



**"ICT4University – WiFi SUD"**  
**Regione CAMPANIA**  
**Seconda Università degli Studi di NAPOLI**  
**Progetto: WIFI SUN 2**  
**22-lug-2008**

Sezione 1 – Dati del proponente

**Università proponente**

Denominazione	Seconda Università degli Studi di NAPOLI
Sede	Napoli
Indirizzo postale	Viale Beneduce n. 10 - 81100 Caserta
Indirizzo e-mail	segreteria.rettorato@unina2.it
Telefono	0815666909
Fax	081296764
Sito web	www.unina2.it
Codice Fiscale	02044190615

**Rappresentante legale**

Cognome e nome	Rossi Francesco
Qualifica	Rettore
Telefono	0815666909
Fax	081296764
Indirizzo e-mail	francesco.rossi@unina2.it

**Referente di progetto**

Cognome e nome	Di Martino Beniamino
Qualifica	Prof.
Telefono	3470461656
Fax	0815037042
Indirizzo e-mail	beniamino.dimartino@unina.it

## Sezione 2 – Sintesi del progetto

### Identificazione e descrizione breve del progetto

Nome progetto	WIFI SUN 2
Finalità progetto	Il progetto si pone l'obiettivo di migliorare la copertura della rete WiFi dell'Ateneo, al fine di erogare con più efficienza i servizi già attivati di Mail Studenti e di gestione carriera studenti online, di fornire l'accesso ad internet alla totalità degli studenti in maniera sicura e controllata. L'Ateneo intende inoltre perseguire la finalità di produrre il servizio di verbalizzazione elettronica degli esami.
Date inizio prevista	04/01/2009
Date fine prevista	18/12/2009

### Struttura finanziaria del progetto

Valore totale del Progetto pari a:	500.000,00
Di cui a carico:	
1. Università	200.000,00
2. Finanziamento richiesto al Dipartimento	300.000,00
3. Altri soggetti pubblici o privati	0,00
4. Altri	0,00
N/A	

### Dettaglio del finanziamento richiesto al Dipartimento

Finanziamento richiesto al Dipartimento:	300.000,00
Di cui:	
1. per servizi (compresi i servizi minimi)	81.000,00
2. per infrastrutture di rete	210.000,00
3. per piano di comunicazione agli studenti	9.000,00

### Copertura della rete senza fili realizzata

Percentuale dell'area dell'Università coperta da rete senza fili prima prima del progetto	30.0
Percentuale dell'area dell'Università che si prevede sarà coperta da rete senza fili al completamento del progetto	85.0
Percentuale di studenti che si prevede saranno raggiunti dalla rete senza fili al completamento del progetto sul totale degli studenti iscritti	90.0
Numero studenti regolarmente iscritti all'ateneo	28000

### Copertura e caratteristiche dei servizi minimi

#### Servizio per l'iscrizione online

Il servizio è già disponibile presso	SI
--------------------------------------	----

l'università?	
Descrizione sintetica	Il servizio sarà reso disponibile attraverso un modulo online per l'iscrizione, mentre è già attivo il pagamento online delle tasse universitarie

#### **Servizio per la verbalizzazione elettronica degli esami**

Il servizio è già disponibile presso l'università?	NO
Descrizione sintetica	Automatizzazione del processo di registrazione degli esami e dall'immediata trasmissione delle informazioni al sistema informativo di Ateneo. Ogni docente riceve una smart card personale, protetta da codice segreto e in grado di generare la firma digitale
Qualora il servizio sia introdotto in modalità sperimentale, indicare la percentuale studenti che ne potranno usufruire (rispetto agli iscritti)	100.0

#### **Copertura e caratteristiche degli eventuali altri principali servizi realizzati**

Denominazione del servizio	Mail Studenti
Descrizione sintetica	Mail fornita a tutti gli studenti dell'università con finalità didattiche e amministrative
Percentuale studenti raggiunti dal servizio (rispetto agli iscritti)	100.0
Eventuali informazioni aggiuntive	

