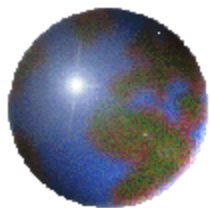


# **Medical Information Systems Security: Memories from the Future**

**Dimitris Gritzalis**

**March 2006**

1<sup>ο</sup> Πανελλήνιο Συνέδριο για την Υγεία και τα Προσωπικά Δεδομένα  
Εθνικό Ιδρυμα Ερευνών  
Αθήνα, 28-29 Μάρτη 2006

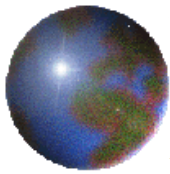


# Ασφάλεια Πληροφοριακών Συστημάτων Υγείας Εμπειρίες από το ...μέλλον

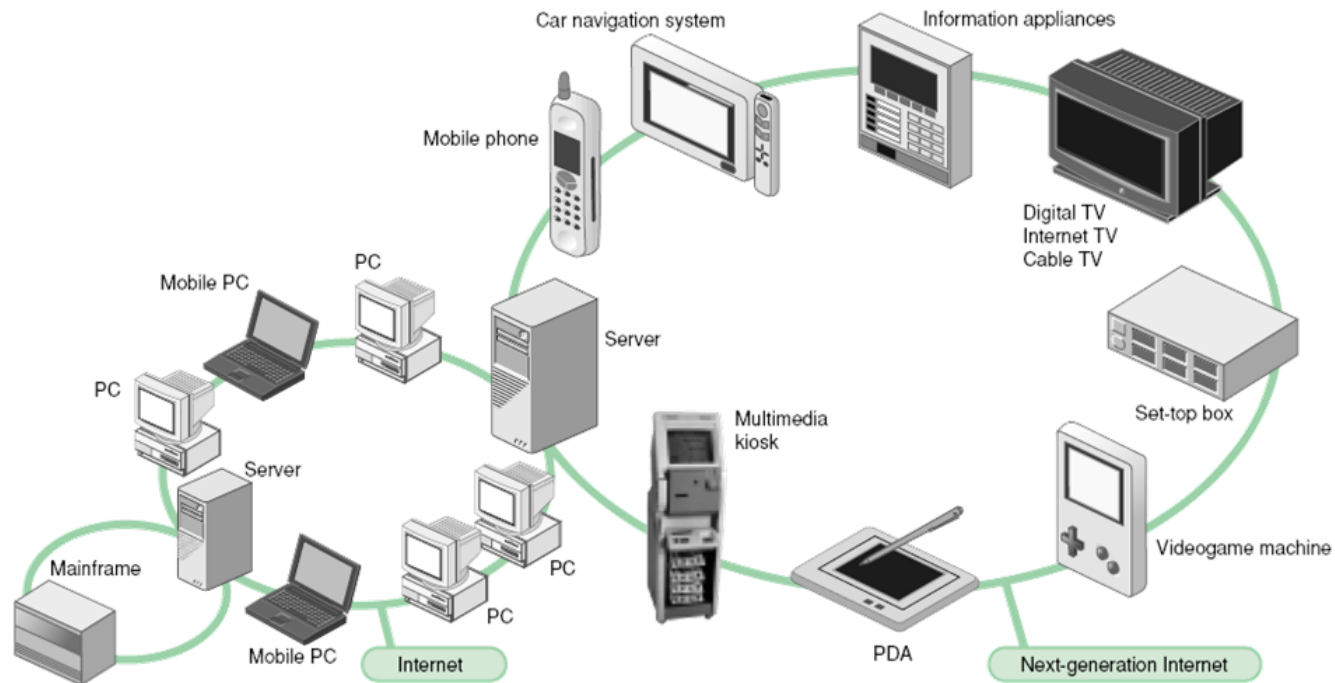
**Δημήτρης Γκρίτζαλης ([dgrit@aub.gr](mailto:dgrit@aub.gr), [www.cis.aub.gr](http://www.cis.aub.gr))**

Αναπλ. Καθηγητής Ασφάλειας στην Πληροφορική και τις Επικοινωνίες

Ερευνητική Ομάδα Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών  
Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών



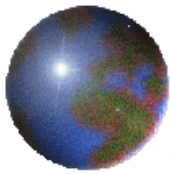
# Απανταχού Υπολογίσεις (UbiComp)



“Το υψηλότερο ιδανικό της **συγκλονιστικής** μηχανής είναι να γίνει ο υπολογιστής τόσο συναρπαστικός, τόσο εκπληκτικός, τόσο ενδιαφέρων, ώστε να μη θέλουμε να υπάρξουμε χωρίς αυτόν”.

“Το υψηλότερο ιδανικό της **αόρατης** μηχανής είναι να γίνει ο υπολογιστής τόσο ταιριαστός, τόσο φυσικός, τόσο προφανής, ώστε να τον αξιοποιούμε χωρίς καν να το συνειδητοποιούμε”.

