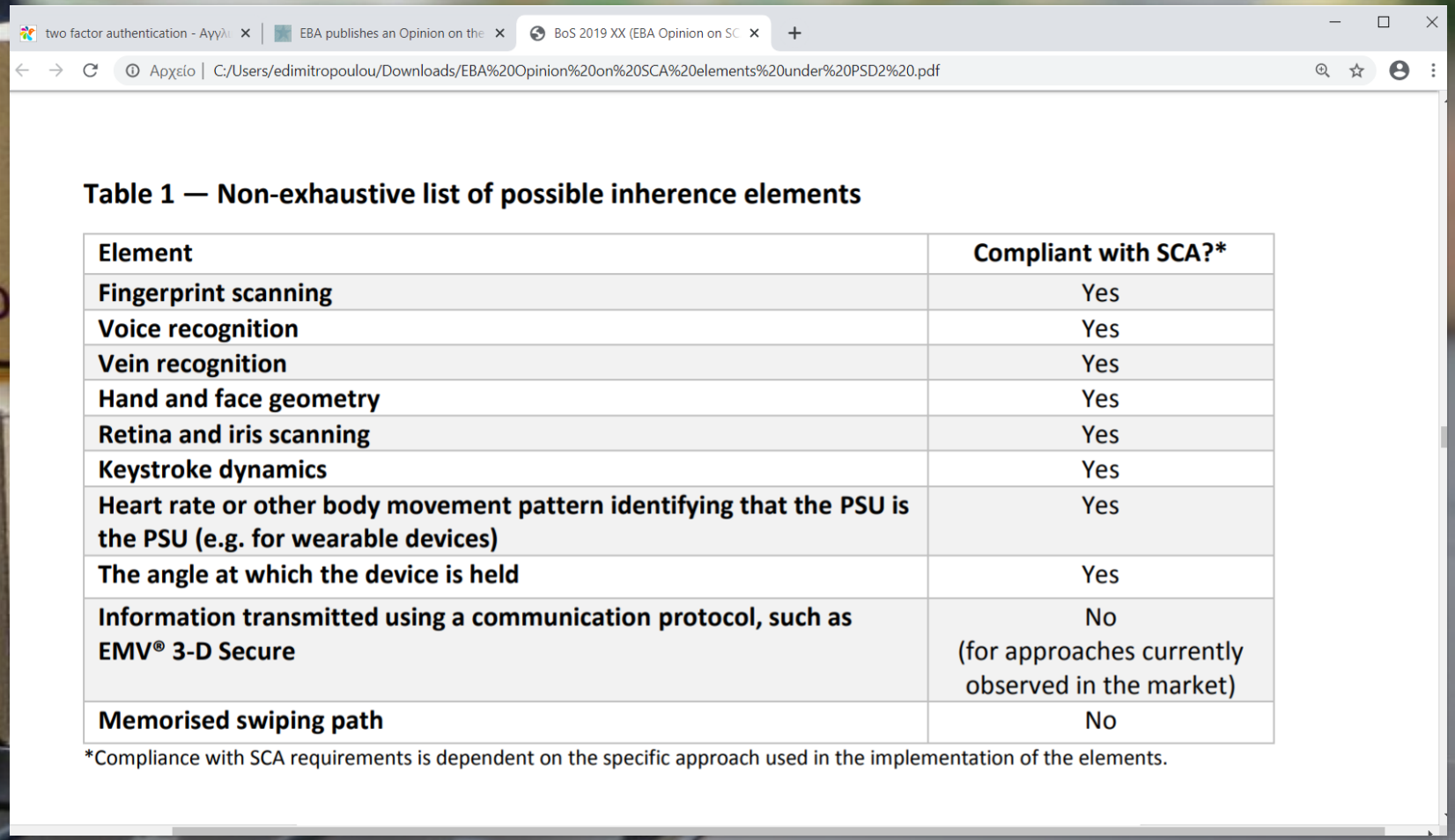


Table 1 — Non-exhaustive list of possible inherence elements

Element	Compliant with SCA?*
Fingerprint scanning	Yes
Voice recognition	Yes
Vein recognition	Yes
Hand and face geometry	Yes
Retina and iris scanning	Yes
Keystroke dynamics	Yes
Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices)	Yes
The angle at which the device is held	Yes
Information transmitted using a communication protocol, such as EMV® 3-D Secure	No (for approaches currently observed in the market)
Memorised swiping path	No

*Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.

Εξαιρέσεις από τη διαδικασία SCA

01

Έμπιστοι δικαιούχοι

02

Επαναλαμβανόμενες συναλλαγές

03

Συναλλαγές μικρής αξίας

04

Συναλλαγές χαμηλού κινδύνου- Αξιολόγηση από τράπεζα του πληρωτή

Συμπεράσματα

Ανησυχίες

1. Μακρύτερη διαδικασία ολοκλήρωσης της ηλεκτρονικής συναλλαγής
2. Δυσαρέσκεια πελάτη- Εγκατάλειψη συναλλαγής

Πραγματικότητα

1. Ομαλή εμπειρία χρήστη
2. Μείωση περιστατικών απάτης
3. Τόνωση εμπιστοσύνης

K G
Law Firm

Ευχαριστώ!

http://www.kglawfirm.gr/