ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

INFORMATION SECURITY
INFOSEC
RESEARCH GROUP @ UOM

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ & ΣΥΣΤΗΜΑΤΩΝ:

Υπηρεσίες Απομακρυσμένης Αυθεντικοποίησης

Ιωάννης Κ. Μαυρίδης
mavridis@uom.gr

MULTIMEDIA SECURITY NETWORKING

Τεχνικές αυθεντικοποίησης χρήστη

- Κάτι που γνωρίζει
  - password/PIN
- Κάτι που κατέχει
  - token
- Κάτι που είναι
  - biometrics
- Κάτι που κάνει
  - actions

Απομακρυσμένη αυθεντικοποίηση πολλαπλών παραγόντων (Multifactor Remote Authentication)

- Όσο περισσότεροι παράγοντες, τόσο πιο ισχυρή η αυθεντικοποίηση, αλλά και πιο υψηλά τα κόστη υλοποίησης και συντήρησης.

- Η ισχυρή απομακρυσμένη αυθεντικοποίηση βασίζεται σε ένα μυστικό κλειδί:
  - που είναι αποθηκευμένο σε ένα hard token
  - και προστατεύεται με ένα συνθηματικό

Τύποι κουπονιών (token)

- Password / PIN
  - με συμβατικό πρωτόκολλο
- One – Time Password (OTP)

  - Συσκευή με οθόνη (συνδυασμός κλειδιού, χρονοσφραγίδας και απαριθμητή) - FIPS 140-2 level 1
  - Κανάλι out-of-band (π.χ. SMS)
- Soft Token
  - κρυπτογραφικό κλειδί αποθηκευμένο σε δίσκο με προστασία password - FIPS 140-2 Level 1
- Hard Token

  - κρυπτογραφικό κλειδί μέσα σε συσκευή ασφαλείας
  - προστασία με password / biometrics
  - αδύνατη η εξαγωγή κλειδιού από τη συσκευή
  - FIPS 140-2 level 2

Πρωτόκολλο απομακρυσμένης αυθεντικοποίησης

- Είναι μια καθορισμένη ακολουθία μηνυμάτων μεταξύ διεκδικούντος (Claimant) και επιβεβαιώνοντος (Verifier) που:
  - αποδεικνύει ότι ο Claimant κατέχει ένα νόμιμο token για να αποδεικνύει την ταυτότητά του
  - Και, προαιρετικά, αποδεικνύει στον Claimant ότι επικοινωνεί με τον σκοπούμενο Verifier.
- Βασίζεται στην απόδειξη κατοχής (proving possession - PoP) ενός token
- Με την προϋπόθεση ότι ο χρήστης μπορεί να κρατήσει μυστικό ένα: ιδιωτικό ή μυστικό κλειδί ή Password ή PIN

Κίνδυνοι για πρωτόκολλα αυθεντικοποίησης

- Eavesdroppers
- Password guessing / cracking
- Replay / playback
- Hijackers
- Impersonation
- Man-in-the-middle

Επίπεδο διασφάλισης αυθεντικοποίησης

- Για την επιτυχή υλοποίηση μιας υπηρεσίας eGov, πρέπει να αποφασιστεί το απαιτούμενο επίπεδο διασφάλισης.
- Περιγράφει το βαθμό βεβαιότητας του οργανισμού για το ότι ο χρήστης παρουσίασε ένα διαπιστευτήριο (credential) που αναφέρεται στην ταυτότητά του.

Διασφάλιση (assurance)

- ο βαθμός εμπιστοσύνης για τη διαδικασία εξέτασης της ταυτότητας αυτού για τον οποίο εκδόθηκε το credential

