



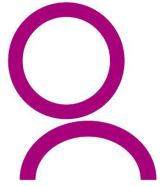
RFID

Giuseppe Tetti



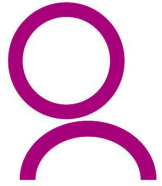
Un po' di storia

- Un primo impiego militare nel settore aeronautico, già prima della seconda guerra mondiale, l'IFF (*Identification Friend or Foe*).
 - L'aereo si dichiarava amico al sistema Radar inviando un segnale di identificazione.
- Fine anni '60: primi sistemi EAS (*Electronic Article Surveillance*)
 - Elementare funzione antitaccheggio con l'utilizzo di *trasponder* in grado di gestire un'informazione di 1 bit per indicare la presenza/assenza di un prodotto, p.e. nei supermercati. Primo vero caso di impiego di massa per applicazioni non militari.



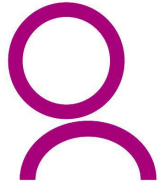
Un po' di storia

- Anni '70: sviluppo degli elementi fondanti della tecnologia RFID.
- Anni '80: la tecnologia è completa e comincia a diffondersi su scala mondiale.
- Anni '90: si realizzano le condizioni per lo sviluppo dell'RFID in senso moderno.
 - I circuiti si miniaturizzano.
 - Si cominciano a sviluppare gli standard internazionali.
 - I nuovi *trasponder* miniaturizzati non hanno più bisogno di una sorgente di energia propria, ma possono essere alimentati dalle stesse onde elettromagnetiche generate dai lettori.
 - Lo sviluppo di Internet e la possibilità di creare trasponder miniaturizzati a basso costo ci proietta verso **Internet of Things**.



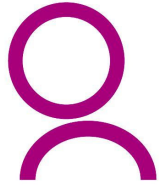
Definizione di sistema RFId

- RFID è l'acronimo di *Radio Frequency Identification* (identificazione a radio frequenza).
- I sistemi RFId fanno parte delle tecnologie di identificazione automatica (Auto-ID), che fanno riferimento ad un sistema che permette di:
 - Acquisire automaticamente i dati necessari per l'identificazione di un oggetto, persona o animale.
 - Di inserire in modo automatico i dati acquisiti all'interno di programmi presenti all'interno di appositi calcolatori per il loro utilizzo successivo o real-time.



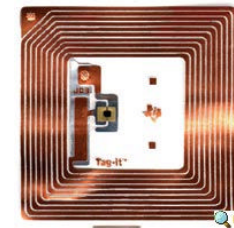
RFID vs Codice a Barre

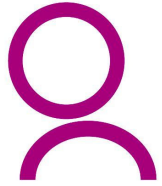
- L'RFID a differenza dei Codici a Barre o Bande Magnetiche:
 - Non ha bisogno della stretta vicinanza per essere letto (bande magnetiche)
 - Non deve essere visibile per essere letto (codici a barre)
 - Può anche aggiungere informazioni sui chip in funzione del tipo di Chip utilizzato (Read Only, Read Once, Read and Write)
 - Ha un tempo per l'identificazione e la verifica dell'ordine dei decimi/centesimi di secondo



Il Trasponder o Tag

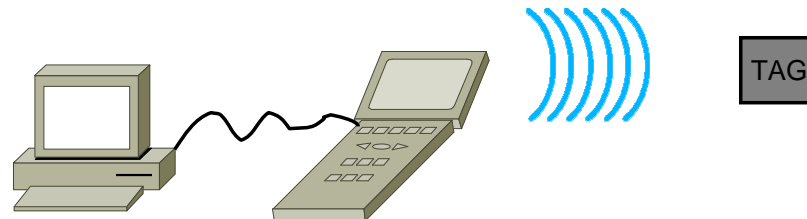
- L'elemento principale di un sistema RFID è costituito dal *Trasponder* o *Tag*.
 - E' un ricetrasmittitore che invia segnali radio a fronte di un'interrogazione, in base ad una cadenza prestabilita o in modo indotto.
 - Può contenere *dati* e *un numero univoco universale UID*.
 - Le applicazioni più frequenti utilizzano il Tag per inviare un segnale di risposta a fronte di un comando esterno necessario per attivare la risposta stessa.
- Il Tag può essere collegato ad un oggetto, una persona, un animale.





