TEKNILLINEN KORKEAKOULU
Informaatio- ja luonnontieteiden tiedekunta
Tietotekniikan tutkinto-ohjelma

INTERNETIN TIETOTURVA

Sähköpostin tekniset turvaratkaisut

Kandidaatintyö

Teemu Teekkari

Tietotekniikan laitos
Espoo 2008

TEKNILLINEN KORKEAKOULU
Informaatio- ja luonnontieteiden tiedekunta
Tietotekniikan tutkinto-ohjelma

KANDIDAATINTYÖN
TIIVISTELMÄ

Tekijä:	Teemu Teekkari	
Työn nimi:		
Internetin tietoturva – Sähköpostin tekniset turvaratkaisut		
Päiväys:	10. joulukuuta 2008	**Sivumäärä:** 12 + 3
Pääaine:	Tietoliikenneohjelmistot	**Koodi:**
Vastuuopettaja:	prof. Lauri Savioja	
Työn ohjaaja:	TkL Sanna Liimatainen	
Tiivistelmätekstiä tähän (finnish)		
Avainsanat:	avain, sanoja	
Kieli:	Suomi	

TEKNISKA HÖGSKOLAN SAMMANDRAG AV
Fakulteten för informations- och naturvetenskaper KANDIDATARBETET
Examensprogrammet för datateknik

Utfört av:	Teemu Teekkari	
Arbetets namn:		
Internetin tietoturva – Sähköpostin tekniset turvaratkaisut		
Datum:	10. joulukuuta 2008	**Sidoantal:** 12 + 3
Huvudämne:	Tietoliikenneohjelmistot	**Kod:**
Övervakare:	prof. Lauri Savioja	
Handledare:	TkL Sanna Liimatainen	
Å så ett abstrakt hit (swedish)		
Nyckelord:	avain, sanoja	
Språk:	Svenska	

HELSINKI UNIVERSITY OF TECHNOLOGY
Faculty of Information and Natural Sciences
Degree Program of Computer Science and Engineering

ABSTRACT OF BACHELOR'S THESIS

Author: Teemu Teekkari

Title of thesis:
Internet Security – Technical Solutuons for Securing Electronic Mail

Date: December 10 2008 **Pages:** 12 + 3
Professorship: Tietoliikenneohjelmistot **Code:**
Supervisor: Professor Lauri Savioja
Instructor: Sanna Liimatainen, Lic. Sc. (Tech)

Here goes the abstract (english)

Keywords: key, words
Language: Finnish

Alkulause

Kiitokset tähän

Espoossa 10. joulukuuta 2008

Teemu Teekkari

Käytetyt lyhenteet

2k/4k/8k mode	COFDM operation modes
3GPP	3rd Generation Partnership Project; Kolmannen sukupolven matkapuhelupalvelu
ESP	Encapsulating Security Payload; Yksi IPsec-tietoturvaprotokolla

Sisältö

Luku 1

Ongelman kuvaus

Esimerkkiteksti tässä on englanniksi. Kandidaatintyö kirjoitetaan kuitenkin äidinkielellä, eli suomeksi tai ruotsiksi, jollei koulusivistystään ole saanut jollakin toisella kielellä.

Viitteitä ainakin riittää, kuten Teekkari (2003) osoittaa (Hinton ja Zemel, 1998).

Some test references (Anderson ja Bezuidenhout, 1995) for language test (Axiotis et al., 2004). The IPDC Forum is an industry forum that investigates the business concepts based on the IP Datacasting technology. They describe IP Datacasting, or IPDC for short, in the following way:

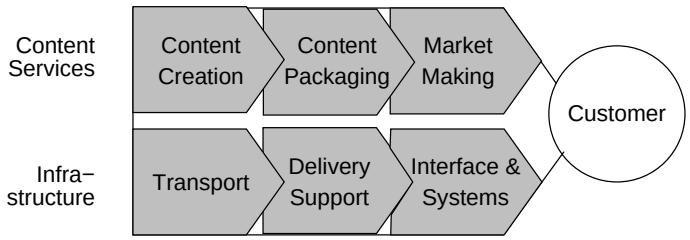
> *In IP Datacasting any digital content can be delivered cost effectively over broadcast networks to large audiences at the same time. For consumers, this means more choice in accessing multimedia content and a likely increase in content possibilities.*
>
> *IP Datacasting is a service where digital content formats, software applications, programming interfaces and multimedia services are combined through IP (Internet Protocol) with digital broadcasting (IPDC Forum, 2004).*

The way IP Datacasting is used can be divided into two rough categories:

- Downloading files or applications for later use, and
- Real-time streaming

The INDICA project uses a customer centric value chain model, based on a similar model laid out by the European Commission (1996), to understand what parts an IPDC service consists of.

INDICA's value chain model is presented in Figure 1.1.



Kuva 1.1: INDICAn kaksitasoinen arvomalli.

This chapter lays out the background of IP Datacasting. First, some usage scenarios illustrate what types of services IP Datacasting enable. Section **??** describes the IPDC value chain, and Section **??** defines terms used in this thesis. Then, Section **??** describes the objective of this thesis, and Section **??** restricts the problem scope. Finally, the structure of the thesis is described in Section **??**.

Taulukko 1.1: The DVB-T transmission parameters.

Physical channel	8 MHz (also 6 MHz or 7 MHz possible)
COFDM mode (number of subcarriers, subcarrier width, signal element length)	8k (6817, 1116 Hz, 896 μs) or 2k (1705,4464 Hz, 224 μs)
Guard interval (8k/4k duration)	1/4 (224/56 μs), 1/8 (112/28 μs), 1/16 (56/14 μs) or 1/32 (28/7 μs)
Inner code rate	1/2, 2/3, 3/4, 5/6 or 7/8
Signal element constellation	QPSK, 16-QAM or 64-QAM

Kirjallisuutta

Ross J. Anderson ja S. Johann Bezuidenhout. Cryptographic credit control in prepayment metering systems. *1995 IEEE Symposium on Security and Privacy*, 1995.

Dimitrios I. Axiotis, Tareq Al-Gizawi, Konstatntinos Peppas, Emmanuel N. Protonotarios, Fotis I. Lazarakis, Constantitnos Papadias ja Panos I. Philippopoulos. Services in interworking 3G and WLAN environments. *IEEE Wireless Communications*, 11(5):14–20, lokakuu 2004.

European Commission. Strategic Developments for the European Publishing Industry towards the Year 2000 - Europe's Multimedia Challenge, 1996.

Geoffrey E. Hinton ja Richard S. Zemel. Autoencoders, minimum description length and Helmholtz free energy. Teoksessa *Advances in Neural Information Processing Systems 6*, Jack D. Cowan, Gerald Tesauro ja Joshua Alspector, toimittajat, sivut 3–10. The MIT Press, Cambridge, MA, USA, 1998.

IPDC Forum. About IP Datacasting - Overview, 2004. URL `http://www.ipdc-forum.org/about/index.html`. IPDC Forumin WWW-sivu. Viitattu 18.2.2004.

Teemu Teekkari. Diplomityöni. Diplomityö, Teknillinen korkeakoulu, Espoo, 2003.