ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Προστασία δεδομένων στα νέα “πορτοφόλια” ψηφιακής ταυτότητας στην ΕΕ: Προοπτικές και προκλήσεις

Δρ. Κωνσταντίνος Λιμνιώτης,

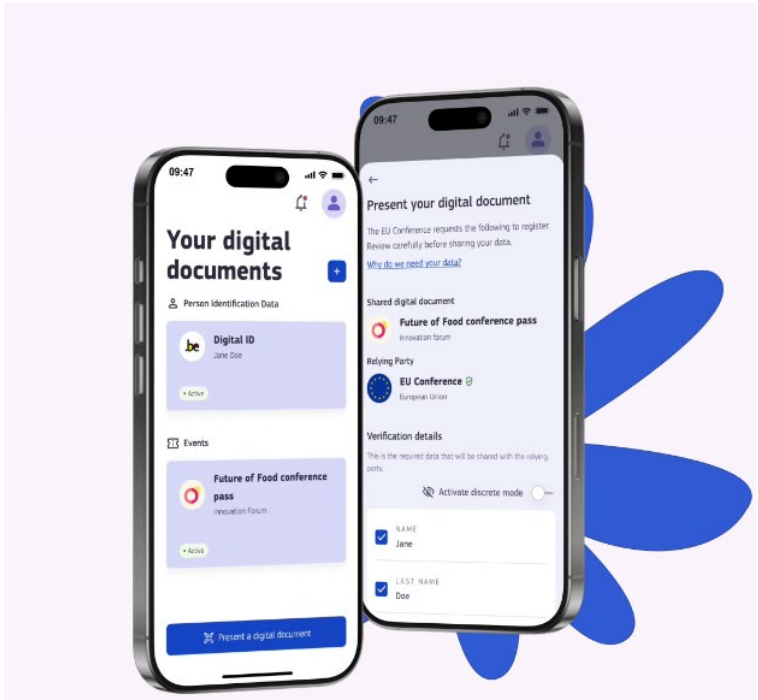
Ειδικός Επιστήμονας Πληροφορικής, Τμήμα Μελετών και Έρευνας

Επισκόπηση

- Τι είναι το νέο «ψηφιακό πορτοφόλι»
  - Στόχοι – Εφαρμογές - Προοπτικές
- Νομικό πλαίσιο
  - Ιστορικό – Τρέχουσα κατάσταση
- Κρίσιμα ζητήματα υλοποίησης
  - «Επίσημα» διατυπωμένοι προβληματισμοί (και) ως προς κρυπτογραφικές επιλογές
- Συμπεράσματα – Σκέψεις
  - Υπό το φως και την προτιθέμενης χρήσης του για επαλήθευση ηλικίας χρηστών

Τι είναι το «πορτοφόλι» ψηφιακής ταυτότητας (DIW)

- Digital Identity Wallet (DIW): Εφαρμογή που επιτρέπει την ασφαλή αποθήκευση, διαχείριση και κοινοποίηση προσωπικών δεδομένων (συμπεριλαμβανομένων διαπιστευτηρίων για επαλήθευση ταυτότητας) που αφορούν τον κάτοχό του
- Οι προσωπικές πληροφορίες στο DIW ονομάζονται «χαρακτηριστικά» (attributes)
  - Π.χ. δελτίο ταυτότητας, άδεια οδήγησης, πτυχίο, κάρτα γυμναστηρίου κ.α.
- Όπως τα φυσικά πορτοφόλια, όμως αντί για μετρητά/πιστωτικές κάρτες τηρούν ψηφιακά χαρακτηριστικά.