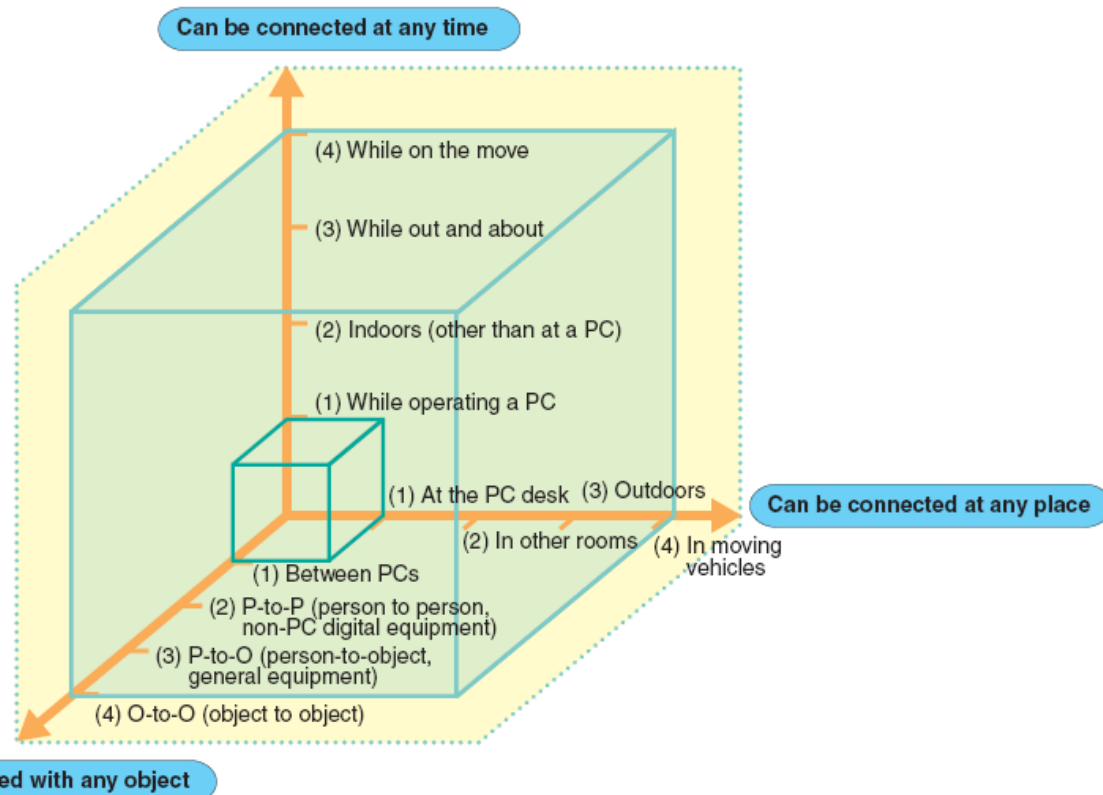
Ο Wieser αποκάλεσε την ιδέα αυτή **Απανταχού Υπολογίσεις (Ubiquitous Computing)**.



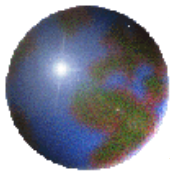
# Οι “διαστάσεις” του Απανταχού Υπολογίζεин

...υπονοεί ένα ενιαίο περιβάλλον υπολογιστικών συσκευών, προηγμένης δικτυακής τεχνολογίας και διεπαφών, που μπορεί να αντιλαμβάνεται τα ιδιαίτερα χαρακτηριστικά της ανθρώπινης παρουσίας και προσωπικότητας, να ικανοποιεί ανάγκες, να αντιδρά έξυπνα σε εκφράσεις επιθυμίας (λεκτικές ή κινητικές) και μπορεί να συμμετέχει ακόμα και σε ευφυή διάλογο [ISTAG, 2001].

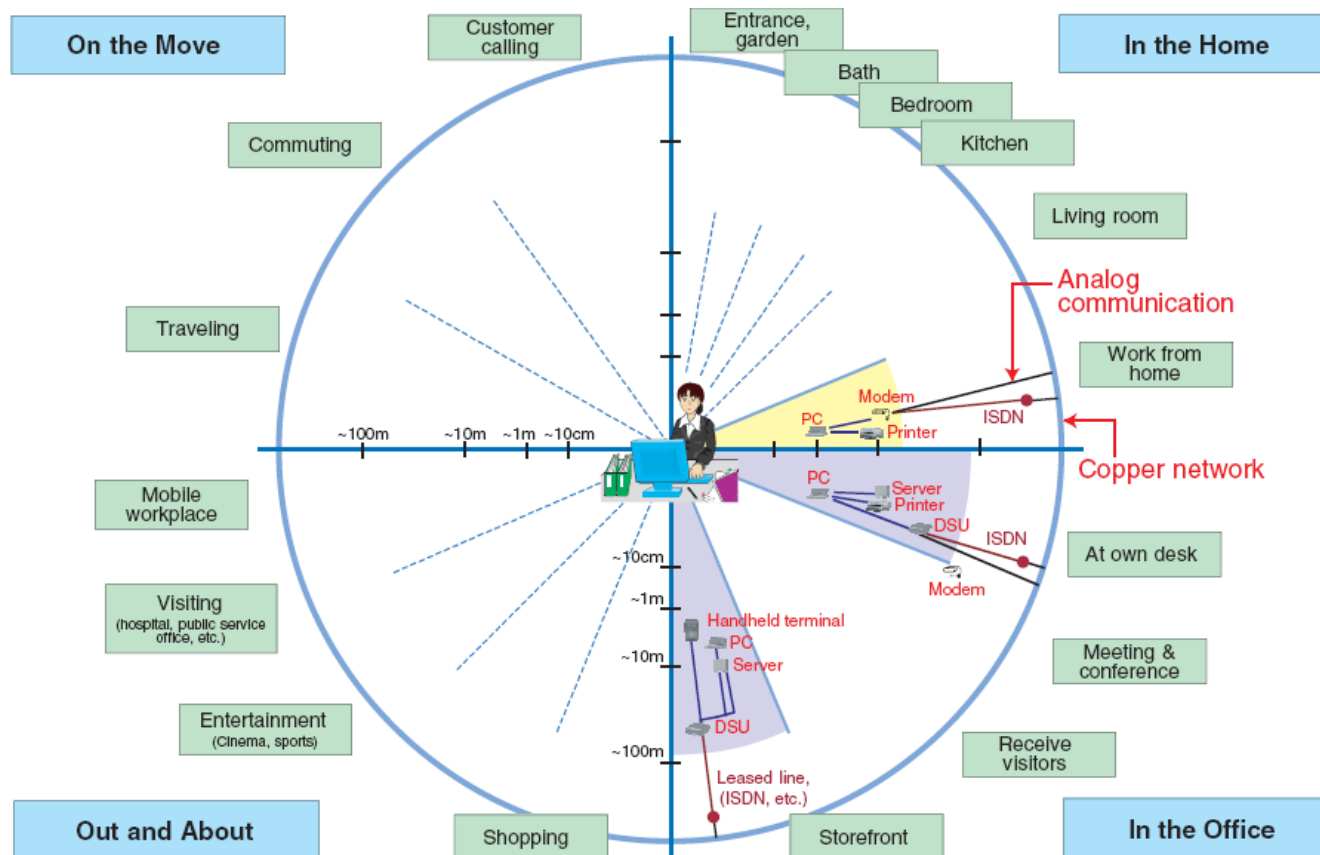
...αφορά τη σύγχρονη τάση προς πολύ-άριθμες, εύκολα προσβάσιμες και συχνά αόρατες υπολογιστικές συσκευές, συχνά ασύρματες ή ενσωματωμένες στο περιβάλλον και συνδεδεμένες σε ένα δίκτυο [NIST, 2001].



