

La tecnologia RFId

Mattia Cavenaghi (mat. 736856)

Università degli Studi di Milano

Dipartimento di Tecnologie dell'Informazione (Crema)

23 Luglio 2010

Indice

Di cosa si parlerà in questa presentazione?

Indice

Di cosa si parlerà in questa presentazione?

L'RFId dal punto di vista...

- ① *tecnologico;*
- ② *architetturale (sistema informativo aziendale);*
- ③ *degli standard;*
- ④ *delle normative;*
- ⑤ *delle minacce alla sicurezza ed alla privacy;*
- ⑥ *applicativo: Verichip.*

Cos'è l'RFId?

Definizione

La *Radio Frequency Identification (RFId)* é la tecnologia che consente l'identificazione di oggetti etichettati, senza che questi siano visibili da un operatore sia esso umano o automatico.

Cos'è l'RFId?

Definizione

La *Radio Frequency Identification (RFId)* é la tecnologia che consente l'identificazione di oggetti etichettati, senza che questi siano visibili da un operatore sia esso umano o automatico.

Il sistema é composto da:

- uno o più *lettori* (dispositivi wireless, es. PDA);

Cos'è l'RFId?

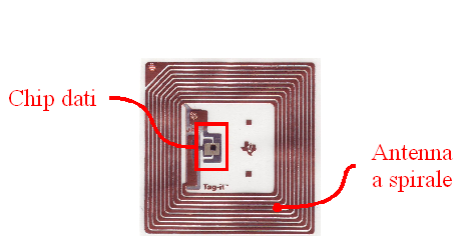
Definizione

La *Radio Frequency Identification (RFId)* è la tecnologia che consente l'identificazione di oggetti etichettati, senza che questi siano visibili da un operatore sia esso umano o automatico.

Il sistema è composto da:

- uno o più *lettori* (dispositivi wireless, es. PDA);
- uno o più *tag* (IC = microchip + antenna [+ batteria]):
 - *attivi*;
 - *passivi*;
 - *semi-attivi* o *semi-passivi*.

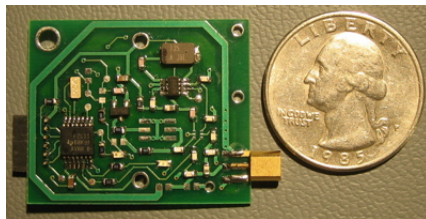
Esempi di tag RFId



Esempio di tag RFId passivo.



Esempio di tag RFId attivo.



Esempio di tag RFId semi-attivo (o semi-passivo).

Frequenze RFId standardizzate

Frequenza	Tipo frequenza	A-P-A/P	ISO	EPC
125/134 kHz	LF	P	18000-2	-
13.56 MHz	HF	P	18000-3	-
868/915 MHz	UHF	A-P-A/P	18000-6	Class 1 Gen 2
> di 2.4 GHz	UWB	A-P-A/P	18000-4	-

L'EPCglobal Network (1/3)

Definizione

É il sistema informativo RFId, standardizzato dalla EPCglobal, che si basa sulla possibilità di identificare in modo semplice ed efficace le merci movimentate nella supply chain aziendale.

L'EPCglobal Network (1/3)

Definizione

É il sistema informativo RFId, standardizzato dalla EPCglobal, che si basa sulla possibilità di identificare in modo semplice ed efficace le merci movimentate nella supply chain aziendale.

Importante!!!

L'EPCglobal Network é tecnologicamente indipendente!!!

L'EPCglobal Network (2/3)

Il sistema é formato da:

- *EPC (Electronic Product Code);*

L'EPCglobal Network (2/3)

Il sistema é formato da:

- *EPC (Electronic Product Code);*
- *ID System;*

L'EPCglobal Network (2/3)

Il sistema é formato da:

- *EPC (Electronic Product Code);*
- *ID System;*
- *EPC middleware (o middleware RFId);*

L'EPCglobal Network (2/3)

Il sistema é formato da:

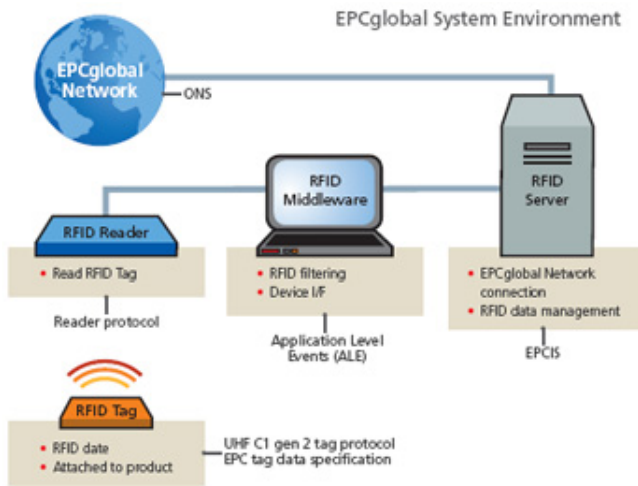
- *EPC (Electronic Product Code);*
- *ID System;*
- *EPC middleware (o middleware RFId);*
- *Object Naming Service (ONS);*

L'EPCglobal Network (2/3)

Il sistema é formato da:

- *EPC (Electronic Product Code);*
- *ID System;*
- *EPC middleware (o middleware RFId);*
- *Object Naming Service (ONS);*
- *EPC Information Service (EPCIS).*

L'EPCglobal Network (3/3)



Standard ISO (1/2)

Definizione

L'*ISO* (*International Organization for Standardization*) é il più grande ente a livello mondiale nato con l'obiettivo di sviluppare e pubblicare standard internazionali, in modo tale da creare un punto di incontro tra i bisogni della società e le applicazioni aziendali.

Standard ISO (2/2)

Tra la moltitudine di documenti inerenti l'ISO, si ricordano:

- *ISO 11784, ISO 11785 ed ISO 14223*: etichettatura e riconoscimento animali;

Standard ISO (2/2)

Tra la moltitudine di documenti inerenti l'ISO, si ricordano:

- *ISO 11784, ISO 11785 ed ISO 14223*: etichettatura e riconoscimento animali;
- *ISO/IEC 14443*: proximity card;

Standard ISO (2/2)

Tra la moltitudine di documenti inerenti l'ISO, si ricordano:

- *ISO 11784, ISO 11785 ed ISO 14223*: etichettatura e riconoscimento animali;
- *ISO/IEC 14443*: proximity card;
- *ISO/IEC 15961 ed ISO/IEC 15962*: interfaccia applicazioni e protocollo dati;

Standard ISO (2/2)

Tra la moltitudine di documenti inerenti l'ISO, si ricordano:

- *ISO 11784, ISO 11785 ed ISO 14223*: etichettatura e riconoscimento animali;
- *ISO/IEC 14443*: proximity card;
- *ISO/IEC 15961 ed ISO/IEC 15962*: interfaccia applicazioni e protocollo dati;
- *ISO/IEC 15693*: vicinity card;

Standard ISO (2/2)

Tra la moltitudine di documenti inerenti l'ISO, si ricordano:

- *ISO 11784, ISO 11785 ed ISO 14223*: etichettatura e riconoscimento animali;
- *ISO/IEC 14443*: proximity card;
- *ISO/IEC 15961 ed ISO/IEC 15962*: interfaccia applicazioni e protocollo dati;
- *ISO/IEC 15693*: vicinity card;
- *ISO/IEC 18000*: interfacce RFId;

Standard ISO (2/2)

Tra la moltitudine di documenti inerenti l'ISO, si ricordano:

- *ISO 11784, ISO 11785 ed ISO 14223*: etichettatura e riconoscimento animali;
- *ISO/IEC 14443*: proximity card;
- *ISO/IEC 15961 ed ISO/IEC 15962*: interfaccia applicazioni e protocollo dati;
- *ISO/IEC 15693*: vicinity card;
- *ISO/IEC 18000*: interfacce RFId;
- *ISO/IEC 18046 ed ISO/IEC 18047*: testing dei dispositivi RFId;

Standard ISO (2/2)

Tra la moltitudine di documenti inerenti l'ISO, si ricordano:

- *ISO 11784, ISO 11785 ed ISO 14223*: etichettatura e riconoscimento animali;
- *ISO/IEC 14443*: proximity card;
- *ISO/IEC 15961 ed ISO/IEC 15962*: interfaccia applicazioni e protocollo dati;
- *ISO/IEC 15693*: vicinity card;
- *ISO/IEC 18000*: interfacce RFId;
- *ISO/IEC 18046 ed ISO/IEC 18047*: testing dei dispositivi RFId;
- *ISO/IEC 19762 ed ISO/IEC 24730: Automatic Identification and Data Capture (AIDC) e Real-Time Locating System (RTLS)*.

L'EPC (Electronic Product Code)

Definizione

L'EPC è un insieme di codifiche di identificazione o standard di numerazione, che a differenza dei codici a barre consente di identificare un prodotto in modo univoco attraverso il suo ID.