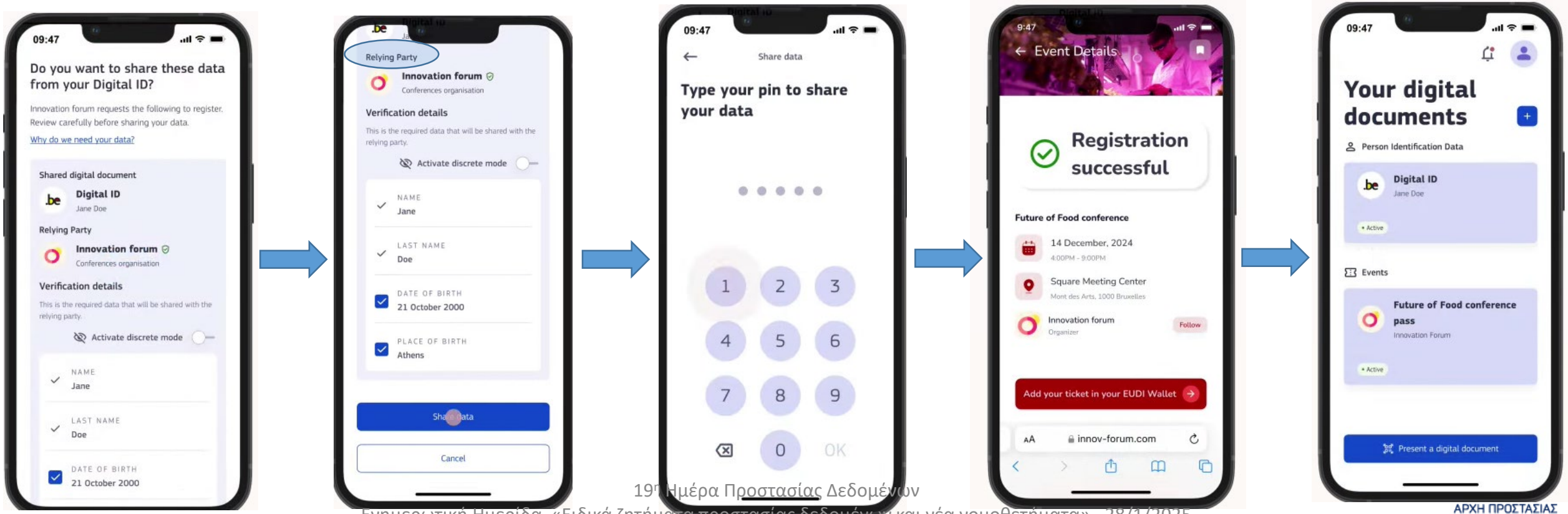


ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Εφαρμογές

Πηγή:
https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+wallet

- Πρόσβαση σε διαδικτυακές υπηρεσίες – Αποθήκευση προσωπικών δεδομένων - Επιλεκτική διαμοίραση προσωπικών δεδομένων – Ψηφιακές υπογραφές



Γενικές ιδιότητες

- Αυθεντικοποίηση χρήστη σε πλήθος φορέων/υπηρεσιών
  - Όχι μόνο σε δημόσιους φορείς, αλλά και σε ιδιωτικούς
  - Συμπεριλαμβανομένων τρίτων φορέων οι οποίοι δεν σχετίζονται με την έκδοση των πρωτότυπων 'χαρακτηριστικών' ('Relying Parties' - ' Βασιζόμενα μέρη')
    - **Και οι πολύ μεγάλες διαδικτυακές πλατφόρμες**
- Διασυνοριακή αυθεντικοποίηση
- Δυνατότητα των χρηστών να υπογράφουν ψηφιακά
- Ασφαλής τήρηση και αποστολή προσωπικών δεδομένων ('χαρακτηριστικών')
  - Μέσω κρυπτογραφικών αλγορίθμων
- Επιλεκτική γνωστοποίηση ('selective disclosure') προσωπικών δεδομένων
- Δυνατότητα χρήσης ψευδωνύμου για το χρήστη
  - Εφόσον ο πάροχος της υπηρεσίας δεν χρειάζεται να γνωρίζει την ταυτότητα του χρήστη

Γενικές ιδιότητες

- Αυθεντικοποίηση χρήστη σε πλήθος φορέων/υπηρεσιών
  - Όχι μόνο σε δημόσιους φορείς, αλλά και σε ιδιωτικούς
  - Συμπεριλαμβανομένων τρίτων φορέων οι οποίοι δεν σχετίζονται με την έκδοση των πρωτότυπων 'χαρακτηριστικών' ('Relying Parties' - ' Βασιζόμενα μέρη')
    - **Και οι πολύ μεγάλες διαδικτυακές πλατφόρμες**
- Διασυνοριακή αυθεντικοποίηση
- Δυνατότητα των χρηστών να υπογράφουν ψηφιακά
- Ασφαλής τήρηση και αποστολή προσωπικών δεδομένων ('χαρακτηριστικών')
  - Μέσω κρυπτογραφικών αλγορίθμων

Συναφή με την αρχή της **ελαχιστοποίησης δεδομένων**

- Επιλεκτική γνωστοποίηση ('selective disclosure') προσωπικών δεδομένων
- Δυνατότητα χρήσης ψευδωνύμου για το χρήστη
  - Εφόσον ο πάροχος της υπηρεσίας δεν χρειάζεται να γνωρίζει την ταυτότητα του χρήστη

Νομικό πλαίσιο (και «ιστορική αναδρομή»)

- Κανονισμός (ΕΕ) 910/2014 (eIDAS Regulation) σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά
- 3 Ιουνίου 2021: Πρόταση της ΕΕ για επικαιροποίηση του Κανονισμού eIDAS (eIDAS Proposal) (eIDAS 2)
  - Εισαγωγή της έννοιας του «πορτοφολιού» ψηφιακής ταυτότητας
  - 28 Ιουλίου 2021: Επίσημα σχόλια του Ευρωπαίου Επόπτη Προστασίας Δεδομένων
- 11 Απριλίου 2024: **Κανονισμός (ΕΕ) 2024/1183** για την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 όσον αφορά τη θέσπιση ευρωπαϊκού πλαισίου για την ψηφιακή ταυτότητα
  - Σχετικές υποχρεώσεις για υλοποίηση ψηφιακού πορτοφολιού από τα Κράτη – Μέλη **έως το 2026**