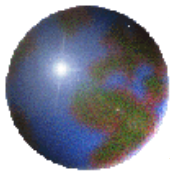
... εξασφαλίζει διασύνδεση οπουδήποτε, οποτεδήποτε και για τον οποιοδήποτε ή το ο,τιδήποτε [ITU, 2006].



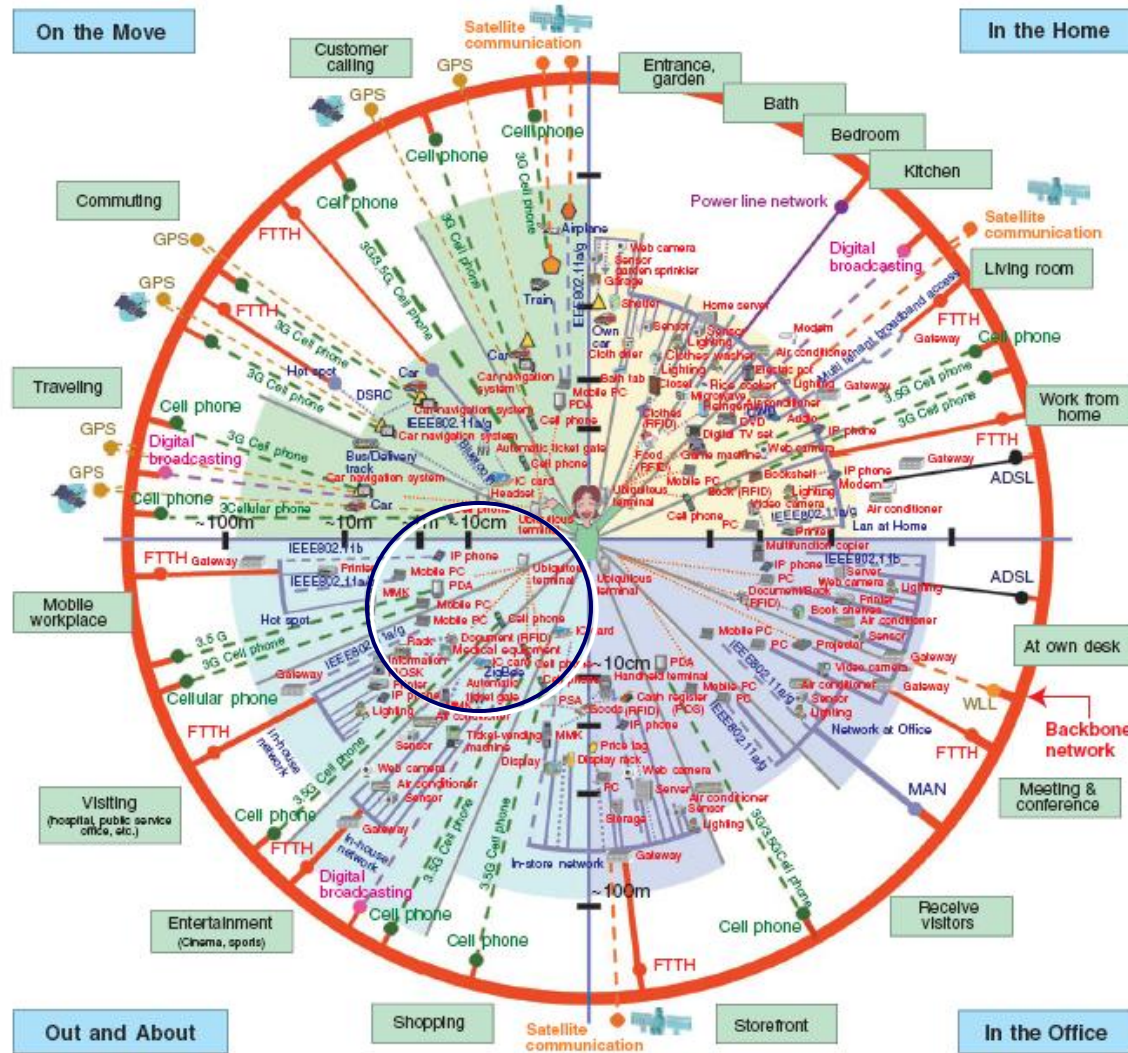
# Από το Δικτυακό Υπολογίζουν (Παράδειγμα -)

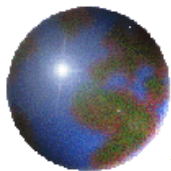


Note: DSU = digital service unit (a device to connect terminal equipment to digital circuits).