Denominazione del servizio	Gestione Carriera Studenti Online
Descrizione sintetica	Visualizzazione dati carriera dello studente, previsione di erogazione del servizio prenotazione esami online
Percentuale studenti raggiunti dal servizio (rispetto agli iscritti)	100.0
Eventuali informazioni aggiuntive	

#### **Misure di sicurezza previste**

Descrizione sintetica delle procedure previste per l'autenticazione e la gestione degli accessi alla rete	Autenticazione basata su protocollo IEEE 802.11/xx con l'utilizzo di un server Radius cooperante con un server LDAP. Tutte le comunicazioni avverranno in maniera cifrata.
Descrizione sintetica di ulteriori misure di sicurezza previste	Il progetto prevede l'installazione di dispositivi di sicurezza di tipo FIREWALL e Proxy Server per ciascuna sede interessata dalla copertura WiFi. Si prevede inoltre la separazione tra le reti Amministrativa e di Ricerca e quella utilizzata dagli studenti.

#### **Utilizzo di soluzioni Open Source e/o riuso di soluzioni disponibili**

Soluzioni Open Source utilizzate nel progetto	Il progetto prevede l'utilizzo di soluzioni Open Source sia per quanto riguarda l'autenticazione attraverso i server OpenLDAP e FreeRadius installati su SO Linux, sia per le misure di sicurezza implementate con l'utilizzo di Proxy Server Squid e di audit tool open source (Nessus, Pandora, Nagios...).
Soluzioni già realizzate, anche da terzi, e	Prevediamo il riutilizzo della applicazione web per la gestione degli account per

riutilizzate nel progetto	l'autenticazione, e della appliance per il management della rete wireless esistente.
---------------------------	--

#### **Piano di comunicazione**

Piano di comunicazione del progetto (ad esempio, bacheche dedicate, poster, depliant illustrativi, ecc.)	Realizzazione di un volantino illustrativo, chioschi divulgativi, sito wifi studenti, locandine pubblicitarie.
--	--

### Sezione 3 – Scheda Progetto

#### **Nome e descrizione del progetto**

##### WIFI SUN 2

L'iniziativa proposta si pone l'obiettivo di completare la copertura wireless di spazi utilizzati dagli studenti all'interno delle Facoltà e degli stabili che ospitano strutture universitarie .

L'accesso alla rete WI-FI sarà reso disponibile in modalità "hot spot" assicurando la copertura all'interno delle seguenti strutture di uso da parte degli studenti:

Aule: aule studenti, spazi adibiti ad aule studio

Biblioteche di Facoltà

Sale conferenze e aule didattiche.

Spazi aperti e cortili

Si provvederà inoltre alla cablatura dei punti rete e alla connessione degli access point alla rete Lan. Essi trarranno l'alimentazione attraverso il cablaggio Ethernet, e saranno collegati alle porte di uno switch di rete.

Gli Access Point saranno dotati di un kit di sicurezza che ne impedirà la rimozione non autorizzata.

Nel caso di punti di accesso wireless installati all'esterno, si dovrà provvedere alla loro messa in sicurezza da agenti esterni (umidità, pioggia...) e da eventuali furti.

Si pone inoltre l'obiettivo di realizzare la verbalizzazione elettronica degli esami. A tal fine verranno utilizzate le carte di identificazione di cui saranno prossimamente dotati tutti gli studenti dell'Ateneo, verranno fornite carte di identificazione ai docenti, e acquisiti dispositivi hardware necessari alla verbalizzazione elettronica.

#### **Obiettivi e ambito del progetto**

La seconda Università degli Studi di Napoli, da qualche anno sta prevedendo servizi per rendere la didattica ed il diritto allo studio più agevole per tutti gli studenti.

- 1) Siti web delle facoltà e dei singoli dipartimenti con aree dei singoli docenti per ogni tipo di informazione sulla didattica.
- 2) Piattaforme di E-learning
- 3) Laboratori informatici ed aule informatizzate
- 4) Posta elettronica Studenti
- 5) Gestione carriera studenti online

Il wi-fi si inserisce in questi servizi ad hoc per lo studente per fare in modo che tali siano usati in modo libero sicuro e gratuito all'interno delle strutture universitarie. Con l'apliamento previsto della copertura, il wi-fi renderà fruibile tutti i servizi messi a disposizione degli studenti con maggiore facilità.