Il Lettore o Reader

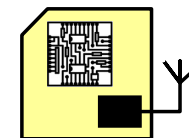
- Il secondo elemento in ordine di importanza è il *Lettore* o *Reader*.
- Il Lettore invia un segnale radio al Tag che ha lo scopo di:
 - Alimentare il Tag, se il Tag necessita di una miniaturizzazione che ne impedisce l'alimentazione propria (Tag passivo).
 - Sollecitare il Tag a fornire in risposta il proprio codice di identificazione o altri dati in aggiunta.

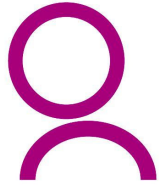




Architettura del *Trasponder* o *Tag*

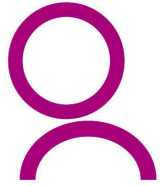
- Un *Trasponder* o *Tag* è costituito da 3 componenti elementari:
 - Il *Chip*: è il componente elettronico dove risiede l'intelligenza per la gestione di tutte le funzioni del trasponder (principalmente: comunicazione e identificazione).
 - L'*Antenna*: è il dispositivo che consente al *Tag* di essere alimentato e di ricevere/trasmettere le comunicazioni con il mondo esterno.
 - Il *Supporto*: è il materiale che sostiene e protegge l'antenna e il chip.





Architettura di un Lettore

- Il Lettore o Reader è costituito da due parti:
 - **L'Unità di Controllo:** è un microcalcolatore con un proprio OS che permette al Reader di gestire in tempo reale:
 - Le interfacce con le antenne (generalmente 4 o 8).
 - L'interrogazione dei Tag che entrano nel campo di azione delle antenne.
 - Le eventuali collisioni tra i messaggi di risposta dei Tag attivi.
 - L'interfaccia con i sistemi informativi tradizionali.
 - **Le Antenne:** sono i dispositivi per la comunicazione radio con i Tag e il loro conseguente interfacciamento. Le antenne possono avere diversi raggi d'azione e gestire Tag di caratteristiche diverse. Le antenne del reader possono anche alimentare i Tag (Tag passivi).
- Il lettore può supportare vari livelli di personalizzazione sulla base delle distanze di lettura, del numero di Tag da gestire e delle relative comunicazioni.



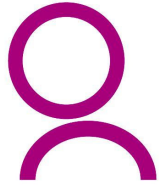
Tipologie di TAG

- La destinazione d'uso di un Sistema RFID ha un impatto limitato sulla struttura del Reader, per il quale è sufficiente dimensionare opportunamente le antenne e l'unità di controllo.
- L'impatto notevole si ha invece sui Tag a seconda delle prestazioni richieste in termini di distanza di lettura, di capacità di memorizzazione, di esposizione ad ambienti aggressivi e così via. Per questo motivo esistono diversi tipi di Tag che si distinguono in:
 - Chipless vs Chip.
 - Passivi, semipassivi, attivi.
 - Sola lettura, lettura/scrittura.



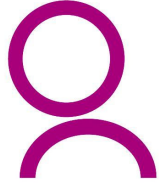
Tag Chipless vs Chip

- A seconda delle informazioni che il Tag deve gestire si possono avere chip di varia natura e costi diversi.
- Nel caso in cui l'informazione da gestire è binaria è possibile fare a meno della presenza del chip.
- Mediante l'applicazione di un piccolo tag chipless agli oggetti in vendita, un negozio può rilevare un eventuale transito non autorizzato di un articolo attraverso un varco. Il varco (composta da antenna) e' collegato ad un dispositivo di segnalazione acustica e visiva. Si parla in questo caso di EAS (*Electronic Article Surveillance*).
- L'EAS tuttavia non permette di rilevare né la tipologia né il numero degli oggetti rilevati.



