

Progetto di "Sicurezza e Privacy"

# La tecnologia RFId



~ Docente ~

dott.ssa C. Braghin

~ Studente ~

Mattia Cavenaghi

Matricola 736856

Anno Accademico 2009/10

## Indice

<b>1</b>	<b>La tecnologia RFId</b>	<b>4</b>
1.1	Definizione . . . . .	4
1.2	I tag RFId . . . . .	4
1.2.1	Tag attivi . . . . .	6
1.2.2	Tag passivi . . . . .	7
1.2.3	Tag semi-attivi (o semi-passivi) . . . . .	8
<b>2</b>	<b>Architettura dei sistemi RFId (EPCglobal Network)</b>	<b>9</b>
2.1	Componenti del sistema EPCglobal Network . . . . .	9
2.2	Funzionamento del sistema EPCglobal Network . . . . .	10
<b>3</b>	<b>Standard inerenti l'RFId</b>	<b>12</b>
3.1	Gli standard ISO . . . . .	12
3.2	Electronic Product Code (EPC) . . . . .	14
3.2.1	Struttura dell'EPC . . . . .	14
3.2.2	Classificazione dei tag secondo lo standard EPC . . . . .	16
<b>4</b>	<b>Normative inerenti l'RFId</b>	<b>18</b>
4.1	Richiami dal D.Lgs 196/2003 (Codice in materia di protezione dei dati personali) . . . . .	18
<b>5</b>	<b>Minacce alla sicurezza ed alla privacy</b>	<b>21</b>
<b>6</b>	<b>VeriChip</b>	<b>25</b>
	<b>Riferimenti bibliografici</b>	<b>27</b>

## Introduzione

Il presente elaborato si propone di approfondire le tematiche connesse alla tecnologia RFId non affrontate nel corso di riferimento. La presente relazione é articolata in sei sezioni:

- *sezione 1:* dove si definisce la tecnologia RFId e si presentano le caratteristiche dei dispositivi coinvolti nei processi di comunicazione;
- *sezione 2:* dove si presenta l'infrastruttura tecnologica adottata dalle principali aziende che utilizzano l'RFId e standardizzata dalla *EPCglobal*;
- *sezione 3:* dove vengono illustrati i principali standard internazionali che hanno consentito l'uniformazione dei dati, delle infrastrutture tecnologiche e dei processi di comunicazione RFId;
- *sezione 4:* dove é vengono effettuati gli opportuni richiami alle norme che regolano l'utilizzo della tecnologia in oggetto nello stato italiano;
- *sezione 5:* dove si sono descritte le principali tipologie di attacco (e le relative contromisure), riscontrate in letteratura;
- *sezione 6:* dove si conclude la nostra esposizione, presentando un caso applicativo analizzato sfruttando i concetti definiti nelle precedenti sezioni: l'utilizzo del *VeriChip*.

Un'ultima sezione è dedicata ai riferimenti bibliografici che riassumono le fonti consultate durante la stesura della presente relazione.

## 1 La tecnologia RFID

### 1.1 Definizione

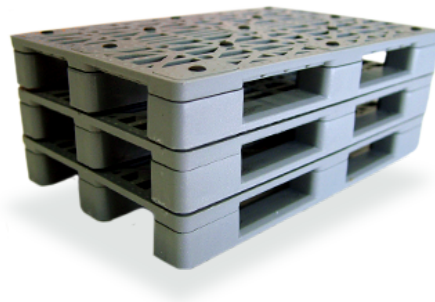
La *Radio Frequency Identification (RFID)* é la tecnologia che consente l'Identificazione di oggetti etichettati, senza che questi siano visibili da un operatore sia esso umano o automatico. Il sistema consiste di un *lettore*, di un *calcolatore elettronico* e di alcuni *tag*, contenenti un microchip ed un'antenna, che vengono posizionati direttamente sull'oggetto da rilevare [5].

Ci sono differenti modalità secondo cui i tag ed i lettori possono comunicare, queste comunicazioni devono seguire tutte un preciso standard e non tutti i lettori possono leggere le varie tipologie di tag.