και

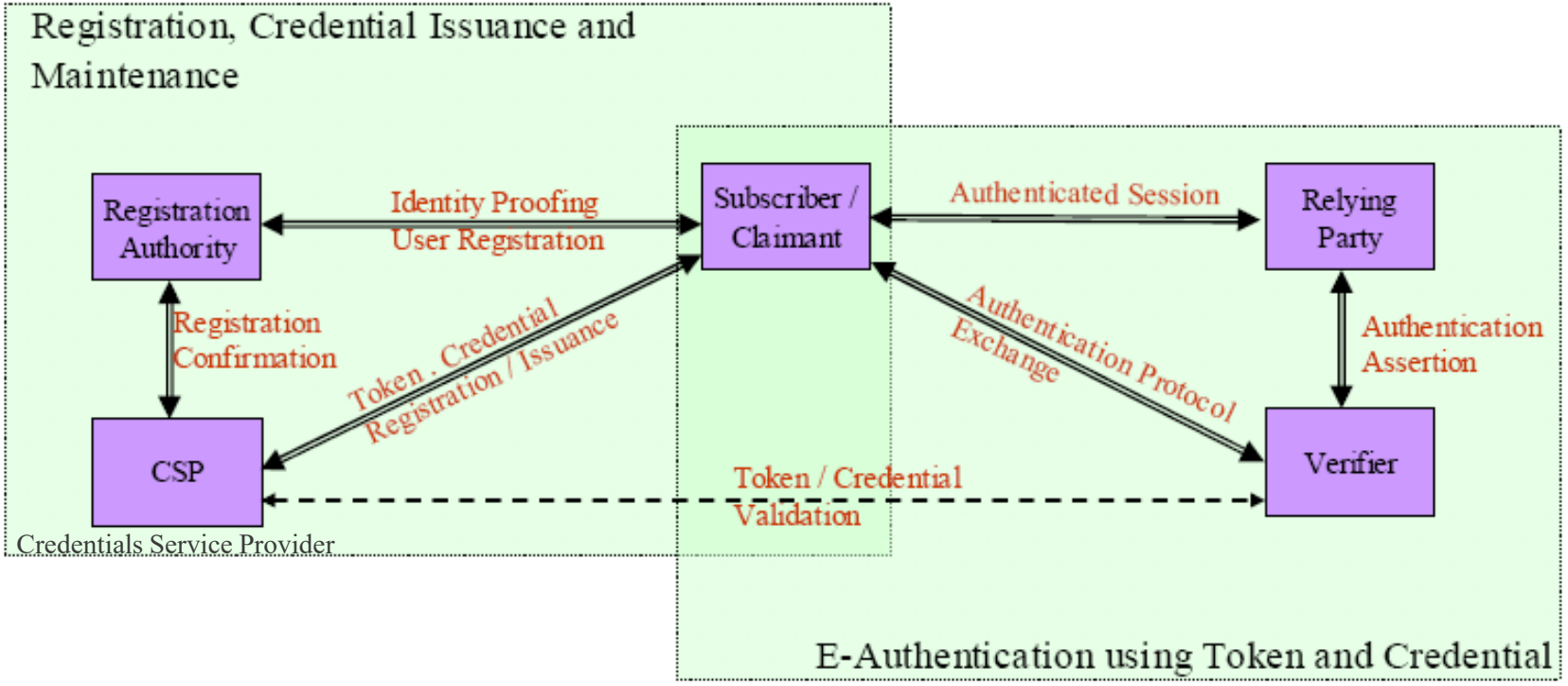
- ο βαθμός εμπιστοσύνης για το ότι αυτός που χρησιμοποιεί το credential είναι αυτός για τον οποίο εκδόθηκε

US E-Authentication

- OMB Memorandum M-04-04
  - E-Authentication Guidance for Federal Agencies, 2003
    - http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
- NIST Electronic Authentication Guidelines
  - SP 800-63-3 suite (Digital Identity Guidelines)

NIST: National Institute of Standards and Technology
OMB: Office of Management and Budget

e-Authentication: αρχιτεκτονικό μοντέλο



Proof of Possession (PoP)

OMB επίπεδα διασφάλισης

- Επίπεδο1: μικρή ή καθόλου εμπιστοσύνη
- Επίπεδο 2: κάποια εμπιστοσύνη
- Επίπεδο 3: υψηλή εμπιστοσύνη
- Επίπεδο 4: πολύ υψηλή εμπιστοσύνη

Τύπος token ανά επίπεδο

Allowed Token Types	*Assurance Levels* 1	2	3	4
Hard token	√	√	√	√
Soft token	√	√	√	
1TPD	√	√	√	
Password	√	√		

Προστασία ανά επίπεδο

	Assurance Levels			
Protection Against	1	2	3	4
Replay	√	√	√	√
On-line guessing	√	√	√	√
Eavesdropper		√	√	√
Verifier impersonation			√	√
Man-in-the-middle			√	√
Session hijacking				√