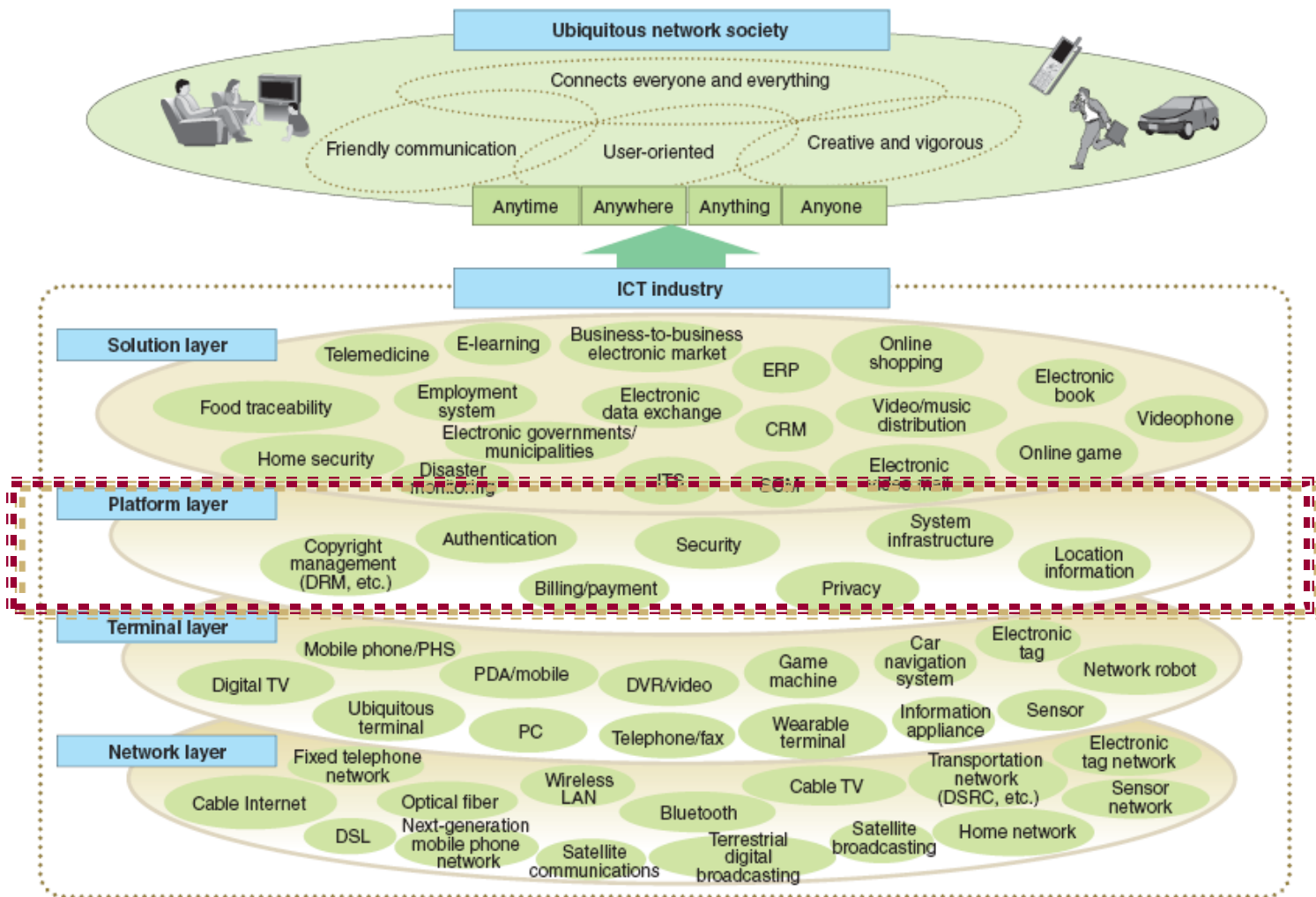


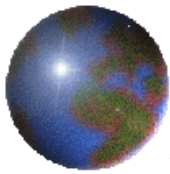
# Στο Απανταχού Υπολογίζεин (Παράδειγμα +)