Le dimensioni dei tag variano in base alla dimensione dell'antenna: possono essere molto piccoli in modo tale da essere incollati sugli oggetti (figura 1a), o molto grandi in modo tale da essere attaccati ai pallet (figura 1b): infine alcuni tag contengono grandi quantità di informazioni, altri solamente un identificativo numerico.



(a)



(b)

Figura 1: esempi di applicazione della tecnologia RFID: (1a) tag RFID passivi in fase di stampa termica; (1b) i bancali qui rappresentati contengono al loro interno un tag RFID passivo riscrivibile che consente l'identificazione delle merci trasportate. (Fonte immagini: (1a) <http://www.italora.com/>, (1b) <http://www.ipallet.it/>)

### 1.2 I tag RFID

L'elemento che caratterizza un sistema RFID è il *transponder* o *tag*, un componente elettronico composto da un *chip* ed una *antenna* (figura (3)). Il chip (grande pochi millimetri) è la parte "intelligente" costituita da una memoria non

volatile contenente un codice unico, il quale viene trasmesso tramite l'antenna (circuitto di trasmissione del segnale) all'apparato lettore che controllerà i dati ricevuti.

Si possono anche aggiungere informazioni sui chip in funzione della tipologia:

- *Read Only*: si possono solo leggere le informazioni contenute;
- *Write Once, Read Many (WORM)*: si possono scrivere nel chip le informazioni una sola volta, ma leggerle un numero illimitato di volte;
- *Read and Write*: si possono leggere e memorizzare informazioni per un numero limitato ma grande di volte. La modalità Read/Write permette non solo una trasmissione di informazioni ma un loro aggiornamento sul chip. Il tag diventa un sistema di identificazione che può tenere traccia della storia di un prodotto fin dalla fase di lavorazione ed essere poi utilizzata in modo interattivo lungo tutta la filiera fino alla distribuzione al dettaglio e in alcuni casi sino al consumatore.

Il vantaggio offerto da questo tipo di tecnologia rispetto ai sistemi di identificazione attualmente più utilizzati (codici a barre e lettori a banda magnetica), è che il lettore (fisso o portatile) non ha bisogno di avere la visibilità ottica rispetto all'etichetta e funziona in tempi estremamente ridotti (circa un decimo di secondo), il sistema è inoltre capace di resistere, con opportune protezioni, all'aggressione di agenti chimici e ambientali, di poter operare immerso in un fluido, dentro l'oggetto che si vuole identificare oppure all'interno di un altro contenitore (purché non completamente metallici) infine sussiste la possibilità di leggere, nello stesso contenitore, il codice di decine o centinaia di etichette in un lasso temporale di pochi secondi, e di trasmetterlo al sistema informativo di gestione [19].

Esistono diversi tipi di tag RFID, alcuni dei quali normati da standard ISO e suddivisi in base alla frequenza od all'operatività del segnale.

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
maggiori di 2.4 GHz	UWB	A-P-A/P	18000-4	-

Tabella 1: classificazione dei tag RFID [12].

I tag 125 kHz 13.56 MHz sono contemplati dalle norme ISO come *passivi* mentre per i tag RFId UHF e Ultrawide band (UWB) sono classificati come *attivi*, *passivi* e *semi-attivi*.

### 1.2.1 Tag attivi

Si definisce un *tag attivo* quando è equipaggiato con una batteria che consente di alimentare totalmente o parzialmente la circuiteria e l'antenna contenuti al suo interno (figura 2): alcuni tag contengono una batteria sostituibile della durata di diversi anni, mentre altri tag sono "sigillati" contenenti batteria non sostituibile. In ogni caso è possibile connettere il tag ad una sorgente di alimentazione esterna [14].

I principali *vantaggi* dei tag attivi sono:

- possono essere letti tramite lettori posti a grande distanza dal tag (maggiore di 30 m);
- possono essere equipaggiati con altri sensori;
- come i lettori, incorporano ricevitore e trasmettitore [4].

I principali *svantaggi* dei tag attivi sono:

- non possono ovviamente funzionare senza una batteria che ne limita il ciclo di vita operativo;
- rispetto ai tag passivi, in questa tipologia di tag la sostituzione delle batterie incide marcatamente sui costi di mantenimento del sistema adottato;
- gli scompensi energetici dovuti alle batterie esaurite si può causare la corruzione dei dati inviati;
- sono costosi, poiché hanno un costo minimo di \$20 cadauno;
- sono fisicamente ingombranti fattore che ne limita i campi applicativi d'impiego.

