Curriculum Vitae
(long)

This long CV includes both the business related activities at Prof-Tel Oy (1991 -), at LUT in the telematic professorship (1988-2012) and at Telecom Finland (1973-1991).

Name: **Kerttula, Esa Johannes**, Prof. Dr., born 21. August 1948, in Kemi, Finland, Finnish citizen.

Address: Långhagintie 32, 02400 Kirkkonummi, Finland, mobile: +358 45 6700 447,
e-mail: esa.kerttula@proftel.fi

Education: Dr. Tech. degree in Communications Engineering in Helsinki University of Technology (1988), Stanford Executive Program (SEP 89) in Stanford Business School, USA (1989).

Languages: Native Finnish language, English and Swedish fluent, German good.

International memberships:
Senior Member of IEEE *(The Institute of Electrical and Electronic Engineers)*, member of ACM *(Association for Computing Machinery)* and member of IACR *(International Association for Cryptologic Research).*

Publications: More than 60 consulting reports (with Prof-Tel Oy Ltd) and more than 70 technical and business publications, and about 150 other publications.

Three professional books:

- *Error Characteristics and Simulation of Error Control with Quality Criterion in 9600 bit/s Public Switched Telephone Channels for Digital Group 3 Facsimile*, Dissertation, in Acta Polytechnica Scandinavica (El 60), Helsinki 1987.

- *Multimedialla tiedon valtatielle* (in Finnish), translated as "Multimedia in Information Highway", Edita 1996, 396 pages.

- *Tietoverkkojen tietoturva* (in Finnish), translated as "Security and Cryptography in Information Networks, 3rd ed., Edita 2000, 510 pages.

Awards: In 1990 the Technology Advancing Prize for the core development of *TeleSampo,* the Value Added Network launched by Finnish PTT in 1987. TeleSampo, the "pre Internet-Web", has been in commercial use from 1986 up to the end of 2004.

Military rank: Captain (Res.)

Professional record:

1991- Managing Director (and owner) and telecommunications consultant, in **Prof-Tel Oy Ltd** (incorporated in Finland in 1991), about 60 consulting cases mainly in Finland for telecommunication operators, telecommunications authorities, service providers, telecommunications and computing industry, broadcasting companies and major users. Some international studies.

2000-2001 VP, Director, PKI Business Technology Development and Business Innovations, Sonera SmartTrust, Düsseldorf, Germany. Leading business oriented development projects related to PKI-based information security. Sonera is now part of TeliaSonera.

1989-1991 Director of Telematics Division (directly some 70 people, some 30 undirectly) in Posts and Telecommunications of Finland (Finnish PTT, then Sonera), responsible for telematics business; strategic and technology planning, marketing, investment budgeting, procurement and operations (*TeleSampo* information network, *Telebox* and *Mailnet* e-mail services, *Edivan* EDI services, *Telematics Laboratory* in Lappeenranta, Finland).

1988-1989 Deputy Director of Non-Voice Communications Division (Finnish PTT).

1984-1988 Head of Telematics Section in Data Communications Department (Finnish PTT).

1973-1984 Several planning, research and development positions in Data Communications Department (Finnish PTT).

1988-2012 *Professor* (in Telematics, part-time) in the Communications Software Laboratory of the Department of Information Technology of the Lappeenranta University of Technology (LUT). More than 2500 students have participated in telematics and other courses of Prof. Kerttula during 1988-2012 (see Appendix). Retired in May 2012.

Consulting experience with Prof-Tel Oy Ltd (1991- 2017):

In the business areas of networking, wireless and mobile communications, mobile service providers, digital broadcasting, Internet, information security:

Strategy, Business, Information society

- business and technology strategies, business models, business plans, feasibility studies and analyses, technical due diligences,
- technology and business analyses in telecom acquisitions,
- mobile payment concepts and strategies,
- telecommunications and information security strategies and policies,

Communications Technology and Theory

- mobile communications and client technologies (2G, 2.5G, 3G, 4G)
- new access technologies and networks (wired, fiber, wireless, mobile), e.g. WiMAX, Flash-OFDM, cdma450 1xEV-DO, HSPA, LTE, …
- broadband networks and technology, e.g. fiber network architectures, Open access, Metro Ethernet, Ethernet to First Mile (EFM), PON, wireless, …
- multimedia technologies and applications,
- Value Added Services technologies and applications in wireless Internet