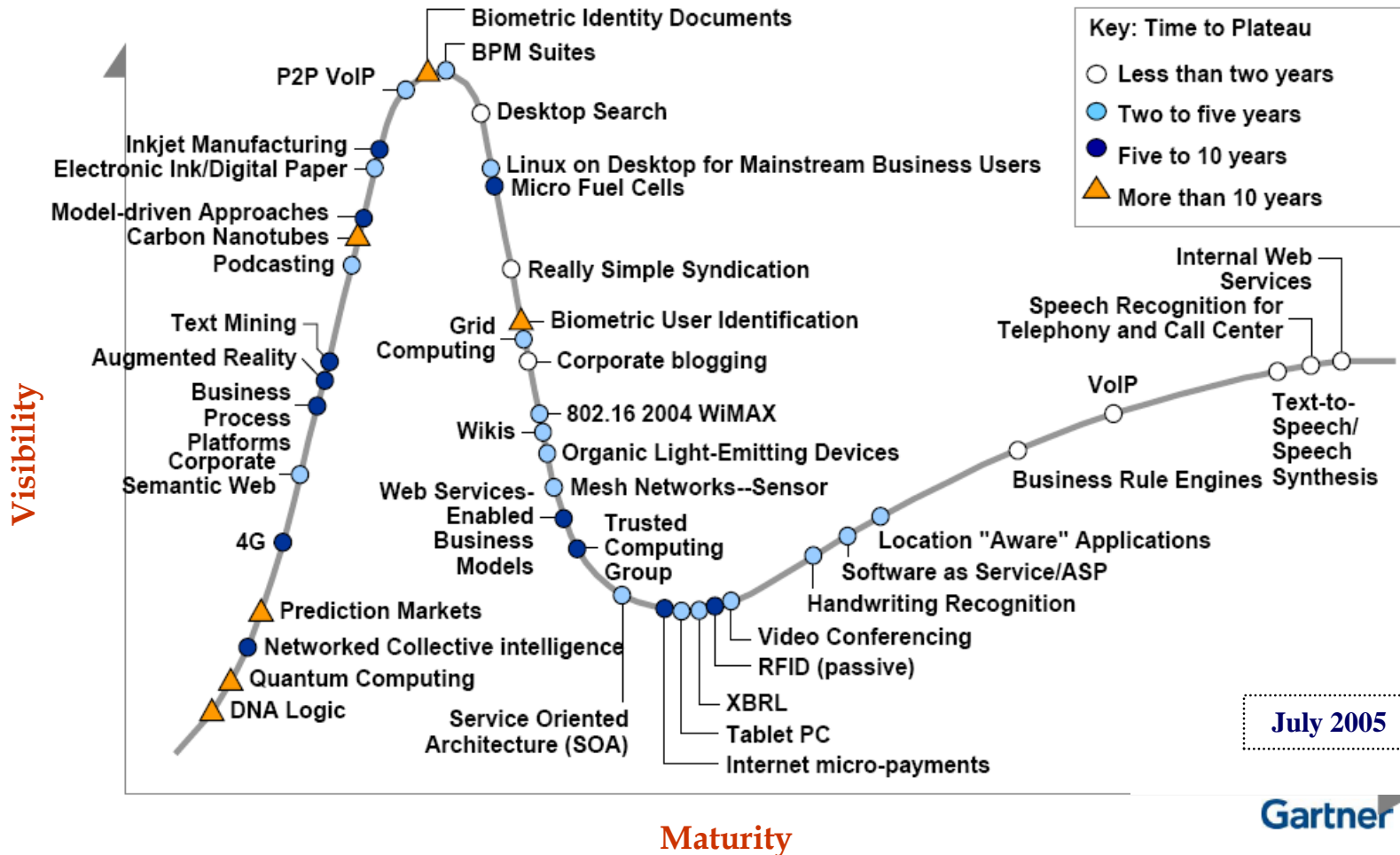


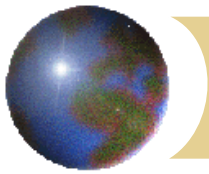
# Δομική Διαστρωμάτωση και Ασφάλεια





# Τεχνολογίες Ασφάλειας

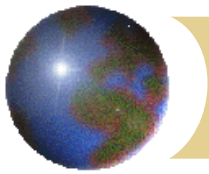




## Εφαρμογές στην Υγεία

**Απανταχού Ιατρική Φροντίδα** (Ubiquitous Healthcare): Αναφέρεται στην παροχή ηλεκτρονικών υπηρεσιών υγείας, οπουδήποτε, οποτεδήποτε και σε οποιονδήποτε, κυρίως με αξιοποίηση των ευρυζωνικών και ασύρματων τεχνολογιών.

<b>Διαχείριση Υγείας και Τηλεϊατρική</b>	Έλεγχος υγείας (checkup) στο σπίτι, Υγεία κατά την άσκηση, Ανάλυση γευμάτων, Επικοινωνία με το θεράποντα ιατρό, Λήψη δεύτερης διάγνωσης κλπ.
<b>Φροντίδα για ασθενείς και άτομα με ειδικές ανάγκες</b>	Επιγραμμής παρακολούθηση φυσικής κατάστασης, Απομακρυσμένη παρακολούθηση χώρου, Ιατρική παρακολούθηση ασθενών με χρόνια νοσήματα (διαβήτης, υπέρταση, καρδιακά νοσήματα), Μετεγχειρητική παρακολούθηση κλπ.
<b>Επείγουσα Βοήθεια</b>	Ειδοποίηση επείγουσας βοήθειας είτε αυτόματα είτε με πρωτοβουλία του ασθενούς κλπ.
<b>Υπηρεσίες οικιακής φροντίδας</b>	Περιβαλλοντικός έλεγχος, Έλεγχος θερμοκρασίας και υγρασίας, Παρακολούθηση περιστατικών κατά τη διάρκεια της νύχτας, Πρόληψη πυρκαγιάς και ατυχημάτων κλπ.

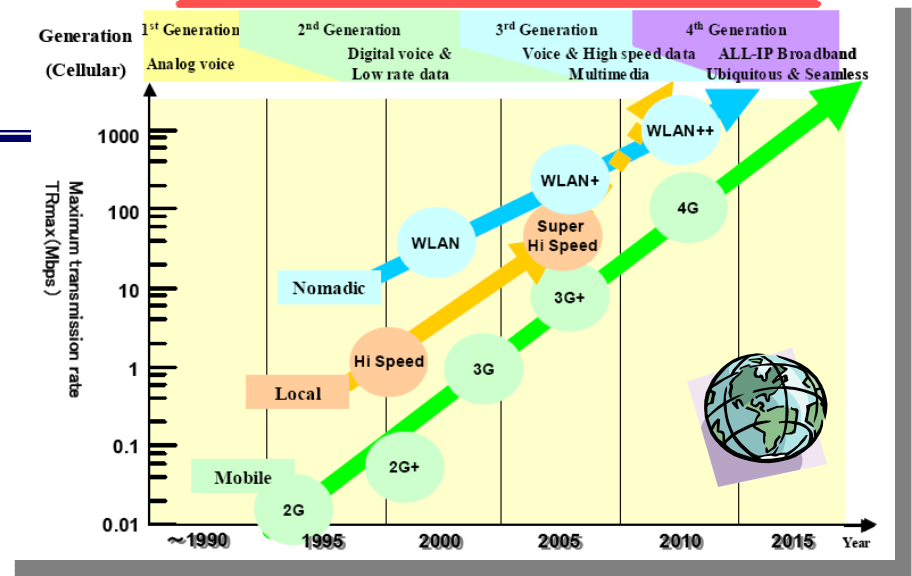


# Broadband - Mobile

Η Ιαπωνία και η Ν. Κορέα επιδιώκουν να αξιοποιήσουν συστηματικά τις εφαρμογές ευρείας ζώνης, με έμφαση στην Υγεία.

Η Ευρώπη επιδιώκει να αξιοποιήσει τις εφαρμογές των Ασύρματων και Κινητών Επικοινωνιών και στην Υγεία.

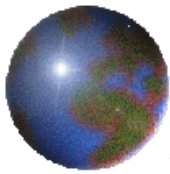
Οι ΗΠΑ επιδιώκουν την ασφάλεια τόσο του φυσικού χώρου, όσο και του κυβερνοχώρου.