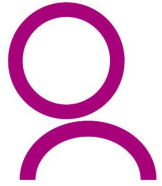
Tag Attivi e Passivi

- I **Tag attivi** hanno una fonte di alimentazione propria (p.e. una batteria). Questo fa sì che possono trasmettere anche se non interrogati. Non hanno bisogno di entrare nel raggio d'azione del Lettore per attivarsi e trasmettere. Possono comunicare a distanze anche dell'ordine dei Km. Per applicazioni sofisticate in aerei militari e civili, mezzi di trasporto in movimento a velocità elevate, ma anche per *l'home-automation*.
- I **Tag semipassivi** hanno una fonte di alimentazione propria ma trasmettono solo se interrogati dal Reader. Comunicano a distanze dell'ordine delle decine di metri. Per applicazioni speciali come il telepass per auto.
- I **Tag passivi** sono alimentati direttamente dal segnale emesso dal Reader. Comunicano a piccole distanze che possono arrivare a circa dieci metri.



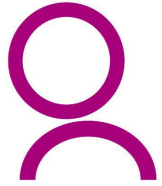
Tag read-only vs read/write

- I Tag possono contenere vari tipi di memorie:
- Le memorie di sola lettura (**ROM** *Read Only Memory*) sono preconfigurate dal costruttore con un numero limitato di informazioni, tra le quali il codice univoco del tag secondo la normativa ISO 15963. Le ROM sono poco costose e hanno vita lunga.
- **Trasponder a bit unico**: utilizzati per sistemi EAS antitaccheggio, indicano gli stati ON e OFF associabili a situazioni regolari o irregolari. Il trasponder è in generale realizzato con materiale magnetico o con circuiti risonanti.
- Le **WORM** (Write Once Read Memory) hanno la caratteristica di poter essere scritte una sola volta dall'utilizzatore che può così personalizzare il Tag.
- Le memorie **SRAM** (STATIC RANDOM ACCESS MEMORY) sono riscrivibili senza limitazione e possono raggiungere una alta densità di dati memorizzati. Necessitano di una fonte di energia permanente.
- Le **EEPROM** (ELECTRICALLY ERASABLE PROGRAMMABLE READ ONLY MEMORY) sono memorie riscrivibili che hanno la caratteristica di necessitare di fonte di energia solo in fase di lettura/scrittura. Sono in grado di mantenere i dati memorizzati anche per lunghi tempi (circa 10 anni). Ideali per Tag passivi.



Propagazione del segnale

- Esistono due principali modi di propagazione del segnale:
- Per induzione magnetica.
 - Un campo magnetico (per esempio generato da una corrente alternata) genera correnti elettriche in oggetti conduttori presenti nelle vicinanze (accoppiamento magnetico).
 - I trasponder hanno generalmente un'antenna costituita da una bobina di tipo:
 - Solenoidale: filo avvolto in aria o su nucleo di ferromagnetico (trasponder VLF)
 - Ad anello: filo avvolto intorno ad una o più spire (trasponder HF)
 - Le bande utilizzate sono:
 - VLF (125-134,2 KHz)
 - HF (13,56 MHz)
- Per propagazione di onde elettromagnetiche.
 - Si utilizzano le proprietà della propagazione dei campi elettrici per trasmettere energia e dati dal reader al trasponder e solo dati dal trasponder al reader. Le antenne hanno dimensioni dell'ordine della mezza lunghezza d'onda della radiazione emessa.
 - All'aumentare della frequenza diminuisce la dimensione dell'antenna (miniaturizzazione). All'aumentare della frequenza aumentano anche i costi di realizzazione dei trasponder.



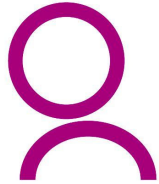
Prestazioni

- Nel considerare la bontà di un sistema RFID si possono tenere in considerazione le seguenti prestazioni:
 - Distanza e condizioni di lavoro tra reader e Tag.
 - Velocità di trasmissione delle informazioni.
 - Abilità a gestire più trasponder contemporaneamente (anticollisione).
 - Grado di errore nelle trasmissioni.
 - Compatibilità elettromagnetica con l'ambiente circostante
 - Dimensioni fisiche e protezione fisica dei trasponder.