Security, Trust and Privacy -- technology and theory

- security technologies, theory and specifications in cryptography, certificates, security architectures and protocols, smartcards, other security tokens,
- electronic identification and authentication in wireless applications,
- Trusted Third Party (TTP) services and Public Key Infrastructure (PKI), Certificate Policies (CP) and Certificate Practice Statements (CPS),
- mobile ID, Digital Identity,
- critical information infrastructure protection (CIIP), cyber security.

Board memberships:

Prof-Tel Oy Ltd	chairman and owner	(1991 -)
Saunalahti Group Oyj	board member	(2001 -2003)
Radicchio Scientific Advisory Board	board member	(2002 - 2003)

Kirkkonummi
10. May, 2017
Dr. Esa Kerttula

Appendix

Description of Telematics and other courses of Prof. Dr. Esa Kerttula in Lappeenranta University of Technology (LUT), held in 1988-2012

What is Telematics? In the following the Telematics is defined as in the Telematics Applications Programme (TAP) of the Fourth Framework Programme of the European Union (1994-1998).

> **Definition:**
> Telematics is derived from the French word 'Telematique' and refers to the use of computers alongside telecommunications systems. As such, Telematics ranges from all forms of dial-up service, through the Internet, and onto broadband applications such as Full Service Network (FSN).
>
> The European Commission, which makes available substantial resources for Telematics research and technology development, is a key proponent of the term.
>
> A more precise definition might relate to computer services offered from or through telecommunications systems.

Fig. 1 shows the development of Telematics from "Early Telematics" from around 1978 until 2000, and the new development, called here as Telematics 2.0, including among other things Web 2.0, Video 2.0 and Messaging 2.0. The convergence and new business models are often described and analysed under the concept of Telco 2.0.
Fig. 2 shows a basic Telematics tree where some of the Telematics services and applications, as well as, the most important networks are shown. Fig. 3 shows the network access systems and standards.

It should be noted that the term Telematics is used more often in meaning of pure Traffic Telematics, especially in car industry, meaning all the technology and services used for automating the traffic and its business.