I tag attivi possono essere utilizzati in applicazioni che richiedono:

- capacità di eseguire monitoraggi, controlli e diagnostiche in modo indipendente;
- capacità di avviare i processi di comunicazione;

- capacità di calcolare il miglior percorso di instradamento dei dati (networking);
- utilizzo nelle comunicazioni a banda larga.



Figura 2: esempio di tag Attivo, nel cerchio rosso è evidenziata la batteria di alimentazione dell' IC (Fonte immagine: <http://realtimeid.com/index.html>).

### 1.2.2 Tag passivi

Si definisce un *tag passivo* quando non contiene una sorgente di alimentazione autonoma poiché fornita esternamente dal lettore: le onde radio emesse dal lettore che irradiano l'antenna contenuta all'interno del tag, generano un campo elettromagnetico fornendo energia al circuito ricevente e consentendo al tag di inviare le informazioni codificate all'interno del proprio chip [14].

I principali *vantaggi* dei tag passivi sono:

- funzionano senza batteria;
- hanno una durata di venti anni o più;
- sono meno costosi dei tag attivi;
- sono molto piccoli.

I principali *svantaggi* dei tag passivi sono:

- possono essere letti solo a brevi distanze (minori di 2 m HF, minore di 6 m UHF);

- a causa dell'assenza di una sorgente di energia interna, non possono integrare sensori;
- possono rimanere attivi per lunghi periodi di tempo, nonostante non facciano più parte della filiera produttiva.

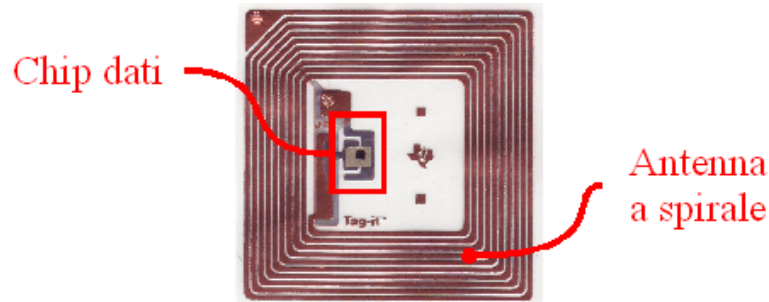


Figura 3: esempio di tag passivo: in figura sono evidenziati il chip contenente i dati (es. codice EPC) e l'antenna per la trasmissione degli stessi al dispositivo lettore (Fonte immagine: <http://www.sagedata.com>).

### 1.2.3 Tag semi-attivi (o semi-passivi)

Questa terza tipologia di tag è dotata di una batteria utilizzata solo per alimentare il microchip e gli apparati ausiliari (sensori), ma non per alimentare il trasmettitore, difatti in trasmissione si comportano come tag passivi ereditandone quindi una limitata distanza operativa (minore di 30 m) [4].



## 2 Architettura dei sistemi RFID (EPCglobal Network)

Il sistema informativo associato ai dispositivi RFID è standardizzato come EPCglobal Network che si basa sulla possibilità di identificare in modo semplice ed efficace le merci movimentate nella supply chain a livello di pallet, fino alla singola unità di vendita al consumatore finale. Questa visione è abilitata dall'associazione della tecnologia RFID con le infrastrutture esistenti per le comunicazioni di rete e l'*Electronic Product Code*. Tale implementazione è tecnologicamente indipendente, difatti la struttura dell'EPCglobal Network è tale per cui la sua implementazione non dipende né da una particolare offerta tecnologica, né da una specifica azienda fornitrice di tecnologia e prevede la possibilità di utilizzare qualsiasi mezzo permetta di acquisire i codici EPC che sono alla base del suo funzionamento [6].