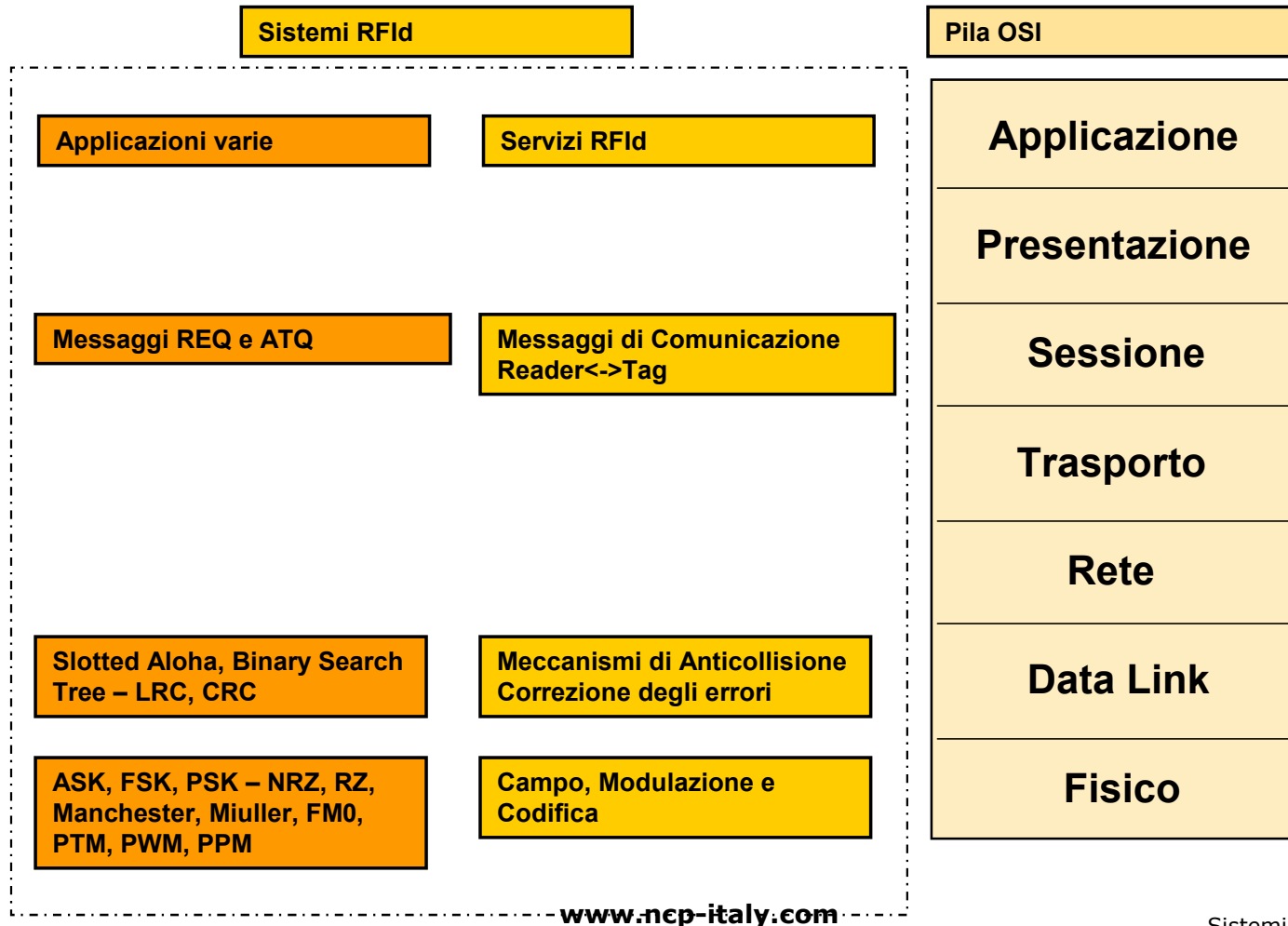


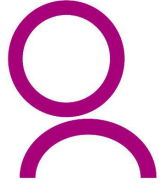
Il modello Trasmissivo

- Per realizzare una comunicazione affidabile Reader \leftrightarrow Tag è necessario considerare i seguenti elementi:
 - Modulazione e codifica dei segnali per minimizzare gli errori massimizzando il trasferimento di energia (gli ambienti possono presentare sensibili segnali di disturbo).
 - Gestione dell'anticollisione che permette di interrogare un Tag alla volta senza generare conflitti.
 - Realizzazione di un protocollo di comunicazione che offra le funzionalità di base per lo sviluppo di procedure di interrogazione e di risposta nella comunicazione Reader \leftrightarrow Tag.
- Avendo a disposizione questi elementi è possibile sviluppare i programmi applicativi per ogni specifico servizio RFID.