Struttura dell'EPC

EPC a 96 bit (GID-96)			
<i>Header</i>	<i>EPC Manager Number</i>	<i>Object class</i>	<i>Serial number</i>
8 bit	28 bit	24 bit	36 bit

Struttura dell'EPC

EPC a 96 bit (GID-96)			
<i>Header</i>	<i>EPC Manager Number</i>	<i>Object class</i>	<i>Serial number</i>
8 bit	28 bit	24 bit	36 bit

I campi del codice EPC sono:

- *Header*: identifica la codifica EPC utilizzata;

Struttura dell'EPC

EPC a 96 bit (GID-96)			
<i>Header</i>	<i>EPC Manager Number</i>	<i>Object class</i>	<i>Serial number</i>
8 bit	28 bit	24 bit	36 bit

I campi del codice EPC sono:

- *Header*: identifica la codifica EPC utilizzata;
- *EPC Manager Number*: identifica l'azienda che gestisce l'oggetto taggato;

Struttura dell'EPC

EPC a 96 bit (GID-96)			
<i>Header</i>	<i>EPC Manager Number</i>	<i>Object class</i>	<i>Serial number</i>
8 bit	28 bit	24 bit	36 bit

I campi del codice EPC sono:

- *Header*: identifica la codifica EPC utilizzata;
- *EPC Manager Number*: identifica l'azienda che gestisce l'oggetto taggato;
- *Object Class*: identifica la classe dell'oggetto taggato;

Struttura dell'EPC

EPC a 96 bit (GID-96)			
<i>Header</i>	<i>EPC Manager Number</i>	<i>Object class</i>	<i>Serial number</i>
8 bit	28 bit	24 bit	36 bit

I campi del codice EPC sono:

- *Header*: identifica la codifica EPC utilizzata;
- *EPC Manager Number*: identifica l'azienda che gestisce l'oggetto taggato;
- *Object Class*: identifica la classe dell'oggetto taggato;
- *Serial Number*: identifica l'istanza (l'oggetto).

Codifiche EPC (1/3)

L'ultima versione dell'*EPCglobal Tag Data Standards* (la versione 1.4) formalizza tredici tipologie di codice:

- *General Type*: questo standard definisce un tipo di identificatore generale, indipendente da qualsiasi specifica o schema di identificazione esistente:
 - *General Identifier (GID-96)*.

Codifiche EPC (2/3)

- *versioni serializzate del GS1*: sfruttano le conoscenze e la struttura dei codici a barre formalizzati nel GS1 (*Global Services*):
 - *Global Trade Item Number (SGTIN-96 SGTIN-198)*: assegnato agli oggetti (prodotti o servizi) che necessitano di essere prezzati, ordinati o richiamati all'interno di una *supply chain*;
 - *GS1 Serial Shipping Container Code (SSCC-96)*: tracciamento del trasporto e l'immagazzinamento dei beni;
 - *GS1 Global Location Number (SGLN-96 e SGLN-195)*: identifica un luogo fisico od entità legali (aziendali);
 - *GS1 Global Returnable Asset Identifier (GRAI-96 e GRAI-170)*: tracciamento di imballaggi riutilizzabili o macchinari di trasporto;
 - *GS1 Global Individual Asset Identifier (GIAI-96 e GIAI-202)*: tracciamento del ciclo di vita dei beni;
 - *Global Service Relation Number (GSRN-96)*: identifica il destinatario di un servizio in un contesto di collaborazioni aziendali;
 - *Global Document Type Identifier (GDTI-96)*: identifica le tipologie di documento accessibili nei database aziendali.

Codifiche EPC (3/3)

- *DOD Construct (DoD-96)*: identifica i beni destinati e provenienti dal Dipartimento della Difesa U.S.A.

Classi EPC

Durante il suo ciclo di vita, EPCglobal ha sviluppato diversi protocolli:

- *Class 0*: identifica una tipologia di tag in sola lettura, programmabili all'atto di fabbricazione del chip;
- *Class 1: identifica una tipologia di tag passivi, semplice dotati di una memoria scrivibile un sola volta;*
- *Class 2*: identifica tag passivi con una memoria di 65 Kb;
- *Class 3*: identifica tag semi-passivi dotati di una memoria di 65 Kb; é essenzialmente un tag Class 2 dotato di una batteria tale da incrementare il raggio operativo di trasmissione/ricezione dei segnali;
- *Class 4*: identifica tag attivi dotati di batteria la quale consente l'alimentazione del tag e la trasmissione broadcast dei segnali;
- *Class 5*: identifica tag attivi che possono comunicare con altri tag di Class 5.