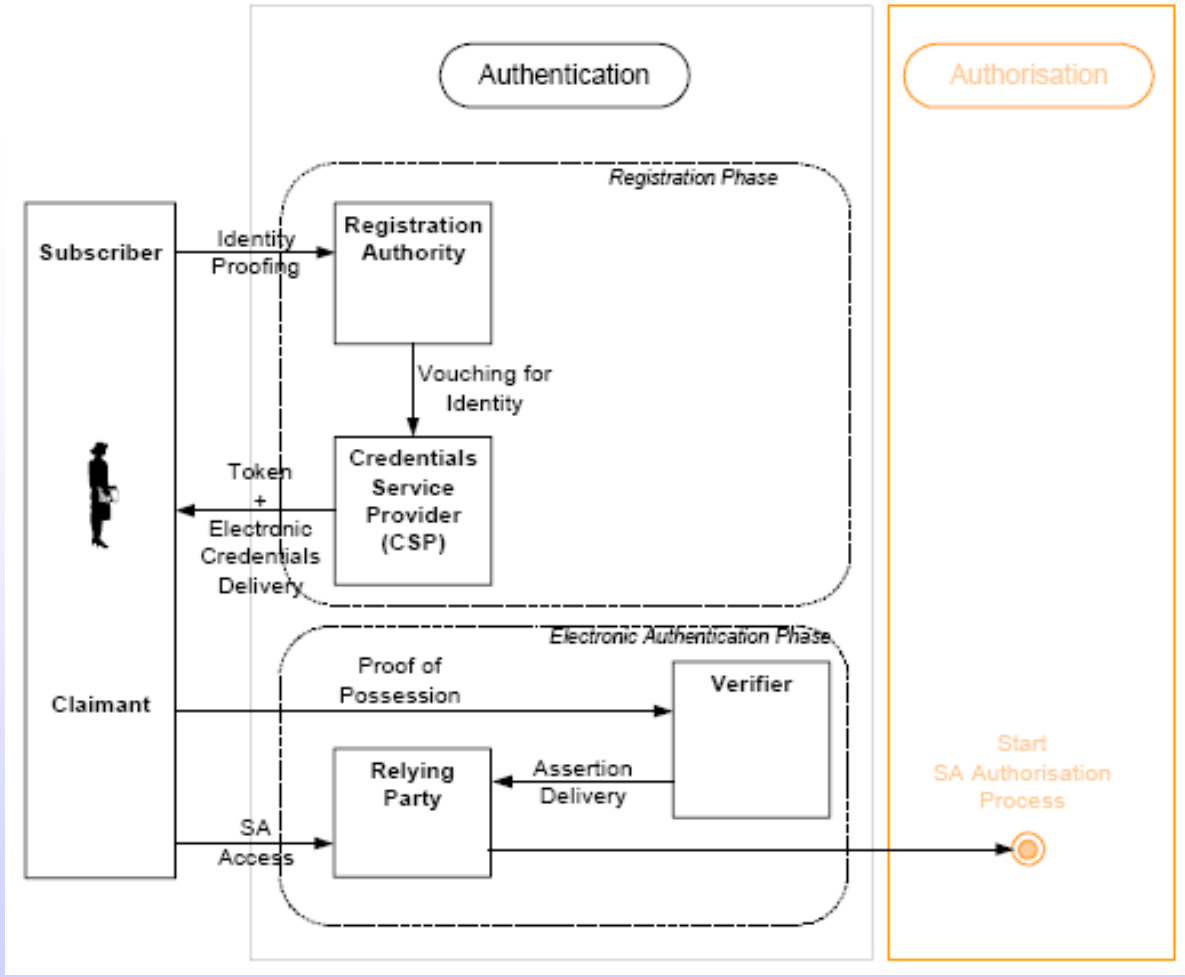
Τύπος πρωτοκόλλου αυθεντικοποίησης ανά επίπεδο

	Assurance Levels			
Authentication Protocol Types	1	2	3	4
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
Tunneled password	√	√		
Challenge-reply password	√			

E-Auth Guidance Process

- Εκτίμηση επικινδυνότητας (risk assessment)
  - Electronic Risk and Requirements Assessment (E-RA): μεθοδολογία και εργαλείο
- Αντιστοίχιση επικινδυνοτήτων με το κατάλληλο επίπεδο διασφάλισης
  - OMB M0404-0404 Guidance
- Επιλογή κατάλληλων τεχνολογικών λύσεων
  - NIST SP800-63 Guidance
- Επικύρωση του υλοποιημένου συστήματος
  - NIST SP800-53A, SP800-37
- Περιοδική Επανεκτίμηση
  - NIST SP800-53A