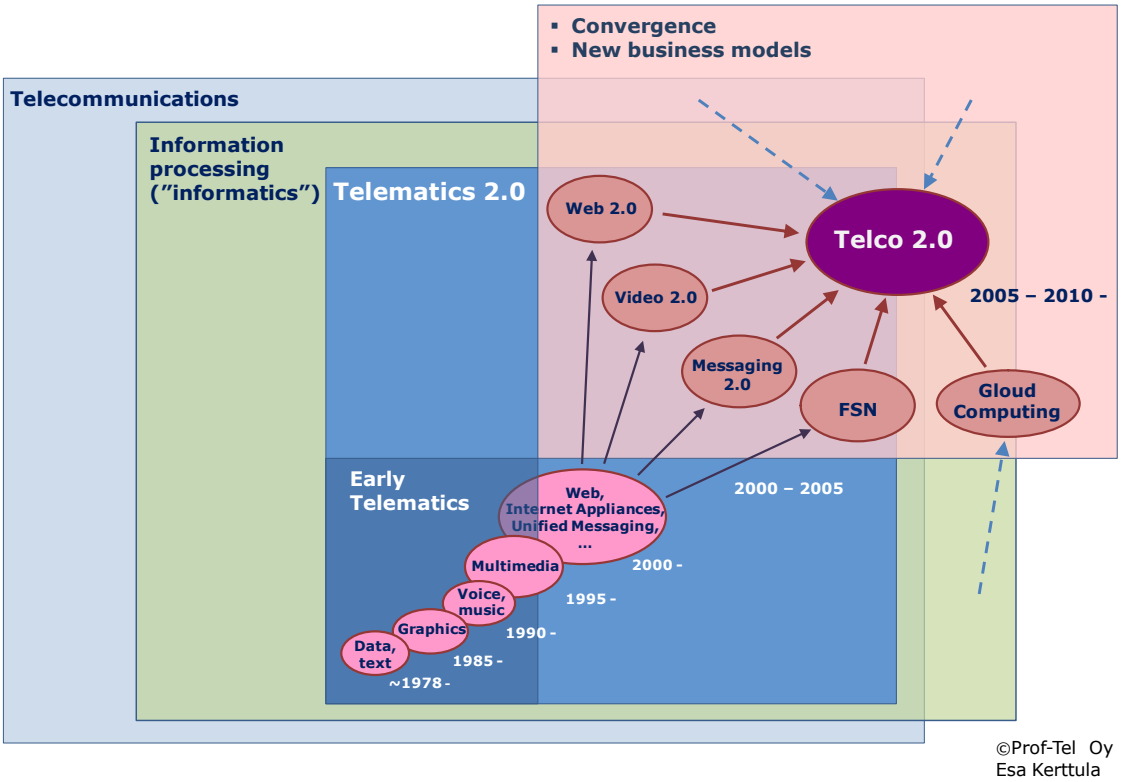

Figure 1
Development of Telematics

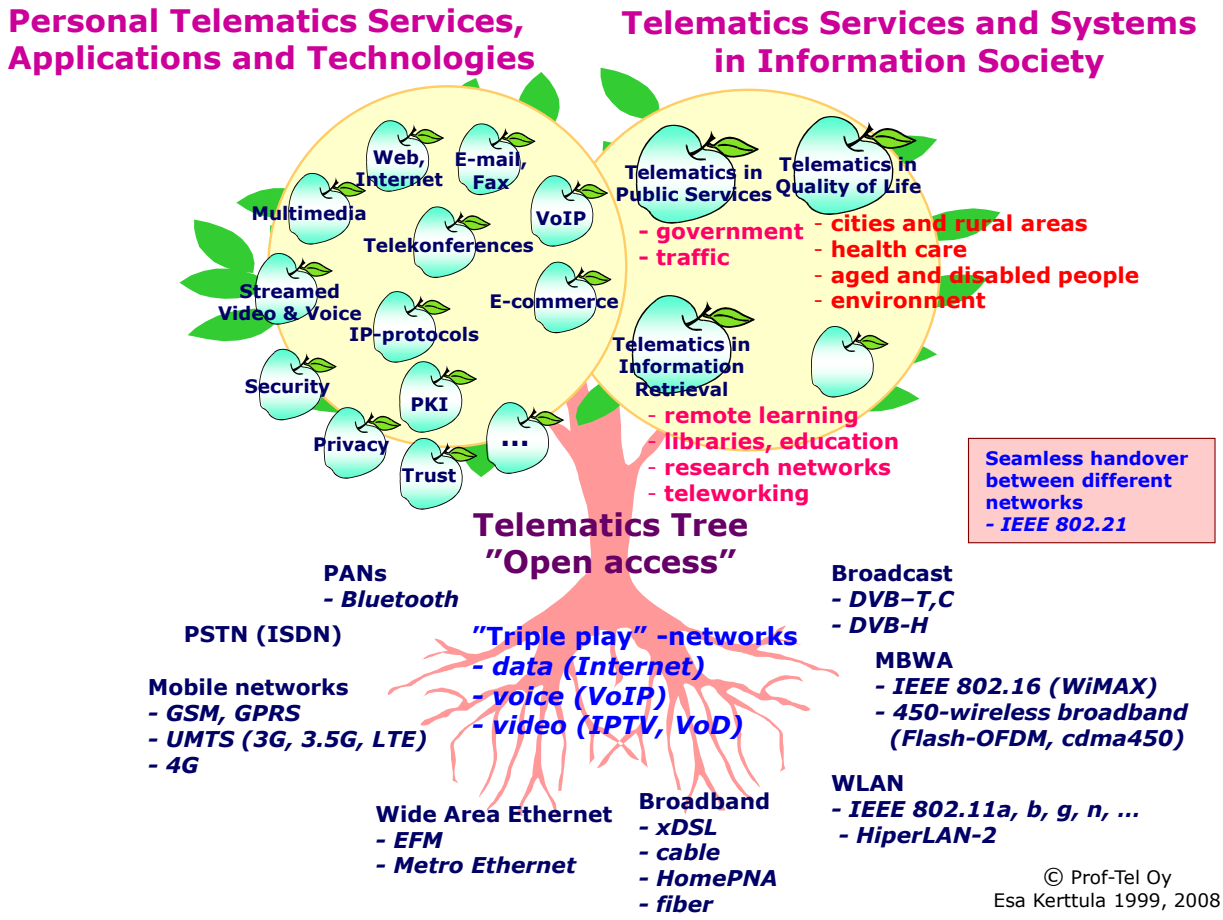

Figure 2
Telematics tree

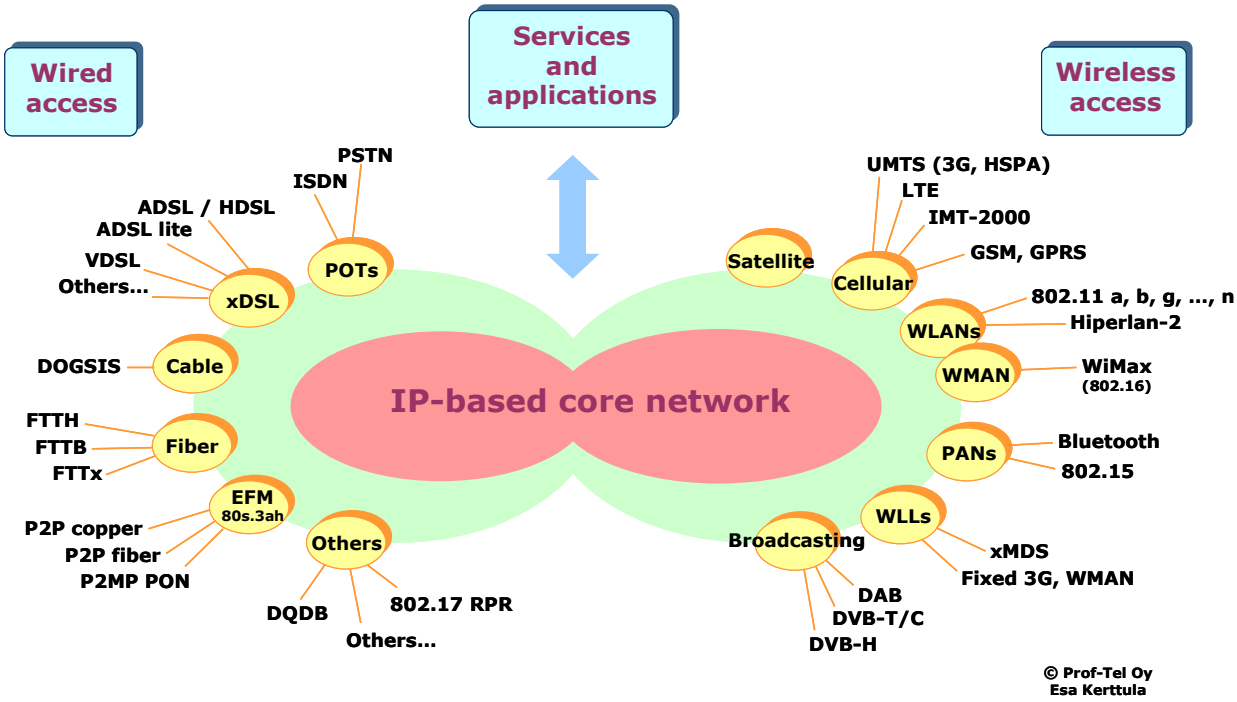

Figure 3
Wired and wireless access networks and standards

Telematics and other courses held by Prof. Dr. Esa Kerttula in the Lappeenranta University of Technology from 1988-2012

Until 2008, the Professorship in Telematics in Lappeenranta University of Technology (LUT) has included two alternating courses, one course of 35 hours (plus home work) per year, or "*Telematics (Ti5312400)"*, and "*Special Topics in Telematics (Ti5318200)"*. From 2009 the basic course (*Telematics*) has been changed to "*Computer networks and security (CT30A3600)"*. The Special Topics in Telematics is now *"Special course in Telematics (CT30A8201)".*