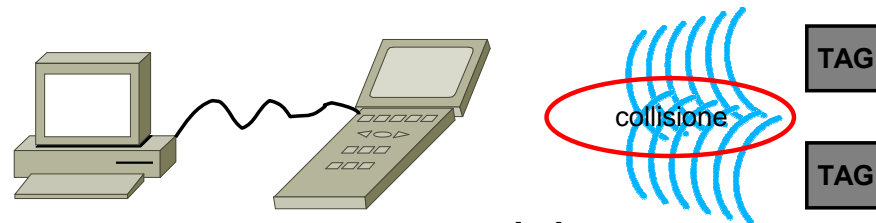
Sistemi RFID e pila OSI



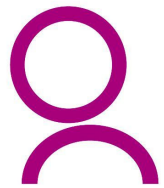


Identificazione dei Tag

- Nel raggio di copertura di un Reader possono essere presenti Tag multipli da identificare.
- Quando i Tag sono illuminati dal campo elettromagnetico del Reader possono rispondere simultaneamente generando delle **collisioni**.
- E' necessario quindi dotare il sistema di comunicazione Reader<->Tag di un meccanismo **anticollisioni**.
- Nei Tag è presente un codice univoco di identificazione chiamato SID (*Simultaneous IS*) che permette l'identificazione simultanea di più Tag all'interno del campo dello stesso Reader.

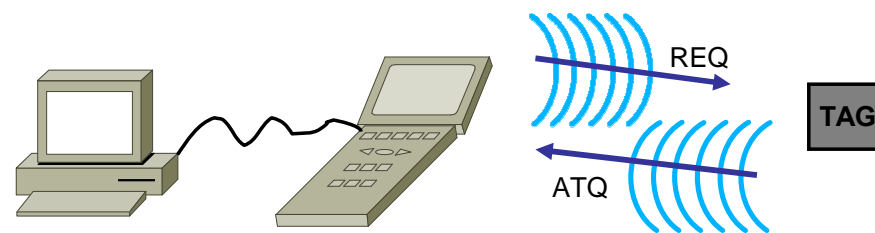


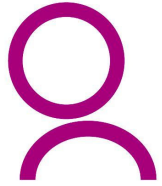
www.ncp-italy.com



Il processo di comunicazione

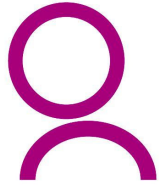
- Il processo di comunicazione tra reader e Tag può essere sintetizzato in due momenti:
- Il Reader invia un messaggio di Interrogazione **REQ** (*Request*) indicando al Tag il tipo di operazioni da eseguire.
- Il Tag risponde con un messaggio **ATQ** (*Answer to Request*) nel quale è presente il SID, eventuali dati aggiuntivi, la correttezza del dialogo, la presenza di errori, l'esito e il risultato delle operazioni eseguite.





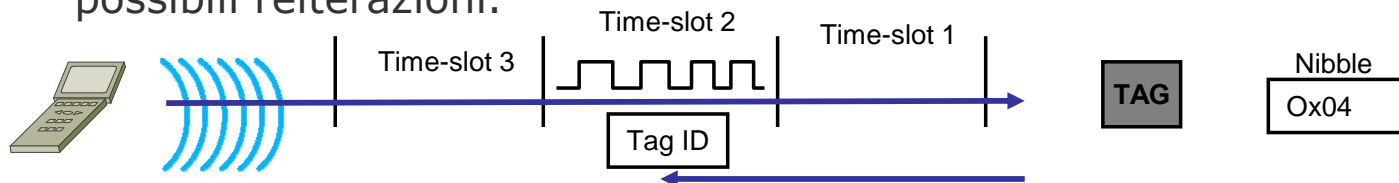
Il processo di Anticollisione

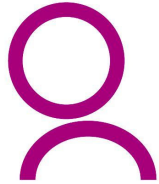
- Esistono due modelli di gestione del meccanismo di anticollisione:
 - Deterministico (ISO 14443 part 3 type A – “Binary search tree”)
 - Stocastico (ISO 14443 part 3 type B – “Slotted Aloha”)
- Il principio di funzionamento è basato sull’accesso multiplo a divisione di tempo TDMA (*time division multiple access*) .