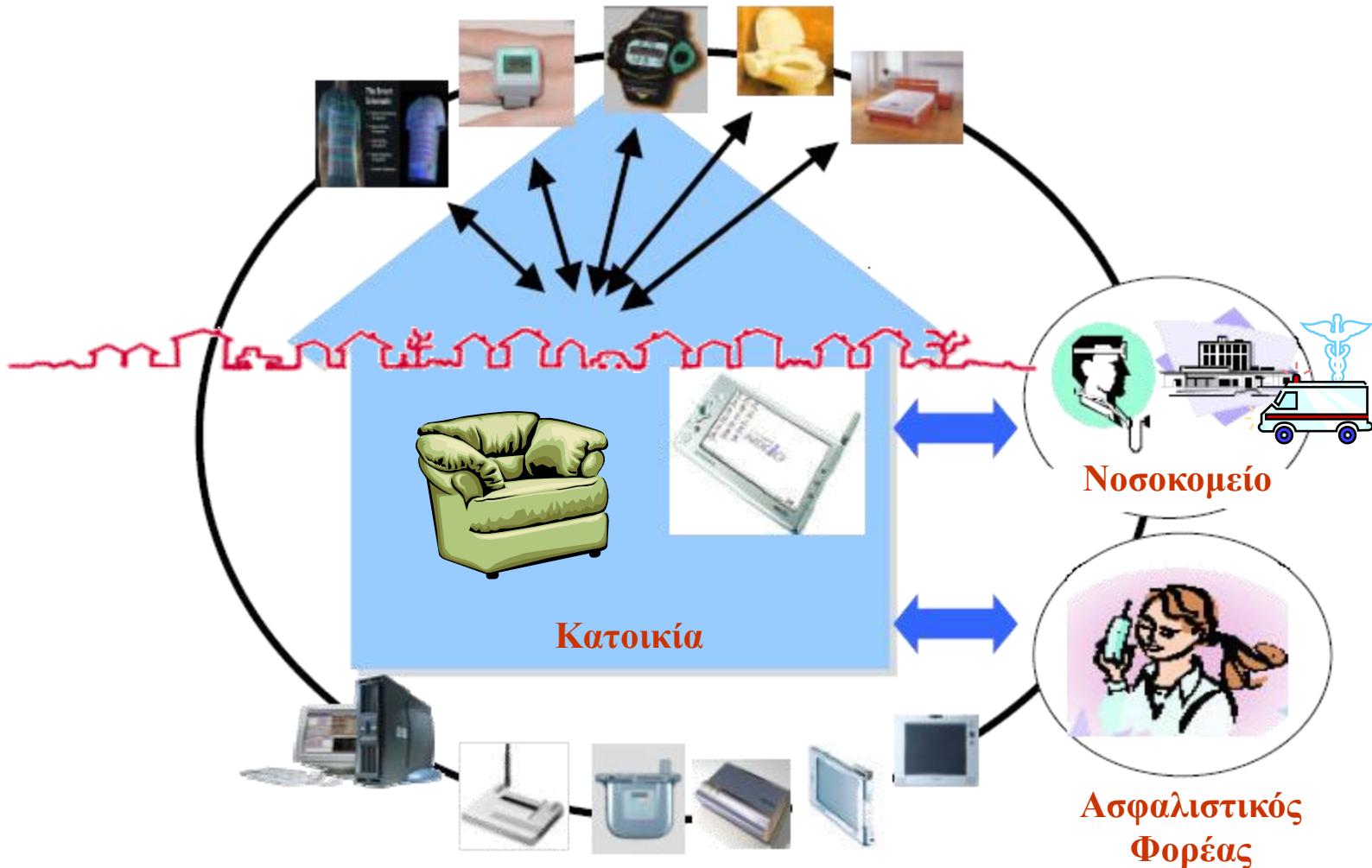
Economy	Mobile Market			Broadband Market			
	Subscr's (M)	Penetrator (%)	As % Internet subscr's (M)	Subscr's (M)	Penetrator (%)	3G <sup>1</sup> mobile subscr's (M)	
China	334.8	25.5	8.71	<sup>2</sup> 1.51	<sup>2</sup> 21.30	<sup>2</sup> 60.3	
Japan	91.5	71.6	25.70	19.10	14.90	56.4	
Korea (Rep.)	36.6	76.1	27.51	11.92	24.90	99.1	
Russia	74.4	51.6	0.18	1.24	0.87	*	
United States	181.1	61.0	49.50	37.89	12.80	59.5	
European Union	France	44.6	73.7	0.04	6.75	11.20	56.6
	Germany	71.3	86.4	0.25	6.90	8.40	*
	UK	61.1	102.8	2.83	6.26	10.50	39.6

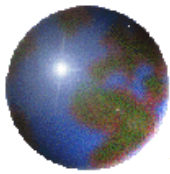
<sup>1</sup> 3G mobile refers to services using CDMA 2000 1x, CDMA 1x EV-DO and W-CDMA standards. <sup>2</sup> Data refer to Hong Kong (China). \* Not referred to in the reviewed ITU and OECD reports.

Στα ελληνικά νοσοκομεία, η δυνατότητα περιήγησης στο Internet ή χρήσης προσωπικού ηλεκτρονικού ταχυδρομείου συχνά δεν είναι δυνατή, ενώ αντίγραφα των βάσεων δεδομένων τους ενίοτε τηρούνται σε ιδιωτικές εταιρείες.