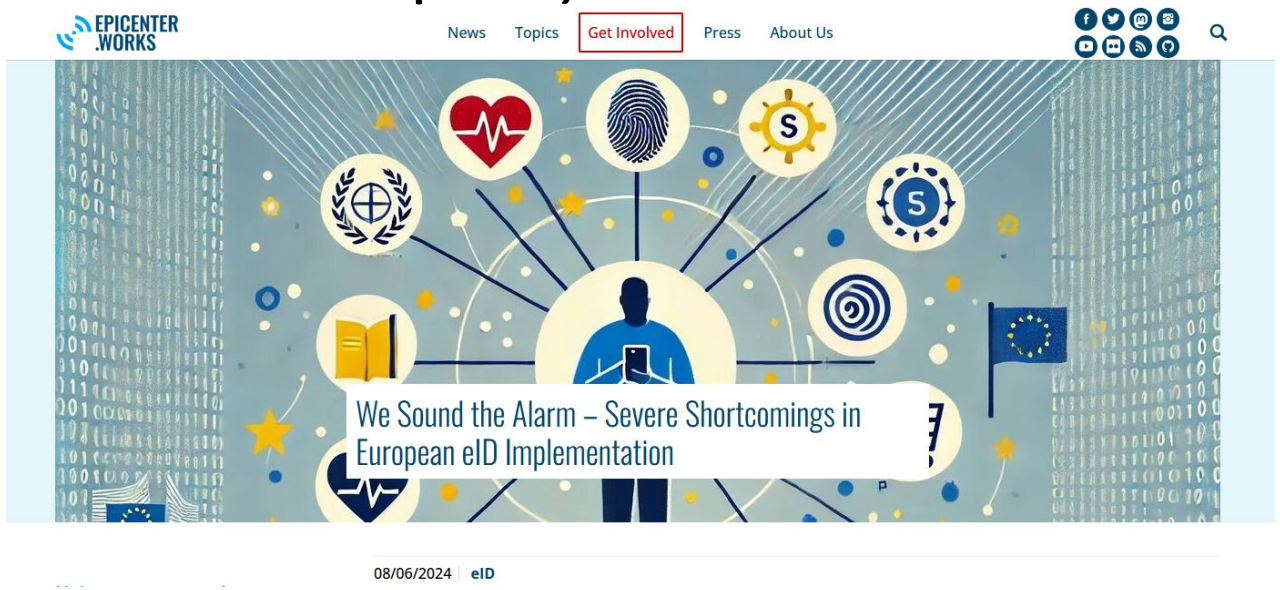
Στοιχεία του νέου Κανονισμού

- Το νέο ψηφιακό πορτοφόλι **δεν θα είναι υποχρεωτικό για τους πολίτες**
  - Είναι όμως υποχρεωτικό για τα Κράτη – Μέλη να παρέχουν τουλάχιστον μία τέτοια λύση, ανοιχτού κώδικα
  - Η ΕΕ θα παρέχει μία λύση, προς πιθανή αξιοποίηση από τα Κράτη – Μέλη
- Άρθρο 5α, στοιχ. 17: *«Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα που διενεργείται από τα κράτη μέλη ή για λογαριασμό τους από φορείς ή μέρη υπεύθυνα για την παροχή των ευρωπαϊκών πορτοφολιών ψηφιακής ταυτότητας ως μέσων ηλεκτρονικής ταυτοποίησης διενεργείται σύμφωνα με κατάλληλα και αποτελεσματικά μέτρα προστασίας δεδομένων. Η συμμόρφωση της εν λόγω επεξεργασίας με τον κανονισμό (ΕΕ) 2016/679 αποδεικνύεται. Τα κράτη μέλη μπορούν να θεσπίζουν εθνικές διατάξεις για να εξειδικεύουν περαιτέρω την εφαρμογή των εν λόγω μέτρων.»*
- Δυνατότητα πιστοποίησης «πορτοφολιών»

Ζητήματα υλοποίησης

- Ο νέος Κανονισμός θέτει ζητήματα δομικά και διακυβέρνησης, διατυπώνοντας μεταξύ άλλων τους επιθυμητούς στόχους, αλλά και τους ρόλους των διαφόρων εμπλεκομένων
- Θέματα υλοποίησης μένουν να αντιμετωπιστούν ανεξάρτητα
- Τεχνικά χαρακτηριστικά της λύσης της Επιτροπής είναι διαθέσιμα:
  - Architecture and Reference Framework (ARF) – τρέχουσα έκδοση: 1.4.0
    - https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/
    - Διαθέσιμο για επιθεώρηση/παρατηρήσεις/σχολιασμό
- Πέντε σχέδια εκτελεστικών Κανονισμών (implementing Regulations) για επιμέρους ζητήματα του πορτοφολιού ψηφιακής ταυτότητας τέθηκαν σε δημόσια διαβούλευση (μέχρι Σεπτέμβριο 2024)
  - Τελικές εκδοχές τους από την Επιτροπή: 28/11/2024

Επιστημονική κοινότητα και φορείς αναφορικά με την υλοποίηση πορτοφολιού ψηφιακής ταυτότητας