Provvedimento sulla privacy del 9 Marzo 2005

Partendo con il presupposto che l'utilizzo della tecnologia RFId deve rispettare tutti gli articoli del *Codice in materia di protezione dei dati personali* (D.Lgs 196/2003), gli utilizzatori devono porre particolare attenzione sui seguenti articoli:

- *principio di necessità* (art. 3);
- *liceità* (art. 11, comma 1, lett. a));
- *finalità e qualità dei dati* (art. 11, comma 1, lett. b), c), d) e e));
- *proporzionalità* (art. 11, comma 1, lett. d));
- *informativa* (art. 13);
- *trattamento da parte di privati*;
- *esercizio dei diritti* (artt. 7-10);
- *disattivazione o rimozione delle etichette*;
- *impianto sottocutaneo di microchip*;
- *ulteriori prescrizioni*.

Minacce alla sicurezza ed alla privacy (1/2)

La tecnologia RFId è di tipo *wireless* e molto invasiva, questi due fattori contribuiscono alle seguenti tipologie di attacco:

- *attacco fisico*: acquisizione o modifica fisica dei dati attraverso manipolazione fisica del tag → realizzare tag anti manomissione, schermature;

Minacce alla sicurezza ed alla privacy (1/2)

La tecnologia RFId è di tipo *wireless* e molto invasiva, questi due fattori contribuiscono alle seguenti tipologie di attacco:

- *attacco fisico*: acquisizione o modifica fisica dei dati attraverso manipolazione fisica del tag → realizzare tag anti manomissione, schermature;
- *skimming* (trad. *strisciare*): acquisizione dei dati a distanza (es. PDA) → autenticazione del lettore, schermature, blocker tag o RFId Guardian;

Minacce alla sicurezza ed alla privacy (1/2)

La tecnologia RFId è di tipo *wireless* e molto invasiva, questi due fattori contribuiscono alle seguenti tipologie di attacco:

- *attacco fisico*: acquisizione o modifica fisica dei dati attraverso manipolazione fisica del tag → realizzare tag anti manomissione, schermature;
- *skimming* (trad. *strisciare*): acquisizione dei dati a distanza (es. PDA) → autenticazione del lettore, schermature, blocker tag o RFId Guardian;
- *spoofing* (trad. *imbrogliare*): utilizzo di tag contraffatti per l'accesso fraudolento ad un sistema → autenticazione con chiave segreta;

Minacce alla sicurezza ed alla privacy (1/2)

La tecnologia RFId è di tipo *wireless* e molto invasiva, questi due fattori contribuiscono alle seguenti tipologie di attacco:

- *attacco fisico*: acquisizione o modifica fisica dei dati attraverso manipolazione fisica del tag → realizzare tag anti manomissione, schermature;
- *skimming* (trad. *strisciare*): acquisizione dei dati a distanza (es. PDA) → autenticazione del lettore, schermature, blocker tag o RFId Guardian;
- *spoofing* (trad. *imbrogliare*): utilizzo di tag contraffatti per l'accesso fraudolento ad un sistema → autenticazione con chiave segreta;
- *Denial of Service (DoS, trad: interruzione del servizio)*: modifica del normale funzionamento di un sistema (*jamming*) → monitoraggio delle frequenze, routine di controllo;

Minacce alla sicurezza ed alla privacy (2/2)

- *eavesdropping* (trad. *origliare*): ascolto in modo passivo e non autorizzato la comunicazione RFId → crittografia delle comunicazioni;

Minacce alla sicurezza ed alla privacy (2/2)

- *eavesdropping* (trad. *origliare*): ascolto in modo passivo e non autorizzato la comunicazione RFId → crittografia delle comunicazioni;
- *tracking* (trad. *monitoraggio*): tracciamento degli spostamenti nel tempo e nello spazio dei tag (ID) → schermature, RFId Guardian, pseudonimi;

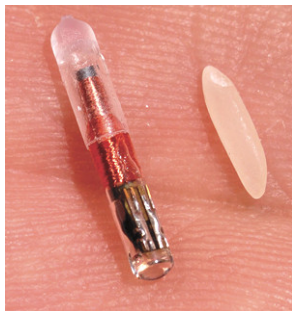
Minacce alla sicurezza ed alla privacy (2/2)