1. Telematics (Ti5312400) (1988-2008)

"Telematics" was a basic course (3 hours/week/semester) with broad, non-deep scope, including objectives of Telematics and study of functionality and principles of case by case selective Telematics Services and Systems, e.g. digital picture transmission with compression, EDI *(Electronic Data Interchange)*, Information Society with applications (e.g. E-Gov), Internet and electronic commerce, commercial VANs, multimedia systems and services, secure communications, public key infrastructure (PKI) and trusted third party (TTP) services and new "triple-play" –strategy (voice, data, video). Basic study and descriptions of the relevant technology and standards, the yearly varying needs depending on the case by case cases, i.e. Internet and IP, Metro Ethernet, SGML, HTML, XML and WWW, multimedia content standards (JPEG, JBIG, MPEGs (1, 2, 4, 7, 21), MHEG), EDIFACT *(EDI For Administration, Commerce and Transport)*, ebXML (electronic business XML), OSI (*Open Systems Interconnection*), VoIP (Voice over IP), LAN, WLAN, GSM (*Group Special Mobile*), GPRS and 3G, as well as emerging 4G and wireless broadband technologies, e.g. WiMAX (IEEE 802.16), Flash-OFDM and other MBWA (IEEE 802.20).

2. Special Topics in Telematics (Ti5318200) (1990-2008)

´Special Topics in Telematics´ was a deeper course (3 hours/week/semester) concentrating on the problems and topics on current interest of Telematics. Up to 2008 the following topic areas have been lectured by Prof. Esa Kerttula.

In **1990** the course dealt with *´Cryptographic Technology and Security Systems in Telematics Services´* including mathematical background and analysis of security theory, basic analysis of the cryptography technology (DES, RSA, ...), analysis of private and public key systems, privacy and authentication methods, certification, security in computer networks, key distribution protocols, CCITT Rec. X.509 and security in OSI protocols.

In **1992** the course dealt with *´Multimedia Information Systems and Multimedia Communication´,* including the principles and objectives in hypertext, multimedia and hypermedia systems and applications, description of the basic system technology in multimedia (CD-ROM, CD-I, DVI, MPC (*Multimedia PC*), GUI (*Graphical User Interface*), basic analysis and discussion of multimedia problems (information and media, applications and databases, communication, multimedia objects, user interface), analysis and topics of multimedia standards (ODA, JPEG, H.261, MPEG, MHEG, SGML, HyTime), ODA extensions with synchronizing and presentation of multimedia objects (HyperODA), analysis and discussion on problems of multimedia communication (FDDI, SMDS, Frame Relay, SDH, ATM), multimedia protocols and synchronization.

In **1994** the course dealt with *"Voice Processing Technology and Applications"* in the field of telematics and wireless communication. The areas covered were speech processing technologies (speech digitalization, text-to-speech, voice recognition (e.g. Hidden Markov Model and Neural Network technologies), speech synthesis), voice processing network functions and applications (call routing, voice mail, interactive voice responce (IVR), fax-on-demand, inbound/outbound voice processing), voice processing vs. multimedia (voice/fax, voice access, 1992 X.400, IN and PCS, ADSI, MPC), voice processing CTI-architectures (TAPI, TSAPI, SCSA, SCAI, CSTA), speech compression, coding and storing technologies (PCM, ADPCM, LD-CELP, QCELP, RPE-LTP, ISO-MPEG), voice processing software tools and programming, voice processing standards and market trends.

The **1996** course dealt with "*Cryptographic Technology and Security Systems in Telematics and Electronic Payment Systems"* the same items that the course in 1990, but updated for the new technology and new

services. Especially the following aspects are new and very important: electronic payment systems (eCash, SET, etc), security in e-mail (PGP, PEM, MOSS, S/MIME, IPv6), authentication and digital signatures, new cryptographic algorithms (MD5, SHA, IDEA, RC5).