Tale servizio dovrà consentire di fornire una connettività "libera" a tutti gli utenti abilitati che intendano accedere alla rete GARR ed a particolari servizi che verranno erogati attraverso la rete di Ateneo a la rete a disposizione del complesso. Le prestazioni del servizio di connettività dovranno essere tali da consentire eventuali future applicazioni VoIP o comunque applicazioni real-time e l'accesso a dispositivi standard 802.11b/g WiFi (Laptop/Notebook, PC Desktop, Palmari, PDA ,etc.).

La sicurezza e le contromisure da eventuali accessi malevoli dall'esterno, non autorizzati, o un uso non corrispondente alle politiche di accesso stabilite dall'Ateneo, avrà un ruolo strategico su cui il progetto pone particolare attenzione, attraverso un potenziamento della rete cablata, la predisposizione di Firewall, e la navigazione attraverso Proxy.

Le connessioni wireless dovranno utilizzare il sistema di autenticazione e crittografia già esistente ed in grado di abilitare o meno gli utenti autorizzati al servizio.

Il sistema di verbalizzazione elettronica degli esami si inserisce nell'ambito della modernizzazione ed automazione delle procedure amministrative con la finalità di semplificare il rapporto tra studente ed Università.

Il sistema di verbalizzazione attualmente in uso dalla SUN si basa sul flusso di statini cartacei compilati dai docenti in sede d'esame e consegnati, in un secondo momento, alla segreteria universitaria, che, a sua volta, deve copiare le stesse informazioni nel proprio database. Tale sistema presenta molti svantaggi: innanzitutto gli esami non vengono mai registrati in tempo reale. Inoltre, la compilazione dello statino è molto laboriosa con elevato rischio di errori.

Il sistema di verbalizzazione elettronica riduce drasticamente il tempo che passa da quando un esame viene sostenuto a quando le relative informazioni vengono memorizzate nel sistema informativo di Ateneo.

#### **Finalità e risultati attesi dal progetto**

---

Lo scopo del progetto wi-fi è quello di ampliare la rete esistente in maniera da raggiungere la quasi totalità degli spazi fruibili e la totalità della popolazione studentesca dell'ateneo per rendere utilizzabili a pieno i servizi che l'Ateneo mette a disposizione

Le attività che si vogliono incentivare sono:

Lo scambio documentale e di informazioni nonché l'accesso a banche dati di natura specialistica. Inoltre con gli strumenti informatici più evoluti è possibile scambiare e condividere materiale didattico (articoli, appunti, ecc.)

Lo scambio di informazioni tra docenti e studenti le esperienze di studio e lo scambio di protocolli di ricerca. In questo contesto è certamente importante che la rete supporti la multimedialità facilitando la teledidattica, la teleconferenza e comunque la condivisione di informazioni, non solo tra Università, ma anche fra tutte le istituzioni.

L'automazione delle procedure di verbalizzazione con la riduzione dei tempi amministrativi

I risultati del progetto saranno determinati dal numero di studenti che avranno accesso ai servizi e dalle prestazioni del sistema realizzato.

Per quanto riguarda il sistema di verbalizzazione degli esami, ci si aspetta una drastica riduzione dei tempi che intercorrono tra l'esame e il relativo inserimento nel sistema informatico di Ateneo.

### **Caratteristiche dei servizi / Procedure di sicurezza**

Una politica di sicurezza è alla base del buon funzionamento e del rispetto delle motivazioni che spingono alla realizzazione di questo progetto. L'architettura di sicurezza sarà centralizzata per quanto riguarda l'autenticazione dello studente, espandendo l'infrastruttura esistente. Le credenziali di accesso rimarranno le stesse già esistenti.

L'architettura esistente si basa sullo standard di autenticazione IEEE 802.1x. Il protocollo EAP (Extensible Authentication Protocol) nella sua variante cifrata EAP-TLS è utilizzato per le comunicazioni tra la stazione di rete e un server RADIUS al quale l'Access Point fa riferimento. Il server Radius interroga in modalità proxy un server LDAP deputato a rendere accessibili i profili di autenticazione/autorizzazione di ciascun utente.