Cryptographers' Feedback on the EU Digital Identity's ARF

Carsten Baum
Technical University of Denmark

Olivier Blazy
École Polytechnique

Jan Camenisch
Dfinity

Jaap-Henk Hoepman
Karlstad University
& Radboud University

Eysa Lee
Brown University

Anja Lehmann
Hasso-Plattner-Institute,
University of Potsdam

Anna Lysyanskaya
Brown University

René Mayrhofer
Johannes Kepler University Linz

Hart Montgomery*

Ngoc Khanh Nguyen
King's College London

Bart Preneel
KU Leuven

abhi shelat
Northeastern University

Daniel Slamanig
Universität der Bundeswehr München

Stefano Tessaro
University of Washington

Søren Eller Thomsen
Partisia

Carmela Troncoso
EPFL

June 2024

GSMA

eIDAS 2.0 and Privacy

Official Response

GSMA Europe

EUROPEAN DATA PROTECTION SUPERVISOR

> ... > TechSonar > Digital identity wallet

Digital identity wallet

Author: Massimo Attoresi

Increased risk of profiling

DIWs intrinsically carry individuals' identification information as well as other pieces of information that could uniquely identify them. In absence of safeguards, this information could be combined by all parties having access to the DIW (providers of identity services in particular but also relying parties) with other information already retained by those parties on the actions performed by the same individual. Furthermore, DIWs can store any possible personal data including sensitive ones, directly or indirectly relating to health, sexual orientation, religious or philosophical beliefs, political opinions, financial situation, family life etc. This accumulation of personal information could encourage both private and public actors' appetite to exploit this data. For this reason, DIWs have a high potential to enable profiling of individuals if the features and use of DIWs are not consistent with a privacy by design and by default approach, and if appropriate policies are not in place. Some specific weaknesses enabling profiling are described below.

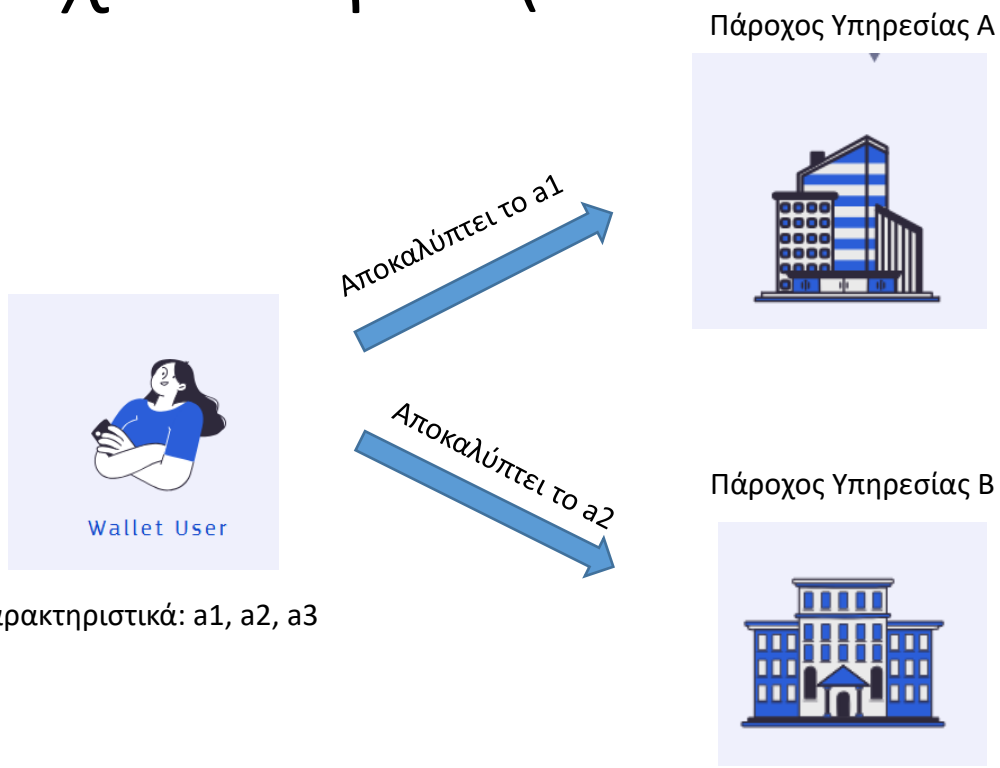
Απαιτήσεις του Κανονισμού (ΕΕ) 2024/1183

- Άρθρο 5α, παρ. 4: Τα ευρωπαϊκά πορτοφόλια ψηφιακής ταυτότητας παρέχουν στον χρήστη [..] τη δυνατότητα:
  - (α) με τρόπο ασφαλή [..] να προβαίνει σε επαλήθευση ταυτότητας έναντι βασιζόμενων μερών εντός διαδικτύου [..] διασφαλίζοντας παράλληλα τη δυνατότητα επιλεκτικής γνωστοποίησης δεδομένων
  - (β) να δημιουργεί ψευδώνυμα και να τα αποθηκεύει κρυπτογραφημένα και τοπικά εντός του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας
- Άρθρο 5α, παρ. 16: Το τεχνικό πλαίσιο του ευρωπαϊκού πορτοφολιού ψηφιακής ταυτότητας:
  - (α) δεν επιτρέπει στους παρόχους ηλεκτρονικών βεβαιώσεων χαρακτηριστικών ή σε οιοδήποτε άλλο μέρος, μετά την έκδοση της βεβαίωσης χαρακτηριστικών, να αποκτούν δεδομένα που επιτρέπουν την παρακολούθηση, τη σύνδεση ή τη συσχέτιση συναλλαγών ή της συμπεριφοράς του χρήστη, ή την απόκτηση με άλλον τρόπο γνώσεων σχετικά με τις συναλλαγές ή τη συμπεριφορά χρήστη, εκτός εάν αυτό επιτρέπεται ρητά από τον χρήστη
  - (β) επιτρέπει τεχνικές για την προστασία της ιδιωτικής ζωής, οι οποίες διασφαλίζουν την αδυναμία σύνδεσης, όταν η βεβαίωση χαρακτηριστικών δεν απαιτεί την ταυτοποίηση του χρήστη.