### 2.1 Componenti del sistema EPCglobal Network

Tale architettura è costituita da cinque componenti [6]:

- *Electronic Product Code (EPC)*: è lo schema di numerazione universale per l'identificazione di tutti gli oggetti fisici movimentati nella supply chain tramite tecnologia RFID (per maggiori approfondimenti consultare la sezione 3.2 a pagina 14);
- *ID System*: è il sistema di identificazione, basato sia sui tag RFID applicati ai beni e sui quali è memorizzato il codice EPC, che sui relativi lettori;
- *EPC Middleware (o middleware RFID)*: è il layer di integrazione tra i device RFID ed i sistemi informativi esistenti. Il suo compito principale è ricevere i dati RFID dalle fonti alimentanti (es. i dispositivi RFID) ed integrare gli stessi nelle applicazioni aziendali. Il middleware gioca un ruolo fondamentale nelle soluzioni RFID in quanto permette di:
  - ricevere le segnalazioni dai lettori RFID distribuiti nella azienda;
  - controllare le informazioni ricevute;
  - memorizzare le informazioni sul database aziendale;
  - elaborare le informazioni ricevute, arricchendone i contenuti con logiche applicative locali oppure aggiornando i sistemi applicativi aziendali.

- *Object Naming Service (ONS)*: è un componente dei Discovery Services, guida i sistemi informatici nel processo di localizzazione delle informazioni in rete (Internet), relative a ciascun oggetto identificato da un codice EPC. Il suo ruolo è simile a quello del DNS (Domain Name System), il quale indirizza i computer in rete al fine di localizzare le pagine associate ad un determinato sito web. Analogamente, l'ONS partendo dal codice EPC restituisce un indirizzo web (od una URL) dove risiedono tutte le informazioni relative ad un determinato bene. Tutto questo permette di immagazzinare un'enorme quantità di dati in rete, più di quanto sarebbe possibile fare sui tag apposti sui singoli oggetti.
- *EPC Information Service (EPCIS)*: Si tratta di risorse informative che registrano le informazioni relative ai singoli oggetti e consentono lo scambio di queste informazioni tra i partner commerciali attraverso il sistema EPCglobal Network. Gli *EPCIS data*, ovvero le informazioni registrate in un EPCIS e suddivise nelle seguenti categorie:
  - *Static Data*: informazioni che non cambiano nel corso della vita delle referenze: nome del prodotto, dimensioni, data di scadenza, numero di lotto, ecc.;
  - *Transactional Data*: informazioni che cambiano nel corso delle vita della referenza identificata, quali: luogo di consegna, ecc.

## 2.2 Funzionamento del sistema EPCglobal Network

Il sistema consente l'identificazione in rete tramite il servizio ONS che è un registro globale e sulla base del codice EPC ricevuto (letto sul tag dal lettore), fornisce al Middleware l'indirizzo dell'EPCIS, ovvero del server locale/remoto sul quale risiedono le informazioni relative al prodotto. L'EPC e tutti i dati riguardanti il prodotto sono registrati presso i server locali (EPCIS) collegati al Web.

Ogni volta che le aziende vorranno consultare i dati aggiornati potranno collegarsi ai database e, se gli operatori sono abilitati, gestire direttamente ogni tipo di cambiamento delle informazioni. Infine il linguaggio di markup (*Physical Markup Language* per la comunicazione tramite web, che sfrutta il *linguaggio XML* [11]) è utilizzato per descrivere tutti i dati relativi ai prodotti quali ad esempio: numeri EPC, orario certificato, identificativo del lettore, la temperatura, nonché la posizione del lettore che ha inviato la query; infine Il PML

## 2 ARCHITETTURA DEI SISTEMI RFID (EPCGLOBAL NETWORK)

funge da interfaccia tra i lettori e le applicazioni che intendono accedere ai dati EPC tramite la rete.