Il sistema esistente effettua un filtraggio a livello 2 della pila ISO/OSI nella parte radio della rete. Il progetto si prefigge lo scopo di effettuare un filtraggio a livello 2 nella parte di rete cablata, attraverso un cablaggio strutturato dedicato.

Laddove non è possibile realizzare un cablaggio strutturato a sé stante, il progetto prevede una separazione logica delle reti.

Il livello di sicurezza verrà ulteriormente elevato agendo a livello 3 attraverso firewall organizzati gerarchicamente e distribuiti sulle diverse sedi dell'università, e a livello 7 utilizzando un filtraggio di tipo applicativo.

La certificazione WI-Fi sarà garante della realizzazione di reti scalabili in cui la copertura radio su ciascuna banda di frequenza può essere ottimizzata in funzione del tipo di antenne e di potenza trasmessa utilizzata.

### **Disegno di massima della soluzione**

Le aree destinate agli studenti (aule, sale studio, biblioteche, Spazi aperti e cortili) saranno completate nelle coperture mediante il modello "hot spot", realizzato con un numero adeguato di wireless access point in posizione baricentrica rispetto alle aree da coprire. Gli access point da utilizzare dovranno essere perfettamente integrabili nel sistema esistente ed in particolare avranno le seguenti caratteristiche funzionali:

Wireless Access Point modulari in Standard IEEE 802.11b/g

Almeno 1 porta 10/100 fast ethernet per la connessione alla LAN e 1 porta console

Protocolli di autenticazione supportati:

802.1X,

EAP-Flexible Authentication via Secure Tunneling

Protected EAP- Generic

EAP-Transport Layer Security (EAP-TLS),

PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP MSCHAPv2),

EAP-Tunneled TLS (EAP-TTLS),

EAP-Subscriber Identity Module (EAP-SIM) to yield mutual authentication and dynamic, per-user, per-session encryption keys (WPA e WPA2)

Protocolli di crittografia e cifratura

AES-CCMP per cifratura WPA2

Temporal Key Integrity Protocol (TKIP): key hashing (per-packet keying), message integrity check (MIC) e sistema di rotazione delle chiavi broadcast via TKIP o WPA TKIP

IEEE 802.11 WEP con chiavi a 40 bits e a 128 bits

Cifratura AES in Hardware

Possibilità di effettuare il secure-roaming tra celle in modo veloce.(gli Access Point devono poter svolgere la funzione di riautenticazione in base al protocollo 802.1x senza comunicare con il server di autenticazione)

Possibilità di connettere vari tipi di antenna (omnidirezionale e monodirezionale) sia per i moduli radio 802.11b/g sia per il modulo radio 802.11a

Conformità allo standard IEEE 802.11i

Certificazione WPA e WPA2

Conformità alle direttive ETSI

Gestione tramite protocolli: BootP, SSH, HTTPS, TFTP, FTP, Telnet, Porta console, SNMP MIB I & II

Dhcp server

I dispositivi che avranno accesso ai servizi wireless dovranno essere monitorati con sistemi di controllo e management evoluta compatibili con quelli già in produzione e che consentono una gestione proattiva degli stessi. Tali sistemi sono responsabili delle funzionalità di governo della rete wireless (come l'intrusion prevention, le policy di sicurezza, la QoS, la gestione delle interfacce radio, la RF prediction, il troubleshooting, l'ottimizzazione della rete, il tracking degli utenti, il security monitoring, la gestione degli access point e i servizi di mobilità). Si potranno così tracciare gli spostamenti di dispositivi Wireless ottimizzando i processi interni e identificando velocemente intrusioni e uso improprio della rete.