Τι συνεπάγονται τεχνικά οι εν λόγω απαιτήσεις

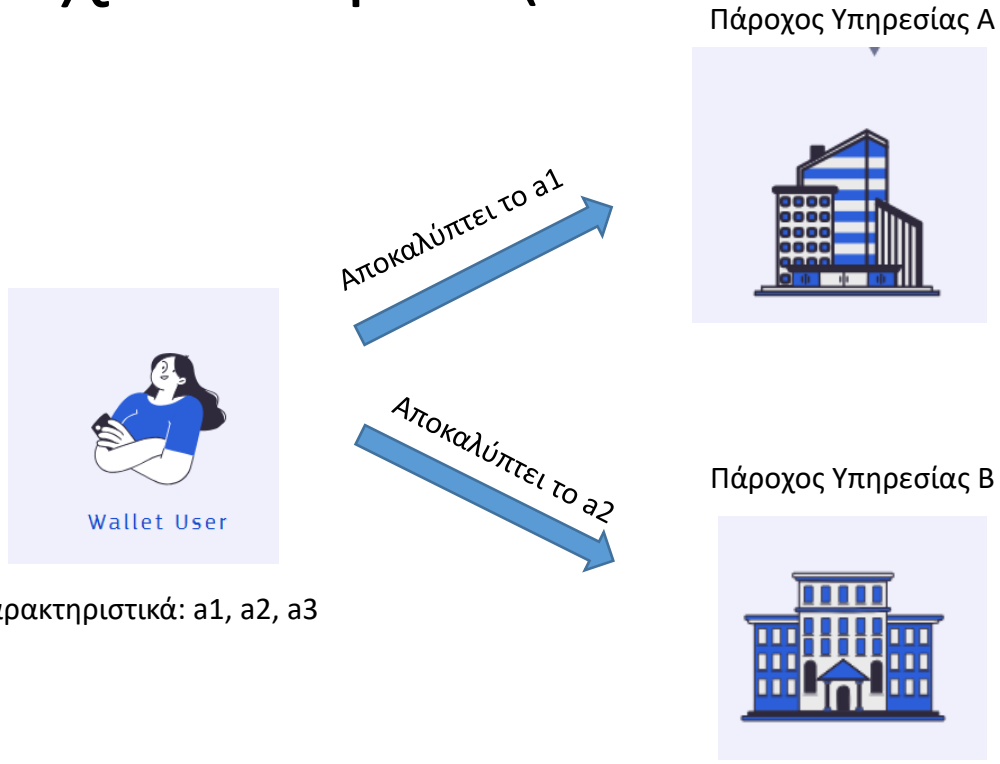
- Επιλεκτικότητα στην γνωστοποίηση δεδομένων: Ο χρήστης πρέπει να μπορεί να αποφασίζει ποια ακριβώς προσωπική του πληροφορία θα διαμοιραστεί
- Μη συνδεσιμότητα (Unlinkability):
  - Εάν ο ίδιος χρήστης αποκαλύψει πληροφορίες του σε δύο διαφορετικές οντότητες, δεν θα πρέπει να προκύπτει ότι οι δύο διαφορετικές αυτές συναλλαγές αφορούν τον ίδιο χρήστη.
  - Μία οντότητα που αποτελεί πηγή δεδομένων ταυτοποίησης - πάροχος βεβαίωσης χαρακτηριστικών (π.χ. άδεια οδήγησης) δεν πρέπει να μαθαίνει σε ποιες άλλες οντότητες αξιοποιούνται (αποστέλλονται ή χρησιμοποιούνται) τα δεδομένα αυτά και για ποιο σκοπό

Τρέχουσα προτεινόμενη κρυπτογραφική τεχνολογία (σε απλοϊκή περιγραφή)