EU: Interchange of Data between Administrations (IDA)



Μοντέλο Αναφοράς Διαδικασίας Αυθεντικοποίησης (Authentication Process Reference Model)

IDA επίπεδα διασφάλισης

- Επίπεδο1: Ελάχιστη διασφάλιση
- Επίπεδο 2: Χαμηλή διασφάλιση
- Επίπεδο 3: Επαρκής διασφάλιση
- Επίπεδο 4: Υψηλή διασφάλιση

Τύποι token ανά επίπεδο

	Assurance Levels			
Allowed Token Types	1	2	3	4
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
One-time password device token	√	√		
Password or PIN token	√			

Πρωτόκολλα αυθεντικοποίησης ανά επίπεδο

	Assurance Levels			
Allowed Protocol Types	1	2	3	4
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
One-time (or strong) Password PoP	√	√	√	
Tunneled password PoP	√	√		
Challenge-reply password PoP	√			

Απαιτούμενη προστασία ανά επίπεδο

	Assurance Levels			
Protection Against	1	2	3	4
Replay	√	√	√	√
On-line guessing	√	√	√	√
Eavesdropper		√	√	√
Verifier impersonation			√	√
Man-in-the-middle			√	√
Session hijacking			√	√

Μηχανισμοί βεβαίωσης

- για την επικοινωνία των αποτελεσμάτων μιας απομακρυσμένης αυθεντικοποίησης σε τρίτα μέρη

	Assurance Levels			
Expiration time	1	2	3	4
Immediate	√	√	√	√
2 hours	√	√	√	
12 hours	√	√		
24 hours	√			

Ανάπτυξη μιας κατάλληλης e-Gov πολιτικής αυθεντικοποίησης

Βήμα 1: Διεξαγωγή μιας γρήγορης εκτίμησης επικινδυνότητας στο σύστημα εφαρμογών

Βήμα 2: Αντιστοίχιση επικινδυνοτήτων με το εφαρμόσιμο επίπεδο διασφάλισης αυθεντικοποίησης

Βήμα 3: Επιλογή κατάλληλων διαδικασιών και τεχνολογιών

Βήμα 4: Υπογραφή Συμφωνητικού Αμοιβαίας Αναγνώρισης μεταξύ των συμμετεχόντων μερών

Βήμα 5: Επικύρωση της επίτευξης του απαιτούμενου επιπέδου διασφάλισης από το υλοποιημένο σύστημα

Βήμα 6: Περιοδική επανεκτίμηση του συστήματος για πιθανή επικαιροποίηση των τεχνολογικών απαιτήσεων

Διαχείριση Επικινδυνότητας

Το αποδεκτό επίπεδο επικινδυνότητας εξαρτάται από:

- Assets (data) valuation
- Correct Identification of Risks
- Potential Damages
- Overall Likelihood Rating
- Impact Severity Scaling
- Measure of Risks by Level:

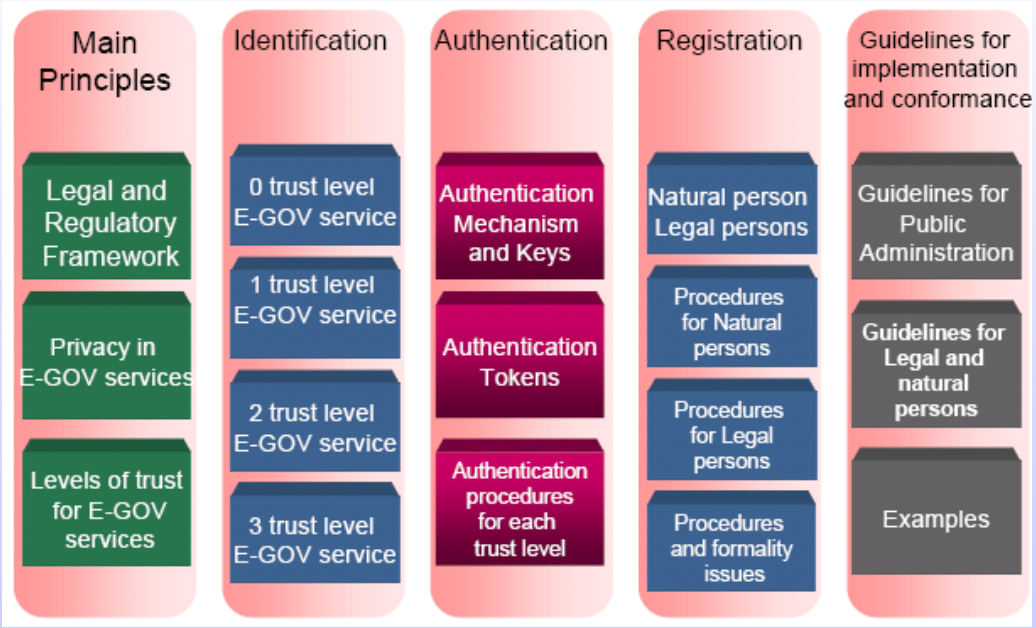
IDA Reference Matrix

		Impact of damages				
	Likelihood	Very High	High	Medium	Low	Negligible
Risk i	Almost certain	(1)	(1)	Level 4	Level 3	Level 3
	Likely	(1)	Level 4	Level 3	Level 3	Level 2
	Moderate	Level 4	Level 3	Level 3	Level 2	Level 2
	Unlikely	Level 3	Level 3	Level 2	Level 2	Level 1
	Rare	Level 3	Level 2	Level 2	Level 1	Level 1

(1):Not applicable to remote authentication over open networks

Πλαίσιο Ψηφιακής Αυθεντικοποίησης

- παρέχει οδηγίες για αναγνώριση και αυθεντικοποίηση χρηστών για υπηρεσίες ηλεκτρονικής διακυβέρνησης



Εγκεκριμένες μέθοδοι αυθεντικοποίησης για υπηρεσίες e-gov

- Passwords
- One-Time Passwords (OTP)
- Soft Digital Certificates
- Hard Digital Certificates

Αντιστοίχιση επιπέδων και μηχανισμών

Trust level	Registration level	Authentication level	Authentication mechanism
0	0	0	-
1	1	1	Passwords
2	2		OTP
3	3	2	Soft digital certificates
			Hard digital certificates

ΠΨΑ - Βασικές αρχές

- Επιλογή των κατάλληλων μηχανισμών αυθεντικοποίησης και διαδικασιών εγγραφής και ταυτοποίησης χρηστών
  - Κατηγοριοποίηση των δεδομένων που επεξεργάζονται οι ηλεκτρονικές υπηρεσίες με βάση την προστασία της ιδιωτικότητας.
  - Καθορισμός Επιπέδων Εμπιστοσύνης (ΕΕ) για τις ηλεκτρονικές υπηρεσίες, με βάση την κατηγορία των δεδομένων και τις πιθανές επιπτώσεις σε περίπτωση μη ορθής λειτουργίας της υπηρεσίας.
  - Συσχέτιση κάθε ΕΕ με κατάλληλα Επίπεδα Αυθεντικοποίησης (ΕΑ)
  - Συσχέτιση κάθε ΕΑ με κατάλληλες Διαδικασίες Εγγραφής (ΔΕ) χρηστών.

Εφαρμογή ΠΨΑ

1. Απλή πληροφόρηση
2. Ηλεκτρονικές Φόρμες
3. Ηλεκτρονική Αίτηση
4. Πλήρης συναλλαγή

Επίπεδα Ολοκλήρωσης Υπηρεσιών ΗΔ (4)

Επίπεδα Ιδιωτικότητας Πληροφοριών (3)

0. Δημόσια Διαθέσιμα Δεδομένα
1. Προσωπικά Δεδομένα
2. Ευαίσθητα Δεδομένα

Επίπεδα Εμπιστοσύνης (4)

1.Προσπέλαση Δημόσιων Δεδομένων
2.Δεδομένα μικρής κρισιμότητας
3. Προσωπικά Δεδομένα
4. Ευαίσθητα Δεδομένα

Επίπεδα Αυθεντικοποίησης (3)

0. Καμία αυθεντικοποίηση
1. Συνθηματικά χρηστών
2. **Ψηφιακά Πιστοποιητικά**

Μηχανισμοί Ταυτοποίησης Χρηστών (3)

1. Ανά Υπηρεσία
2. Μέσω Ερμή, χωρίς αποθήκευση
3. Ερμής, με αποθήκευση

Όχι Μοναδικό Αναγνωριστικό

Μηχανισμοί Εγγραφής Οντοτήτων (3)

1. Φυσικά Πρόσωπα (3 επίπεδα)
2. ΝΠΔΔ
3. ΝΠΙΔ