Il processo di Anticollisione

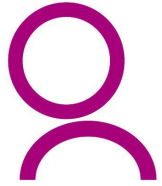
- Il reader esegue un *polling* verso i Tag presenti nel suo campo d'azione generando un certo numero di **partizioni temporali** ad ognuna delle quali associa un **treno di impulsi** crescente.
- Ogni **Tag conta il numero di impulsi** ricevuto per ogni time-slot e lo confronta con il cosiddetto *nibble* (4bit) più significativo del SID.
- Ogni **Tag risponde con il proprio SID**, utilizzando il *time-slot* che corrisponde al treno d'impulsi pari al valore contenuto nel nibble più significativo.
- Se **si verifica una collisione** perché due Tag hanno lo stesso valore di nibble, allora il reader
 - identifica un errore associandolo al time slot corrente
 - invia un messaggio di polling aggiuntivo per permettere ai Tag in collisione di cambiare time-slot andando a considerare il nibble immediatamente meno significativo
 - prosegue ai time-slot successivi
- Questo sistema permette di gestire 16 possibili trasponder con 16 possibili reiterazioni.





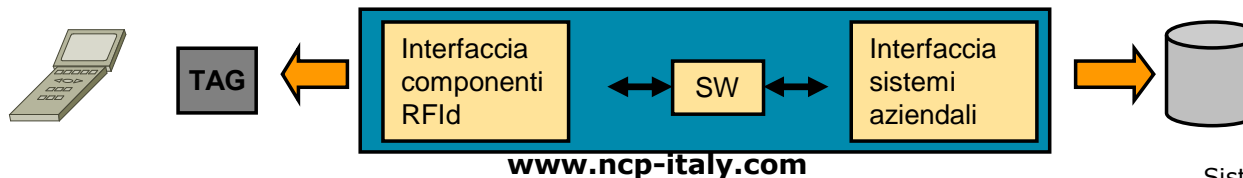
Frequenze di utilizzo

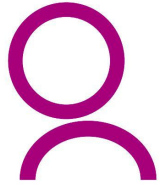
< 135 kHz	low frequency, inductive coupling	72 dB μ A/m
6.765 .. 6.795 MHz	medium frequency (ISM), inductive coupling	42 dB μ A/m
7.400 .. 8.800 MHz	medium frequency, used for EAS (electronic article surveillance) only	9 dB μ A/m
13.553 .. 13.567 MHz	medium frequency (13.56 MHz, ISM), inductive coupling, wide spread usage for contactless smartcards (ISO 14443, MIFARE, LEGIC, ...), smartlabels (ISO 15693, Tag-It, I-Code, ...) and item management (ISO 18000-3).	42 dB μ A/m
26.957 .. 27.283 MHz	medium frequency (ISM), inductive coupling, special applications only	42 dB μ A/m
433 MHz	UHF (ISM), backscatter coupling, rarely used for RFID	10 .. 100 mW
868 .. 870 MHz	UHF (SRD), backscatter coupling, new frequency, systems under development	500 mW, Europe only
902 .. 928 MHz	UHF (SRD), backscatter coupling, several systems	4 W - spread spectrum, USA/Canada only
2.400 .. 2.483 GHz	SHF (ISM), backscatter coupling, several systems, (vehicle identification: 2.446 .. 2.454 GHz)	4 W - spread spectrum, USA/Canada only, 500 mW, Europe
5.725 .. 5.875 GHz	SHF (ISM), backscatter coupling, rarely used for RFID	4 W USA/Canada, 500 mW Europe



Il Middleware RFId

- La gestione delle informazioni ricevute dai Tag attraverso i Reader è soggetta a vari momenti di manipolazione a seconda dello scopo a cui è destinato il sistema RFId.
- Per rendere possibile la corretta gestione dei flussi di informazione lungo l'intera catena del processo è necessario sviluppare dei programmi applicativi in grado di agire da **interfaccia intelligente** tra il mondo RFId e i sistemi di gestione aziendali.
- Questo strato di software che rappresenta il punto di integrazione tra i componenti attivi RFId e il mondo dei processi ERP viene chiamato: **Middleware RFId**.