Χαρακτηριστικά: a1, a2, a3

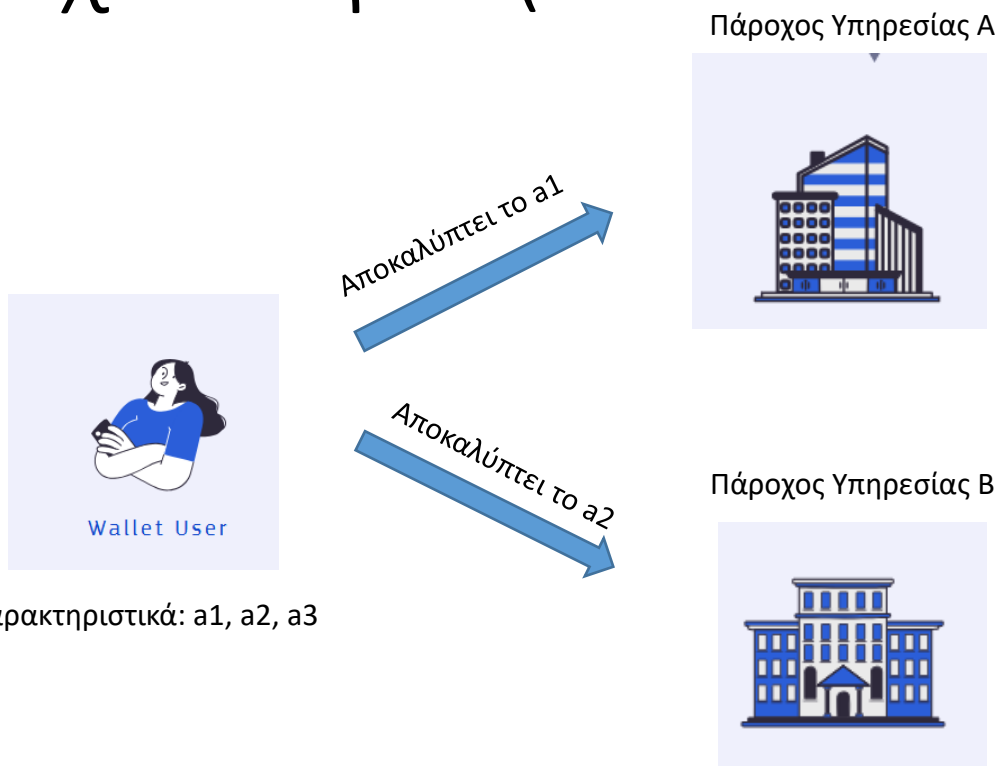
Τρέχουσα προτεινόμενη κρυπτογραφική τεχνολογία (σε απλοϊκή περιγραφή)



Ο πάροχος Α θα συλλέξει (μεταξύ άλλων):

- $d_2 = h(a_2)$, $d_3 = h(a_3)$, όπου το h είναι μία κρυπτογραφική συνάρτηση κατακερματισμού (hash function), άρα μη αναστρέψιμη
- *Μία ψηφιακή υπογραφή S, που εξαρτάται από* τα d_1,d_2,d_3 (όπου $d_1 = h(a_1)$). Μόνο ο κάτοχος των χαρακτηριστικών μπορεί να παράγει μία έγκυρη υπογραφή S

Τρέχουσα προτεινόμενη κρυπτογραφική τεχνολογία (σε απλοϊκή περιγραφή)



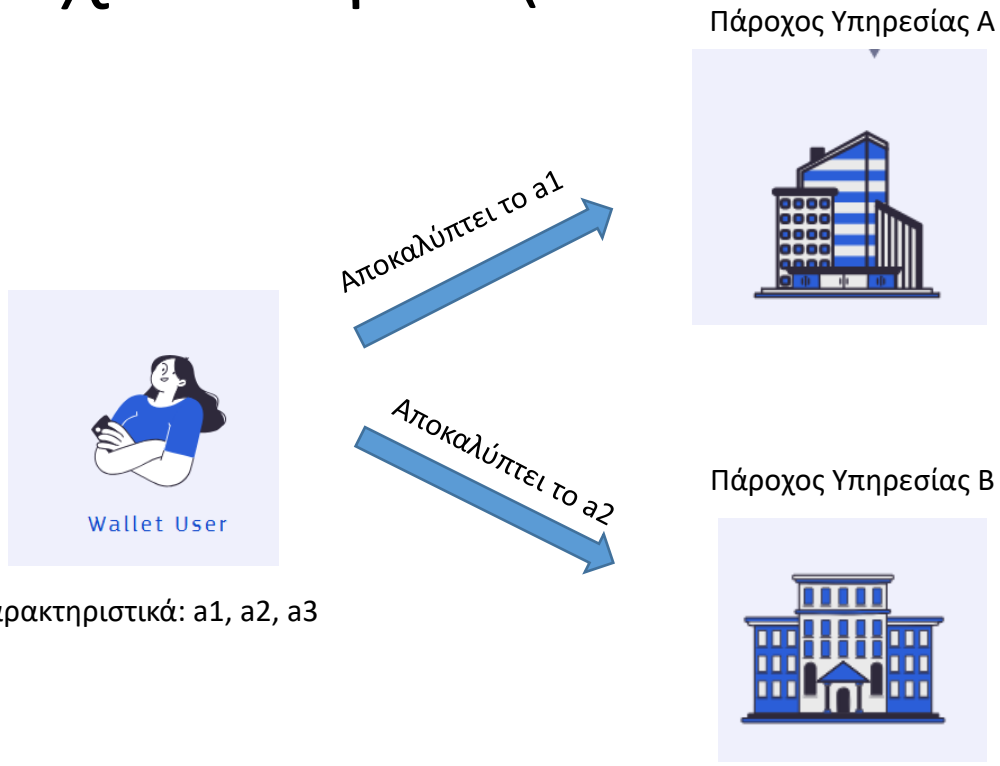
Ο πάροχος Α θα συλλέξει (μεταξύ άλλων):