- *eavesdropping* (trad. *origliare*): ascolto in modo passivo e non autorizzato la comunicazione RFId → crittografia delle comunicazioni;
- *tracking* (trad. *monitoraggio*): tracciamento degli spostamenti nel tempo e nello spazio dei tag (ID) → schermature, RFId Guardian, pseudonimi;
- *relay attacks* (trad. *attacchi a staffetta*): *man-in-the-middle* → schermatura, RFId Guardian, *autenticazione a due fattori*;

Minacce alla sicurezza ed alla privacy (2/2)

- *eavesdropping* (trad. *origliare*): ascolto in modo passivo e non autorizzato la comunicazione RFId → crittografia delle comunicazioni;
- *tracking* (trad. *monitoraggio*): tracciamento degli spostamenti nel tempo e nello spazio dei tag (ID) → schermature, RFId Guardian, pseudonimi;
- *relay attacks* (trad. *attacchi a staffetta*): *man-in-the-middle* → schermatura, RFId Guardian, *autenticazione a due fattori*;
- *virus RFId*: aggressione al back-end ed al sistema RFId → disabilitazione dello scripting lato back-end, limitazione dell'accesso ai database, vincoli sul tipo di parametri e dati elaborati nel processo di comunicazione.

Verichip (1/3)



Tag Verichip.

Obiettivo:

- accesso da parte del personale medico ai dati relativi ai pazienti in cura.

Verichip (2/3)

Caratteristiche tecniche:

- tag passivo (125 kHz);
- ID: numero univoco a 16 cifre in chiaro, simile al *Social Security Number (USA)* od ai codici a barre;
- capsula di vetro rivestita di *Biobond*;
- innestato attraverso l'operazione di *chipping*: nel braccio tra gomito e spalla del braccio destro (quasi invisibile).

Verichip (3/3)

Problemi relativi alla privacy:

- i dati sono in chiaro \rightarrow spychip.

Verichip (3/3)

Problemi relativi alla privacy:

- i dati sono in chiaro → spychip.

Problemi relativi alla sicurezza:

- i dati non sono crittati, non c'è autorizzazione selettiva del lettore → inserire il tag in un braccialetto;
- ... nel 2006 é stato clonato l'identificatore contenuto in un VeriChip e sul web sono pubblicate le istruzioni per la clonazione.

Verichip (3/3)

Problemi relativi alla privacy:

- i dati sono in chiaro → spychip.

Problemi relativi alla sicurezza:

- i dati non sono crittati, non c'è autorizzazione selettiva del lettore → inserire il tag in un braccialetto;
- ... nel 2006 é stato clonato l'identificatore contenuto in un VeriChip e sul web sono pubblicate le istruzioni per la clonazione.

In Italia?

- utilizzo solo in “...casi eccezionali, per comprovate e giustificate esigenze a tutela della salute delle persone...” (Provvedimento del Garante della privacy, 9 Marzo 2005).

Verichip (3/3)

Problemi relativi alla privacy:

- i dati sono in chiaro → spychip.

Problemi relativi alla sicurezza:

- i dati non sono crittati, non c'è autorizzazione selettiva del lettore → inserire il tag in un braccialetto;
- ... nel 2006 é stato clonato l'identificatore contenuto in un VeriChip e sul web sono pubblicate le istruzioni per la clonazione.

In Italia?

- utilizzo solo in “...casi eccezionali, per comprovate e giustificate esigenze a tutela della salute delle persone...” (Provvedimento del Garante della privacy, 9 Marzo 2005).

Conclusione?

- il progetto *Health Link* é stato abbandonato a causa della mancanza di volontari per il testing...

Fonti

Per l'approfondimento presentato, si sono consultati:

- *Wikipedia*: definizioni ed articolo di partenza sull'RFId, http://it.wikipedia.org/wiki/Pagina_principale.
- *ISO*: standard, <http://www.iso.org/iso/home.html>.
- *EPCglobal*: standard e relativi approfondimenti, <http://www.epcglobalinc.org/home/>.
- *RFIDjournal*: notizie ed approfondimenti relativi alla tecnologia RFId, <http://www.rfidjournal.com/>.
- *Garante per la protezione dei dati personali*: legislazione italiana relativa all'utilizzo dell'RFId, <http://www.garanteprivacy.it/garante/navig/jsp/index.jsp>.
- *Comitato Antichip*: "comitato" U.S.A. contro l'impiego del Verichip, <http://www.antichips.com/default.htm>.

Fine

Grazie per la cortese attenzione...

Fine

Grazie per la cortese attenzione...