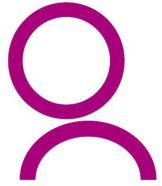


Gli standard

- Gli standard sono principalmente redatti dalla ISO (*International Organization of Standardization*) in collaborazione con IEC (*International Electric Committee*).
- In particolare la struttura dei comitati/sottocomitati/gruppi di lavoro è:



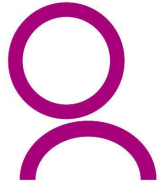
- **JTC1** (*Joint Technical Committee 1 on IT*)
 - **SC31** (*Automatic identification and data capture techniques*), **SC17** (*Cards and personal identification*)
 - SC31/WG1, SC31/WG2, SC31/WG3, SC31/WG4, SC31/WG5, SC31/WG8
 - SC17/WG4, SC17/WG8, SC17/WG1



Gli standard

Riportiamo di seguito alcuni degli standard più noti:

- ISO 10536 (ISO SC17/WG8) - *Close coupled cards*
- ISO 14443 (ISO SC17/WG8) - *proximity cards*
- ISO 15693 (ISO SC17/WG8) - *vicinity cards*
- ISO 10373 (SC17/WG1/8) *Identification cards - Test Methods*
- ISO 15960 (SC31 WG2/4) - *RFID for Item Management; - Transaction Message Profiles*
- ISO 15961 (SC31 WG2/4) - *RFID for Item Management; - Host Interrogator - Tag functional commands and other syntax features*
- ISO 15962 (SC31 WG2/4) - *RFID for Item Management; - Data Syntax*
- ISO 15963 (SC31 WG2/4 - *Unique identification of RF Tag and Registration Authority to manage the uniqueness*
- ISO/IEC TR 18000 (SC31 WG4/SG3) - *RFID for item Management; Air Interface*
- ISO 18001 (SC31 WG4) - *Information technology - RFID for Item Management - Application Requirements Profiles*



Le applicazioni

- GESTIONE DEI MAGAZZINI E DEI PUNTI VENDITA
- GESTIONE DEI TRASPORTI
- CONTROLLO DI CARICO E SCARICO
- CONTROLLO PRESENZE E ACCESSI
- SICUREZZA SUL LAVORO
- TRACCIAMENTO PRATICHE
- ASSISTENZA E MANUTENZIONE
- LOGISTICA
- IDENTIFICAZIONE DEGLI ANIMALI
- GESTIONE BIBLIOTECHE
- SISTEMI ANTITACCHEGGIO
- RILEVAZIONE DEI PARAMETRI AMBIENTALI
- CATENA DEL FREDDO E DEL FRESCO



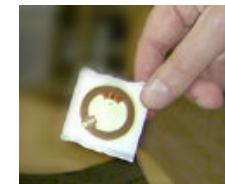
La sicurezza

- Un'equipe di ricercatori della Vrije Universiteit, polo universitario olandese, precisamente di Amsterdam in occasione della *Pervasive Computing and Communications Conference* tenutasi a Pisa il 15 marzo 2006, ha mostrato come fosse possibile inserire un virus che va ad "infettare" parte di un chip a radio frequenza.
- Fino ad ora il problema della sicurezza, ed in particolare degli effetti di codice "dannoso" inserito in un tag, veniva considerato una questione marginale rispetto ad altri ambiti: la ricerca del gruppo olandese ha invece dimostrato come debbano esserci preoccupazioni lecite a riguardo, che giustificano lo studio di contromisure adeguate alla situazione. E' evidente come un tag danneggiato possa compromettere ogni attività in cui è utilizzato: si pensi alla sicurezza sulla merce in un supermercato o ad un intero processo industriale oppure ancora in ambito sanitario. Una delle motivazioni di questa insicurezza, secondo i ricercatori, si trova nel costo della tecnologia e nella tendenza del mercato: il tentativo di costruire dispositivi a radio frequenza sempre più economici infatti, non garantisce sempre un alto livello di sicurezza del prodotto.

Estratto da www.newsrfid.com

Secondo il portale rfidvirus.org, questa è la foto del primo RFID infetto al mondo

www.ncp-italy.com



Sistemi RFID 1 - 27