- $d_2 = h(a_2)$, $d_3 = h(a_3)$, όπου το h είναι μία κρυπτογραφική συνάρτηση κατακερματισμού (hash function), άρα μη αναστρέψιμη
- *Μία ψηφιακή υπογραφή S, που εξαρτάται από* τα d_1,d_2,d_3 (όπου $d_1 = h(a_1)$). Μόνο ο κάτοχος των χαρακτηριστικών μπορεί να παράγει μία έγκυρη υπογραφή S

Ο πάροχος Β θα συλλέξει (μεταξύ άλλων):

- $d_1 = h(a_1)$, $d_3 = h(a_3)$, όπου το h είναι μία κρυπτογραφική συνάρτηση κατακερματισμού (hash function), άρα μη αναστρέψιμη
- *Μία ψηφιακή υπογραφή S, που εξαρτάται από* τα d_1,d_2,d_3 (όπου $d_2 = h(a_2)$). Μόνο ο κάτοχος των χαρακτηριστικών μπορεί να παράγει μία έγκυρη υπογραφή S

Τρέχουσα προτεινόμενη κρυπτογραφική τεχνολογία (σε απλοϊκή περιγραφή)



Ο πάροχος Α θα συλλέξει (μεταξύ άλλων):

- $d_2 = h(a_2)$, $d_3 = h(a_3)$, όπου το h είναι μία κρυπτογραφική συνάρτηση κατακερματισμού (hash function), άρα μη αναστρέψιμη
- *Μία ψηφιακή υπογραφή S, που εξαρτάται από* τα d_1,d_2,d_3 (όπου $d_1 = h(a_1)$). Μόνο ο κάτοχος των χαρακτηριστικών μπορεί να παράγει μία έγκυρη υπογραφή S

Ο πάροχος Β θα συλλέξει (μεταξύ άλλων):

- $d_1 = h(a_1)$, $d_3 = h(a_3)$, όπου το h είναι μία κρυπτογραφική συνάρτηση κατακερματισμού (hash function), άρα μη αναστρέψιμη
- *Μία ψηφιακή υπογραφή S, που εξαρτάται από* τα d_1,d_2,d_3 (όπου $d_2 = h(a_2)$). Μόνο ο κάτοχος των χαρακτηριστικών μπορεί να παράγει μία έγκυρη υπογραφή S

Λόγω της ψηφιακής υπογραφής S, οι δύο πάροχοι μπορούν να ανταλλάξουν πληροφορίες και να διασταυρώσουν ότι πρόκειται για το ίδιο άτομο

Η απλή αυτή περιγραφή είναι εμπνευσμένη από την περιγραφή στο blog του J. Hoepman

Συνέπειες

- Έχουμε δυνατότητα συνδεσιμότητας και, άρα, ιχνηλάτησης (παρακολούθησης) του χρήστη, αλλά και συγκέντρωσης περισσότερων πληροφοριών για αυτόν από ό,τι θα έπρεπε
  - Δεν ικανοποιούνται οι ειδικές απαιτήσεις του άρθρου 5^{α} του Κανονισμού (ΕΕ) 2024/1183
    - Οι οποίες θα μπορούσαν να θεωρηθούν ως ειδική έκφανση της αρχής της ελαχιστοποίησης του άρθρου 5 του ΓΚΠΔ

Παράδειγμα

- Ας υποθέσουμε ότι ένας ενήλικας παίζει διαδικτυακά παιχνίδια και αγοράζει αλκοόλ, χρησιμοποιώντας και στις δύο περιπτώσεις το δίπλωμα οδήγησής του για να αποδεικνύει ότι είναι ενήλικας
  - Δεν αποκαλύπτει όμως το ονοματεπώνυμό του ούτε άλλο στοιχείο ταυτοποίησης (**επιλεκτική γνωστοποίηση δεδομένων)**
- Ο ίδιος ενήλικας ταξιδεύει στο εξωτερικό και χρησιμοποιεί το δίπλωμα οδήγησης ως ταυτοποιητικό έγγραφο
- Όλες οι ανωτέρω δραστηριότητές του μπορούν να συσχετιστούν και να αποδοθούν στο άτομό του αν όλοι οι ανωτέρω φορείς ανταλλάξουν πληροφορίες μεταξύ τους.