The **1998** course dealt with *Electronic Commerce*. This course was comprehensive and included the following items; the *driving and forces* of e-commerce: Internet and multimedia, global village, 24/7, ...; *business forces*: from EDI to e-commerce, needs to change the transaction and delivery sosts; *business architectures*: foreground, ground, background technologies, virtual markets, new value chain and new intermediarities, media convergence, new content customers; *e-commerce technologies and enablers*: HTTP, HTML, XML, SSL, EDI, XML/EDI, push, agents, etc.; *digital cash and digital payment systems*: First Virtual, *i*KP, CyberCash, e-Cash, CAFE, SET, C-SET, EMV, etc., *e-architectures and shopping/trading protocols*: SEMPER, JEPI, OTP, OBI, SIT; *electronic brokerage architectures*: ABS, COBRA, ...; public key infrastructure (PKI) and trusted third party (TTP) services in e-commerce, e-commerce implementation, examples.

In **2000**, prof. Kerttula was in vacation from LUT, and had no courses in Telematics (see Note).

The **2002** course dealt with *High Speed Access Networks: New modulation and Channel Coding Technologies*. The course introduces those modulation techniques used in modern wireless and wireline access communications (Fig. 2). The course covers many modulation techniques, such as Continuous Phase Modulations (CPM) and Gaussian Minimum Shift Keying (GMSK), as well as the classic modulation methods, such as Quadrature Phase Shift Keying (QPSK), Staggered-QPSK (SQPSK), pi/4-QPSK and Minimum Shift Keying (MSK). Also modulations such as Quadrature Amplitude Modulation (QAM), which are used in wireline (VDSL, V.34) and wireless systems, are presented.

In the course, multitone modulation, usually referred to, as Discrete Multitone (DMT) and Orthogonal Frequency Division Multiplexing (OFDM), are described. DMT is a standard, throughout the world for ADSL and VDSL. Recently, there has been a lot of interest in OFDM for use in future wireless mobile communications systems. OFDM is also the basis for broadband wireless access systems such as Hiperlan2. Trellis coded modulation, (or Ungerboeck coding), the Viterbi Algorithm and a new, very promising Turbo-coding, also are discussed. FDMA, TDMA, and CDMA (including WCDMA), were discussed and compared. Three of the five IMT-2000 Radio Interface Standards are based on WCDMA.

The **2004** course was about "*Identification, Authentication, Authorization and Privacy in Information Networks – technologies, applications and business*". The basic authentication schemes, theory and concepts in current businesses (e.g. passwords, OTP, SecurID, Skey, SKID2/SKID3, Wide-mouth frog, PKI authentication (X.509v3)) are discussed and the differences in weak and strong authentication schemes explained. The most popular digital signature technologies (shared secrets, RSA, DSA, El-Gamal, ECDSA, …), biometrics and security tokens (e.g. smartcards, SIM, USB-tokens) in authentication are explained as well as the different authentication services (e.g. Kerberos, MS passport, SSO, …), and trusted third parties (RA, CA) and their security policies (CP, CPS) discussed. Digital Identity Management standards and new SSO-schemes (Liberty Alliance, WSFederation, Shibboleth) are discussed. The European union directive on Electronic Signatures (1999/93/EU) including the requirements on *secure signature-creation device* (SSCD) are discussed. The new Finnish authentication services, PKI-based Finnish ID (using smartcard or SIM), and Tupas concept used in banking sector, are presented. XML-based security technologies and user cases are discussed (XKMS, SAML, XMLsec, XMLdigsig). Some trends in PKI evolution as well as the privilege management infrastructure (PMI, X.509v4) concept are discussed. Shortly the formal approaches in analyzing the authentication protocols by using BAN-logic are discussed. Also the zeroknowledge proofs of identity (e.g. Fiat-Shamir) shortly are discussed. Finally the privacy requirements in information networks and some privacy-enhancing technologies (PET) are presented, including the promising digital credentials (from S. Brands).

The **2006** course was about "*Next Generation Authentication, Security and Privacy Schemes in Telematics – Requirements, Technologies and Solutions*". This course follows closely to the course in 2004, adding new issues such as: ECC *(Elliptic Curve Cryptography)* in practice, Public Key Cryptography in general *(IEEE P1363)*, security in new network components (e.g. in IPsec, WiMax, SIP, HIP, IMS, NGN), security trends and business as well as trust&security dimension, mobile authentication and security in 3G, IPv6, Id Mgmt, RFID, WS-security, privacy and PETs, digital credentials, European union directives.