Le funzionalità della piattaforma attualmente in uso sono le seguenti:

Funzionalità per la scoperta, localizzazione e disabilitazione di AP non autorizzati presenti in rete o nell'area di copertura wireless;

Funzionalità di autoscoperta degli apparati di accesso alla rete;

Funzionalità per applicare le policy di security agli apparati e ai client wireless;

Funzionalità per la scoperta di WLAN presenti in rete;

Capacità di gestire dinamicamente la copertura radio, per permettere agli AP di ottimizzare l'area di copertura in caso di problemi agli AP adiacenti;

Capacità di scoperta delle interferenze radio e di monitorare i guasti;

Interfaccia che mostri la situazione della rete, carico degli apparati, uso delle radiofrequenze, errori e associazione dei client. Capacità di configurare da remoto gli AP e i bridge, le VLAN e di aggiornare il firmware degli apparati;

Possibilità di essere integrato con altri tool di network management;

Interfaccia di gestione accessibile tramite protocollo HTTPS;

Compatibile con apparati in standard 802.11 b e g;

Capacità di monitorare la disponibilità dei server IEEE 802.1X, Extensible Authentication Protocol (EAP), Protected EAP (PEAP) e RADIUS e dei loro tempi di risposta.

Allo stato attuale, il sistema di controllo e management è realizzato tramite una appliance dedicata. Si prevede che l'estensione del sistema deve essere integrabile con il sistema in uso.

Il sistema di autenticazione in uso va ridonato con l'acquisizione di un server identico configurato in load balancing.

Andranno anche acquisiti degli apparati di rete fissa per il collegamento degli Access Point.

L'alimentazione degli access point dovrà sfruttare il cablaggio nelle aree interessate alla copertura, secondo gli standard in-line power con apparati operanti PoE IEEE 802.1af o utilizzando apparati preesistenti a cui saranno associati power injectors. Si dovrà provvedere al cablaggio strutturato delle aree in cui è prevista la copertura.

Nell'ambito del progetto, sulla base della copertura fornita agli studenti, si è considerata l'ipotesi di creare un servizio VoIP ad uso degli studenti, per migliorare e agevolare il libero scambio di informazioni all'interno della università. A tal proposito si pensa che il sistema possa erogare il servizio in maniera sperimentale ad una frazione degli studenti. Il sistema si baserà su soluzioni Open Source e verrà progettato e sviluppato attraverso risorse interne, acquisendo l'hardware necessario per supportarlo.

Il sistema di accesso già realizzato nell'ambito del precedente progetto prevede l'utilizzo di un account basato su username e password che consente di identificare l'utente all'interno della rete wifi e nella fruizione dei servizi messi a disposizione. Tale sistema necessita della gestione degli account. Il progetto prevede, utilizzando risorse e competenze interne, la realizzazione di una applicazione per la gestione degli account.

In particolare esso fornirà le funzionalità di gestione password, gestione stato utente (attivo, disabilitato, sospeso,...), gestione accessi. Tale soluzione si baserà su software Open Source ed avrà interfaccia di tipo web.

Per lo sviluppo di servizi di accesso e di messa in sicurezza, si provvederà alla realizzazione degli stessi mediante consulenza interna e/o esterna di esperti del settore ICT, ed eventualmente mediante l'acquisizione di firewall e proxy server.

Presumibilmente, il numero minimale di access point necessari alla copertura delle strutture sopra citate è di 300 unità.

Si rende necessario inoltre prevedere 15 access point di riserva che verranno utilizzati in caso di malfunzionamenti per le eventuali sostituzioni momentanee.

Il sistema di verbalizzazione elettronica degli esami universitari ha come obiettivo principale l'automatizzazione del processo di registrazione degli esami e dall'immediata trasmissione delle informazioni al sistema informativo di Ateneo, con la eventuale possibilità di eliminare completamente l'archivio cartaceo.

I principi di funzionamento del sistema prevederà che ogni docente che si registra riceve una smart card personale, protetta da codice segreto e in grado di generare la firma digitale. La piattaforma dovrà essere in grado di gestire contemporaneamente più sorgenti di informazioni:

1) attraverso l'uso di un dispositivo hardware:

questa modalità di registrazione prevede che il professore utilizzi in sede di esame un dispositivo per la registrazione. Durante l'appello il docente si autentica per mezzo della propria smart card e viene guidato, tramite semplici passaggi, nella procedura di registrazione degli esami, nella quale è possibile identificare lo studente digitando il relativo numero di matricola od, in alternativa, mediante tessere magnetiche o smart card compatibili con quelle già in uso dello studente. Il dispositivo deve supportare la modalità di funzionamento off-line, laddove non c'è la disponibilità di sorgenti di alimentazione e connessioni di rete;

2) attraverso interfaccia Web:

i presidenti di commissione dovranno poter effettuare operazioni di registrazione degli esami direttamente da interfaccia web. L'applicazione web dovrà essere progettata con un alto livello di sicurezza: l'inserimento di informazioni può infatti avvenire solo dopo che il professore ha digitato login e password e si è autenticato tramite la propria smart card.