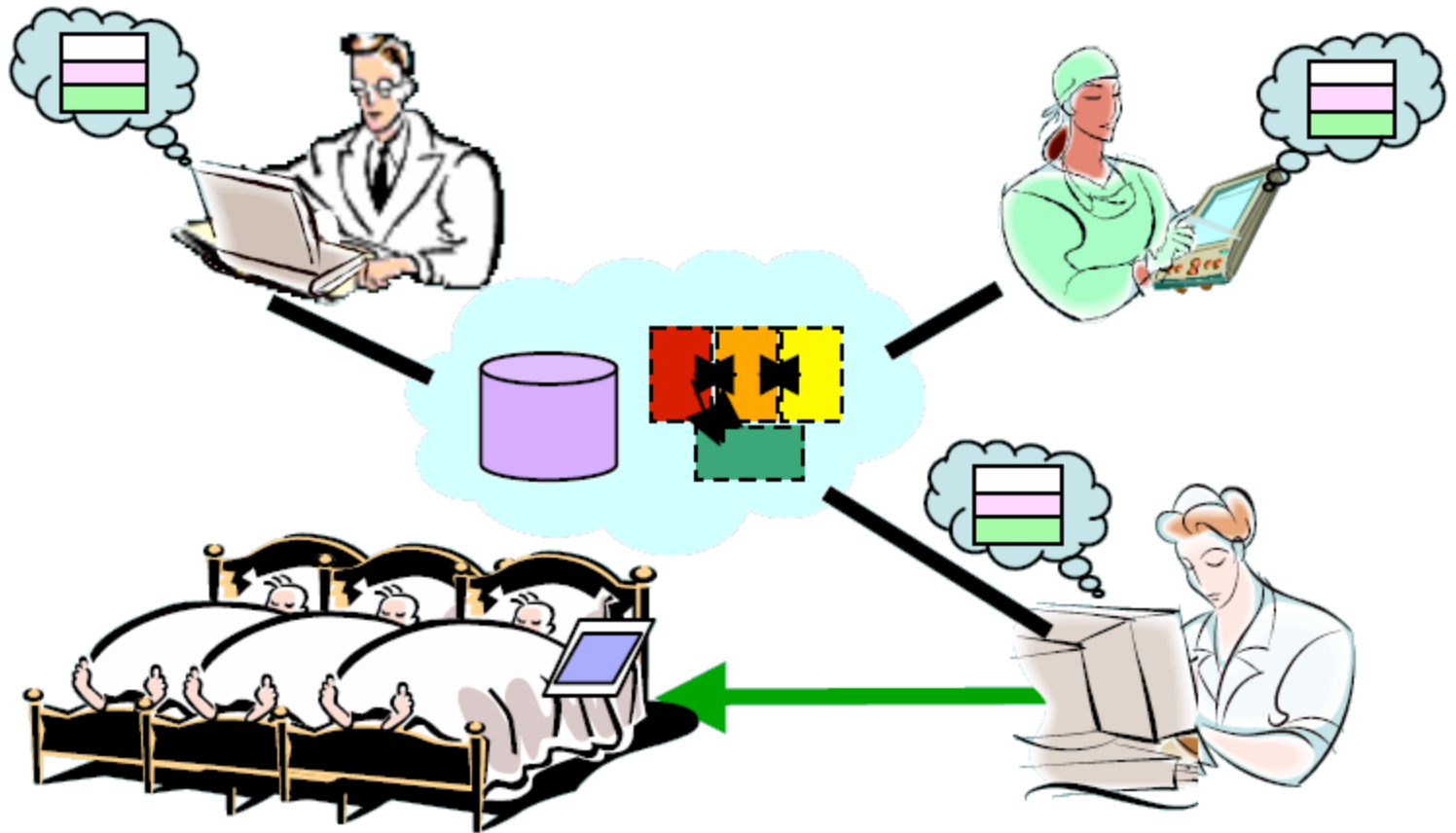


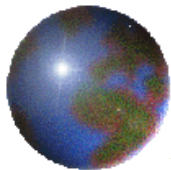
# Σενάριο I: Καρδιακή προσβολή στο σπίτι