The **2008** course was about *"Selected Authentication, Security and Privacy Schemes in Telematics – Requirements, Technologies and Solutions".* This is nearly the same course than in 2006 and 2004. In this course, however, the following items were more pointed out than in previous courses; IPsec and IPv6, 3g/4G security, WiMax security, IEEE802.21 security, and privacy schemes.

The **2010** (**Special course in Telematics**, **CT30A8201) (2010)** course was about *"New telecom business models: Web2.0, IdM2.0, Telco2.0 – convergences, platforms, basic technologies, tools".* The course discusses the business trends in information networking and information society. The EU/FP7 from Telematics point of view shortly is described. The basic technology and tools as well as trends are discussed (e.g. SIP-protocol, VoIP, IPTV standards, IMS, NGN). Networks and business convergence is discussed (e.g. principles and technology within Web 2.0, Video 2.0, Messaging 2.0, IdM 2.0). The whole convergence is discussed under the concept of Telco 2.0. In this course the new converged framework as Telematics 2.0 is called. Identity management and trust is very important area in new business models and user-centric Identity. In the course the most important technology and standards are described, as well as authentication and authorization in Web systems (e.g. Open Trust Framework, OpenID, Card Space, Liberty Alliance, IdM in ITU-T).

Fig. 4 shows the main parts of the new course. Left part shows the Web 2.0 development, business transformations and the role of Telcos, and Telco 2.0 "two-sided" telecom business model. The right part shows the concrete building blocks from access networks, control plane (here IMS based), and application layer to new social networking services with relevant standardization organizations and forums.

Next course is in 2012.

Note:
Prof. Esa Kerttula has been in a duty free period in 2000 and 2001 because of his other appointment abroad.