Il sistema deve interagire con il sistema informativo di Ateneo. La gestione delle identità digitali degli attori del sistema potrà avvenire o attraverso la creazione di una Certification Authority interna, ovvero attraverso una fornitura esterna. I livelli di sicurezza delle identità digitali potranno essere differenti tra le varie tipologie di utenti del sistema. Si prevede una fase iniziale, non superiore ai tre mesi, in cui la gestione della eventuale Certification Authority interna può essere affidata personale esterno o a contratto.

I sistemi proposti dovranno prevedere dei piani di formazione per il personale addetto. Inoltre si prevede una fase iniziale, non superiore ai tre mesi, in cui la gestione può essere affidata personale esterno o a contratto.

Si propone di realizzare un sistema di segnalazione problemi basato su applicazione web intranet, per assistere gli studenti nella fruizione dei servizi per un periodo iniziale di tre mesi. A tal fine è possibile prevedere l'utilizzo di personale esterno o a contratto.

## **Approccio e Piano di realizzazione**

La presente proposta progettuale rappresenta di fatto un Progetto Preliminare che include una indicazione delle specifiche esigenze percepite, le basi tecnologiche della soluzione richiesta elencando brevemente le soluzioni tecnologiche e le scelte progettuali previste. A tale Progetto Preliminare dovrà seguire un Progetto Esecutivo cui, sulla base delle piantine delle aree interessate e delle analisi di copertura effettuate sul campo, saranno concordate e definite le posizioni degli Access Point.

Il piano di realizzazione di massima è brevemente descritto nel seguente cronoprogramma che dettaglia le varie fasi della messa in opera. Il cronoprogramma compilato con le voci inerenti l'attività specifica, deve contenere almeno i seguenti items:

Anno 2009

Approvvigionamento materiali:

Gennaio-Aprile;

Realizzazione Servizi:

Febbraio-Giugno;

Start Up Servizi:

Giugno-Agosto;

Realizzazione infrastrutture di base:

Marzo-Luglio;

Installazione apparati di accesso wireless:

Maggio-Ottobre;

Installazione e configurazione SW:

Agosto-Settembre

Collaudo, Documentazione finale di impianto, Piano di Comunicazione:

Novembre

## **Utilizzo di soluzioni Open Source e riuso di soluzioni già disponibili**

Nell'ambito di un precedente progetto di Ateneo per la realizzazione di una infrastruttura di rete wireless sono stati installati 100 Access Point presso le seguenti sedi:

- Facoltà di Architettura

    Complesso di S. Lorenzo ad Septimum, via S. Lorenzo – Aversa (CE)

    Sede di Marcianise, via Duomo – Marcianise (CE)

- Facoltà di Economia

    Complesso delle Dame Monache (ex caserma Fieramosca), via Gran Priorato di Malta – Capua (CE)

- Facoltà di Giurisprudenza  
Palazzo Melzi, piazza Matteotti – Santa Maria Capua Vetere (CE)  
Aulario, loc. Quattro Santi – Santa Maria Capua Vetere (CE)
- Facoltà di Ingegneria  
Complesso della Real Casa dell'Annunziata, via Roma, 29 – Aversa (CE)  
Aulario, via Michelangelo – Aversa(CE)
- Facoltà di Lettere e Filosofia  
Complesso di S. Francesco, piazza S. Francesco - Santa Maria Capua Vetere
- Facoltà di Medicina e Chirurgia  
Edificio di S. Andrea delle Dame, via de Crecchio – Napoli  
Edificio di S. Patrizia, via L. Armani – Napoli
- Facoltà di Psicologia, Scienze Ambientali, Scienze MMFFNN  
Complesso di via Vivaldi 43 – Napoli
- Facoltà di Studi politici e per l'Alta formazione europea e mediterranea "Jean Monnet"  
Complesso monumentale del Belvedere di S. Leucio, via del Setificio Caserta

Nell'ambito dello stesso sono stati acquisiti N. 2 Server per l'autenticazione e il monitoraggio della rete, N. 1 appliance di monitoraggio e management. Il sistema di autenticazione si basa sistemi Open Source, in particolare: SO Linux, OpenLDAP, FreeRadius.