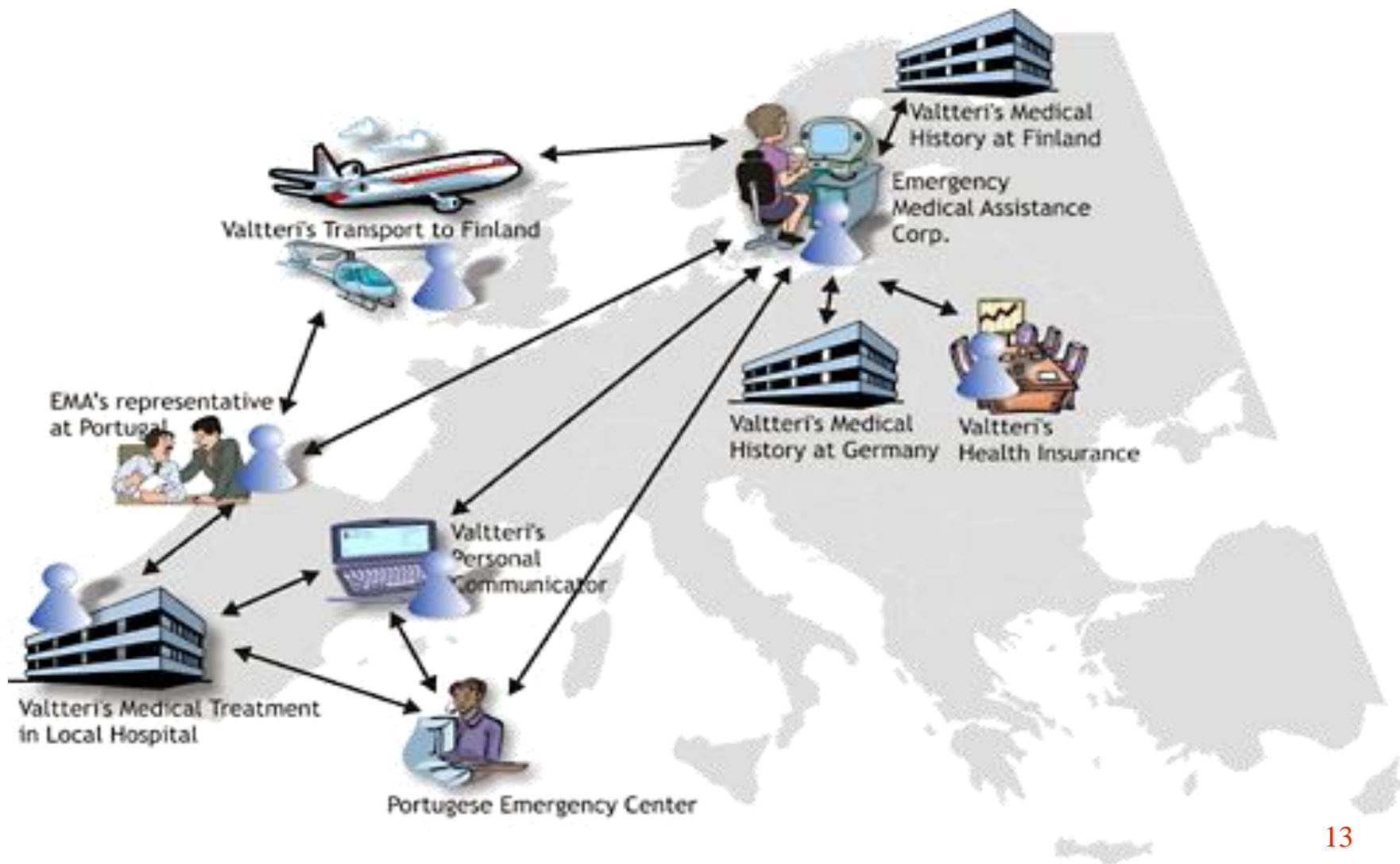


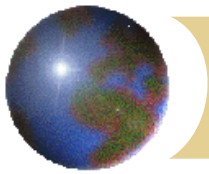
## Σενάριο II: Νοσοκομειακή περίθαλψη





# Σενάριο III: Στην εποχή του UbiComp





## Μέχρι τότε, τι;

---

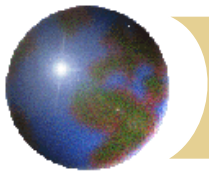
...θα εξακολουθούμε να συναντάμε εργαζόμενους σε Νοσοκομεία που **και θέλουν και μπορούν** να αξιοποιήσουν τις ΤΠΕ, και μάλιστα με σύγχρονες τεχνολογίες, αλλά δεν αρκούν μόνοι τους...

...θα εξακολουθούμε να εργαζόμαστε μαζί με πληροφορικούς, γιατρούς και διοικητικά στελέχη που **αντιλαμβάνονται τη σημασία της προστασίας** των προσωπικών δεδομένων, αλλά δεν θα μπορούν να κάνουν και πολλά γιαυτό...

...θα χαιρετίζουμε την προσπάθεια της **Αρχής Προστασίας Προσωπικών Δεδομένων** να ενθαρρύνει και να υποστηρίζει κάθε πρωτοβουλία που αποβλέπει στην προστασία των ευαίσθητων δεδομένων που αφορούν την Υγεία...

... θα εξακολουθούμε να συνεργαζόμαστε με τους εργαζόμενους και τις διοικήσεις των νοσοκομείων και να **εκπονούμε τις αναγκαίες μελέτες ασφάλειας** των πληροφοριακών τους συστημάτων, ώστε να προστατεύονται επαρκώς...

...θα πρέπει να πείσουμε ότι στο αναδυόμενο παράδειγμα των ΤΠΕ, οι σημερινές τεχνολογίες ασφάλειας πληροφοριακών συστημάτων και προστασίας προσωπικών δεδομένων της υγείας θάναι όπως τα τόξα στους πολέμους του 21<sup>ου</sup> αιώνα...



## References

1. Dritsas S., Gritzalis D., Lambrinouidakis C., "Protecting Privacy and Anonymity in Pervasive Computing: Trends and Perspectives", *Telematics and Informatics Journal*, Vol. 23, No 3, pp. 196-210, 2006.
2. Gritzalis D., Lambrinouidakis C., "A Security Architecture for Interconnecting Health Information Systems", *International Journal of Medical Informatics*, Vol. 73, pp. 305-9, 2004.
3. Gritzalis D., "Embedding privacy in IT applications development", *Information Management & Computer Security Journal*, Vol. 12, No. 1, pp. 8-26, MCB University Press, 2004.
4. Gritzalis D., Lambrinouidakis C., "A data protection scheme for a remote vital signs monitoring service", *Medical Informatics Journal*, Vol. 25, No. 2, pp. 207-224, Taylor & Francis, July 2000.
5. Gritzalis D., "Enhancing security and supporting interoperability in healthcare information systems", *Medical Informatics*, Vol. 23, No. 4, pp. 309-324, 1998.
6. Gritzalis D., "A baseline security policy for distributed healthcare information systems", *Computers & Security*, Vol. 16, No. 8, pp. 709-719, 1997.
7. Gritzalis S., Iliadis J., Gritzalis D., Spinellis D., Katsikas S., "Developing secure web-based medical applications", *Medical Informatics*, Vol. 24, No. 1, pp. 75-90, 1999.
8. Kokolakis S., Gritzalis D., Katsikas S., "Generic Security Policies for Healthcare Information Systems", *Health Informatics Journal*, Vol. 4, No. 3-4, pp. 184-195, 1998.
9. Lekkas D., Gritzalis D., "Long-term verifiability of healthcare records' authenticity", *International Journal of Medical Informatics*, Vol. 76, Issue 5-6, pp. 442-448, 2006.
10. Pavlopoulos S., Gritzalis D., et al., "Vital signs monitoring from home with open systems", in *Proc. of the 16<sup>th</sup> International Congress for Medical Informatics*, pp. 1141-1145, IOS Press, 2000.
11. Pangalos G., Gritzalis D., Khair M., Bozios L., "Improving Medical Database System Security", in *Proc. of the 11<sup>th</sup> International Information Security Conference*, pp. 11-25, Chapman & Hall, 1995.