Άλλα ζητήματα

- Οι κρυπτογραφικές λύσεις που προτείνονται για υλοποίηση δεν είναι μετα-κβαντικά ασφαλείς
- Γενικότερα, γνωστές προηγμένες κρυπτογραφικές τεχνικές για ενίσχυση της ιδιωτικότητας δείχνουν (προς το παρόν;) να απουσιάζουν
- Ναι μεν ο χρήστης επιλέγει τι πληροφορίες θα διαμοιράσει, ωστόσο πρέπει να ληφθεί υπόψη ότι δεν τίθενται, από το νέο Κανονισμό, πρόσθετες εγγυήσεις ως προς τι πληροφορίες θα ζητούνται από τους παρόχους υπηρεσιών
- … και διάφορα άλλα

Προοπτικές;

- Η ΕΕ, σε επιστολή της το Σεπτέμβριο του 2024 ως απάντηση σε ανοιχτή επιστολή από οργανώσεις, αναφέρει μεταξύ άλλων:
- *«The European Commission is working closely with a team of leading cryptographers in order to integrate into the wallet advanced privacy-enhancing technologies including zero-knowledge proofs. In this context, zero-knowledge-proof verification mechanism which can be implemented in secure hardware using secure cryptographic algorithms will be specifically developed for the wallet. These verification mechanisms would become a default standard in the future, and this will further improve privacy safeguards for the user. The implementing rules include a specific reference to their update in line with technological development».*

Επαλήθευση ηλικίας χρήστη

CALL FOR TENDERS | Publication 16 October 2024

Call for tenders: Development, consultancy and support for an age verification solution

Opening: 15 October 2024

Closing: 18 November 2024

The Commission launches a call for tender to develop an age verification solution

The Commission has made the protection of minors one of its enforcement priorities under the Digital Services Act (DSA) and continues to implement the Better Internet for Kids (BIK+) strategy to support and complement the DSA. Among other initiatives, the Commission is committed to a proportionate and risk-based approach to age verification.

The DSA requires all online platforms to ensure a high level of safety, security and privacy for minors. The DSA imposes specific obligations on very large platforms and very large search engines ("VLOPs" and "VLOSEs") to address substantial risks to minors' well-being. These platforms must mitigate such risks by, for example, **applying a robust age verification policy** for all users, where appropriate.

The Louvain-la-Neuve Declaration calls on the European Commission to integrate tools from the Digital Services Act (DSA) and the European Digital Identity Wallet to ensure robust protections for digital service users in the Union, especially vulnerable groups like minors.

Therefore, a tender for "**Development, consultancy and support for an age verification solution**" was issued on 15 October 2024, with a budget of EUR 4 million, funded by the new amendment to the Digital Europe Programme.

The objective of the call is to develop technical specifications, with input from Member States and other stakeholders, for a privacy-preserving age verification solution. This will allow to verify that a user is aged 18 years or older without sharing any other information about the person. As part of the solution, a generic (white label) application supporting a Zero-Knowledge Proof protocol a feature allowing to verify an attribute is true without disclosing any further details) could be developed and localised and published by Member States in the app stores. It may also be reused for other proofs or verification needs.

Freepic

Contact

DG CONNECT - Communications Networks, Content and Technology / Unit G3 - Accessibility, Multilingualism and Safer Internet

Related topics

Better Internet for Children

Strengthening trust and security

Online platforms and e-commerce

Digital Europe Programme | Funding for Digital

Digital Services Act Package

- Προτείνεται για την επαλήθευση ηλικίας χρήστη, στο πλαίσιο της Πράξης για τις Ψηφιακές Υπηρεσίες (Digital Service Act), αλλά μπορεί να καλύψει και τις σχετικές απαιτήσεις του ΓΚΠΔ
- Κρυπτογραφικά πρωτόκολλα μηδενικής γνώσης (zero-knowledge protocols):
  - Ο χρήστης αποδεικνύει ότι γνωρίζει μία πληροφορία/κατέχει μία ιδιότητα, χωρίς όμως να την αποκαλύπτει
- Πρόκειται κατ' αρχήν για λύση προς την κατεύθυνση ελαχιστοποίησης της πληροφορίας
  - Όμως, χρήζει μεγάλης προσοχής η υλοποίηση
- Τελικά, τα ψηφιακά πορτοφόλια θα καθίστανται υποχρεωτικά;

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Συμπεράσματα - Επίλογος

- Το πορτοφόλι ψηφιακής ταυτότητας μπορεί να αποτελέσει ένα σημαντικότατο «εργαλείο» για πολίτες και οργανισμούς
- Πολύ σημαντικές οι απαιτήσεις προστασίας προσωπικών δεδομένων που προδιαγράφονται στον Κανονισμό (ΕΕ) 2024/1183
  - Ωστόσο, φαίνεται ότι ακόμα υπάρχει «κενό» μεταξύ των προτεινόμενων τεχνολογιών και των “state-of-the-art” λύσεων για προάσπιση ιδιωτικότητας
  - Προηγμένες κρυπτογραφικές τεχνικές θα μπορούσαν να συμβάλλουν στην υλοποίηση των απαιτήσεων για την προστασία δεδομένων
- Θα πρέπει να γίνουν μεγαλύτερες προσπάθειες για «σύζευξη» των νομικών απαιτήσεων με τις πλέον κατάλληλες τεχνολογικές υλοποιήσεις
  - Τα επιχειρήματα της επιστημονικής κοινότητας πρέπει να λαμβάνονται υπόψη
  - Στο πλαίσιο αυτό, δέον είναι να συμβάλλουν από τη δική τους σκοπιά και οι εποπτικές αρχές

Σας ευχαριστώ για την προσοχή σας!