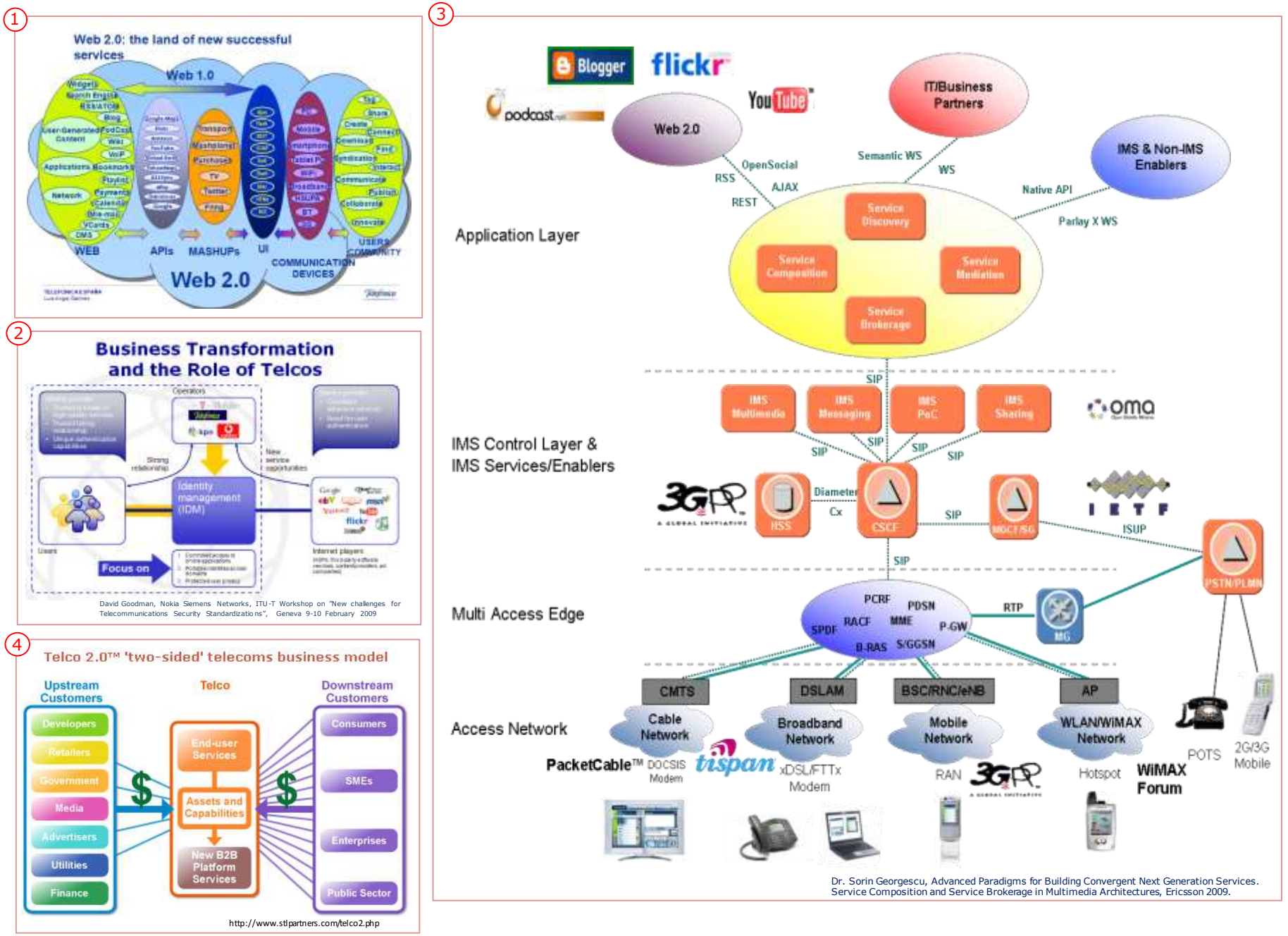

Figure 4. New business models: Web2.0 → IdM2.0 → Telco2.0

3. Computer networks and security (CT30A3600) (2009-2011)

Computer networks and security is a basic course composed of 28 class hours and home work. The course discusses the most essential technology and service roadmaps in current computer networks (terminals, processing, broadband, mobile, wireless and fiber access, Internet), and trends and visions in networking and data security. The networks include 3g/4g (e.g. HSPA, LTE), Wimax, xDSL, Cable, Metro Ethernet and MPLS. Ethernet standards for LAN (Standard Ethernet (10 Mbit/s), Fast Ethernet (100 Mbit/s), Gigabit Ethernet (1 Gbit/s), Ten-Gigabit Ethernet (10 Gbit/s)), Ethernet to First Mile (EFM), Metro Ethernet shortly are discussed. Main principles in IPv4/IPv6, VPN/IPsec, MPLS, Open access, and peer-to-peer are described.

The security part includes security principles, threat models, networks attacks (e.g. DoD/DDoS, e-mail spams), and the security solutions in selected networks. The course discusses also the most important security solutions and standards in networking (e.g. next-gen firewalls, perimeter security, intrusion detection, SIEM/IDM and UTM).

Some other Courses held by Prof. Esa Kerttula in the Lappeenranta University of Technology from 2005–2012

The other courses lectured by Prof. Esa Kerttula in LUT during 2005-2010 are *Computer networks and data transmission (CT30A2300)* and some *Updating career and supplementary courses*.

4. Computer networks and data transmission (CT30A2300)

This course is elementary course about principles, basic theory, technology and some roadmaps in computer communications and data transmission.

In **2008** Prof. Esa Kerttula was lecturing this course. In 2008 the course was about layered architecture of computer networks (OSI, Internet), network applications, protocols, broadband development (DSL, wireless, mobile), signals, line coding, analog and digital transmission, basic modulation schemes, error detection and correction (ARQ, FEC), flow control, ADSL and VDSL2, Ethernet standards for LAN (Standard Ethernet (10 Mbit/s), Fast Ethernet (100 Mbit/s), Gigabit Ethernet (1 Gbit/s), Ten-Gigabit Ethernet (10 Gbit/s)), Ethernet to First Mile (EFM), Metro Ethernet standards, IPv4/IPv6, VPN/IPsec, MPLS, Open access, peer-to-peer principles.

5. Updating career and supplementary courses

Updating career and supplementary courses are for those who are updating their career from some other sector to ICT sector, or who continue to study from old B.Sc degree to new M.Sc. or diploma engineer degree.

In **2005-2010** during the career updating programs, Prof. Esa Kerttula lectured some selected parts from Telematics course, each spring during one course. See the content of Telematics course above.

Kirkkonummi, Finland
10. April 2012

Esa Kerttula
Professor