Prevediamo di utilizzare software Open Source per la realizzazione dei Proxy.

### Iniziative e Piano di comunicazione

L'iniziativa in progetto verrà pubblicizzata mediante questi sistemi di informazione attiva:

Opuscoli destinati agli studenti con tutorial alla fruizione dei servizi disponibili in wireless e suggerimenti alla configurazione dei terminali;

Workshop informativi per gli studenti;

Realizzazione di pannelli e targhe informativi .

Sito WiFi Studenti

### Struttura finanziaria del progetto

#### Servizi

HW: € 74.000,00

SW: € 60.000,00

Gestione: € 25.000,00

Formazione: € 10.000,00

Progettazione: € 20.000,00

Sub TOT: € 189.000,00

#### Comunicazione:

HW: € 5.000,00

Gestione: € 6.000,00

Sub TOT: € 11.000,00

TOTALE Fondi Università € 200.000,00

#### Fondi Dipartimento

##### Rete

HW: € 170.000,00

Gestione: € 10.000,00

Formazione: € 10.000,00

Progettazione: € 20.000,00

Sub TOT: € 210.000,00

##### Servizi

HW: € 50.000,00  
SW: € 31.000,00  
Sub TOT: € 81.000,00  
Comunicazione  
Gestione: € 9.000,00  
Sub TOT: € 9.000,00  
TOTALE Fondi Dipartimento € 300.000,00

Totale Generale

Rete  
HW: € 170.000,00  
Gestione: € 10.000,00  
Formazione: € 10.000,00  
Progettazione: € 20.000,00  
Sub TOT: € 210.000,00

Servizi

HW: € 124.000,00  
SW: € 91.000,00  
Gestione: € 25.000,00  
Formazione: € 10.000,00  
Progettazione: € 20.000,00  
Sub TOT: € 270.000,00

Comunicazione

HW: € 5.000,00  
Gestione: € 15.000,00  
Sub TOT: € 20.000,00  
TOTALE Generale € 500.000,00

**Eventuali ulteriori informazioni**

---

Sezione 4 – Allegati

Delega\_di\_firma\_Rettore



## Seconda Università degli studi di Napoli

21 LUG 2008

Caserta .....  
N° di protocollo **Rettorato 24338**  
Posizione .....  
Risposta al FI n° ..... del .....  
Allegati .....

Al Dipartimento per l'Innovazione e le  
Tecnologie della Presidenza del  
Consiglio dei Ministri  
Via Po, 14  
00198 Roma

E, p.c. Al Chiar.mo Prof.  
Beniamino Di Martino  
Facoltà di Studi Politici e per l'Alta  
Formazione Europea e Mediterranea  
"Jean Monnet"

Tit. III, Cl. 10

Il sottoscritto Prof. Francesco Rossi, Rettore Pro-tempore e legale rappresentante della Seconda Università degli Studi di Napoli, nato a Striano (NA) il 15/06/48 e domiciliato per la carica in Viale A. Beneduce n.10 (CASERTA)

### DELEGA

In qualità di referente scientifico del progetto denominato "**WIFI SUN**" il Prof. Beniamino Di Martino Professore Ordinario della Facoltà di Studi Politici e per l'Alta Formazione Europea e Mediterranea "Jean Monnet" di questo Ateneo, nato a Castellamare di Stabia il 14/06/67 e residente in Via Appia lato Napoli, snc - Formia (LT) - alla gestione nonché alla sottoscrizione di tutti gli atti relativi al suddetto progetto.

IL RETTORE  
Prof. Francesco Rossi