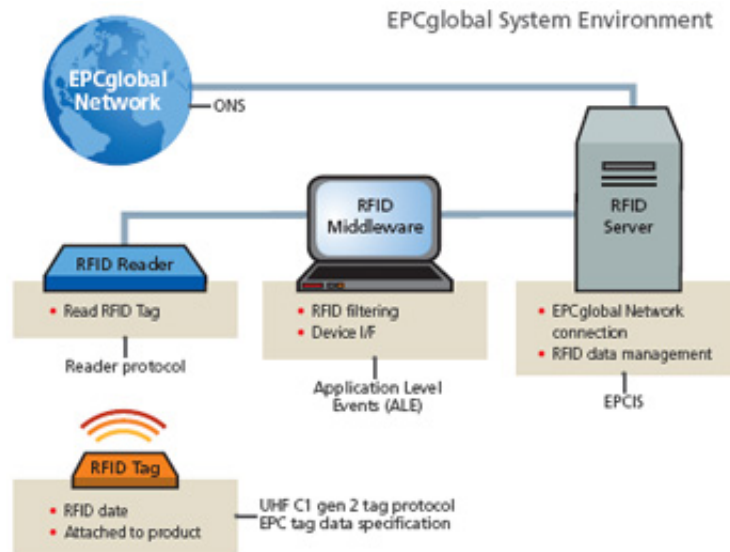


Figura 4: schematizzazione dell'EPCglobal Network e del relativo funzionamento (Fonte immagine: [http://www.nec.co.th/asp/sol\\_RFId.asp](http://www.nec.co.th/asp/sol_RFId.asp)).

## 3 Standard inerenti l'RFID

### 3.1 Gli standard ISO

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

Nella tecnologia RFID si sono sviluppati nel corso degli anni diversi standard ISO formalizzando tutti gli aspetti relativi ad essa quali la tipologia del segnale, i campi di applicazione, i metodi di test delle performance, etc. I principali documenti riconducibili all'RFID sono [12] [8]:

- *ISO 11784, ISO 11785 ed ISO 14223*: formalizzano la struttura dei codici RFID per il riconoscimento degli animali, definendo la procedura di attivazione dei transponder, ed il processo di comunicazione dei dati in esso contenuti utilizzando apparecchi ricetrasmittenti [16];
- *ISO/IEC 14443*: [17] è costituito da quattro parti e descrive due tipologie di carte elettroniche (*proximity card*): *Type A* e *Type B*, entrambe operanti ad una frequenza radio di 13.56 MHz. Sebbene entrambe le tipologie di carte elettroniche utilizzino il medesimo protocollo di trasmissione dei dati, presentano delle differenze che risiedono nella modulazione del segnale, negli schemi di codifica e nel protocollo di inizializzazione;
- *ISO/IEC 15961 ed ISO/IEC 15962*: definiscono l'interfaccia interposta tra le applicazioni ed il protocollo dati, includendo la sintassi e la codifica della stessa per il trasferimento dei dati, dei comandi e la struttura dei messaggi di risposta (lato applicativo). Opera indipendentemente alla tipologia di comunicazione definita nello standard *ISO/IEC 18000*;
- *ISO/IEC 15693*: [18] è lo standard ISO per le schede elettroniche operanti ad una frequenza di 13.56 MHz e ad una distanza massima di lettura di 1-1.5 m (*vicinity card*). Tale standard è suddiviso in tre parti e definisce le caratteristiche fisiche dei dispositivi, la frequenza operativa ed i protocolli di inizializzazione, anticollisione e trasmissione;
- *ISO/IEC 18000*: definisce una serie di interfacce RFID per la gestione dei beni. Suddiviso in sette parti, è lo standard principe della tecnologia RFID, poiché formalizza pressoché qualsiasi aspetto di essa:

- *parte 1*: definisce l'architettura generica per tutte le interfacce di comunicazione definite nella serie di standard ISO 18000;
- *parte 2*: definisce i parametri per attivare la comunicazione con interfacce operanti ad una frequenza inferiore ai 135 kHz. Inoltre definisce due tipologie di tag RFID:
  - \* *Type A (FDX)*<sup>1</sup>: alimentate permanentemente dal dispositivo interrogante (anche nella fase di comunicazione tag→lettore) ed operanti ad una frequenza di 125 kHz;
  - \* *Type B (HDX)*<sup>1</sup>: alimentate permanentemente dal dispositivo interrogante (eccetto nella fase di comunicazione tag→lettore) ed operanti ad una frequenza di 125 kHz o 134.2 kHz.
- *parte 3*: definisce i parametri per attivare la comunicazione con interfacce operanti ad una frequenza di 13.56 MHz;
- *parte 4*: definisce i parametri per attivare la comunicazione con interfacce operanti ad una frequenza di 2.45 GHz. Lo standard definisce due tipologie di tag:
  - \* *tag passivi*: non possono avviare per primi la comunicazione lettore→tag;
  - \* *tag dotati di batteria (attivi)*: possono avviare per primi la comunicazione tag→lettore.
- *parte 5*: [2] definisce i parametri per attivare la comunicazione con interfacce operanti ad una frequenza di 5.8 GHz (caduto in disuso per insufficiente impiego applicativo);
- *parte 6*: definisce i parametri per attivare la comunicazione con interfacce operanti ad una frequenza variabile tra i 860 MHz ed i 960 MHz. Definisce anche in questo caso tre tipologie di tag:
  - \* *Type A* e *Type B*: la cui differenza principale risiede nell'algoritmo anticollisione impiegato;
  - \* *Type C*: conosciuto come *EPCglobal Class 1 Gen 2* (sezione 3.2 nella pagina successiva).

---

<sup>1</sup>Con le abbreviazioni HDX ed FDX si identifica come i tag di tipo passivo comunicano con il lettore. Nella modalità HDX (*Half Duplex*) il segnale di attivazione è attivo per metà del tempo totale di impiego del dispositivo, mentre nella modalità FDX (*Full Duplex*) il segnale di attivazione è attivo per tutta la durata di impiego del dispositivo (Fonte: <http://www.digitalangel.com>).

- *parte 7*: definisce i parametri per attivare la comunicazione con interfacce operanti ad una frequenza di 433 MHz.
- *ISO/IEC 18046 ed ISO/IEC 18047*: definiscono i metodi per testare le performance dei dispositivi RFId (siano essi lettori o tag);
- *ISO/IEC 19762 ed ISO/IEC 24730*: definiscono le tecniche per realizzare sistemi *Automatic Identification and Data Capture (AIDC)* e *Real-Time Locating System (RTLS)* tramite l'utilizzo della tecnologia RFId<sup>2</sup>.

## 3.2 Electronic Product Code (EPC)

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. Questo standard è ritenuto dai maggiori esperti come il futuro sostituto del codice a barre il quale consente principalmente di memorizzare il nome del produttore ed il tipo di prodotto; l'EPC invece non solo contiene questi dati, ma ne memorizza altri come il numero seriale ed il lotto di appartenenza, inoltre se il sistema di identificazione viene collegato ad un database è possibile mantenere memoria di informazioni specifiche su quel determinato oggetto come la data di produzione e di scadenza, il colore od il sapore di un certo prodotto, ma anche la disposizione sugli scaffali, o la tracciatura della spedizione [5].

### 3.2.1 Struttura dell'EPC

Sebbene l'EPC esista in due differenti versioni (*short* a 64 bit e *standard* a 96 bit) e codifichi tredici diversi codici, essi rispettano tutti uno schema prefissato (tabella 2).

- *Header*: identifica la lunghezza globale, il tipo, la struttura, la versione e la generazione dell'EPC;
- *EPC Manager Number*: è un codice univoco rilasciato da EAN.UCC che descrive l'entità (l'azienda) responsabile della gestione univoca dei campi seguenti;

---

<sup>2</sup>Con i termini AIDC ed RTLS si fa riferimento a tutti quei metodi di identificazione automatica, raccolta dati e memorizzazione degli stessi nei calcolatori, che identificano gli oggetti. L'adozione della tecnologia RFID in questo settore ha permesso di ampliare i campi di applicazione relativi all'identificazione, includendo ad esempio il settore della zootecnia e del commercio automobilistico, sistemi che richiedono la tracciabilità in movimento delle entità coinvolte nei processi.

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

Tabella 2: struttura dell'EPC (GID-96).

- *Object Class*: codice univoco per un oggetto o la sua unità di vendita, detta anche *SKU (Stock Keeping Unit)*;
- *Serial Number*: identifica l'istanza (l'oggetto) in modo univoco.

L'ultima versione dell'*EPCglobal Tag Data Standards* (la versione 1.4) formalizza le seguenti 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)*: è composto da tre campi, il *General Manager Number*, l'*Object Class* ed il *Serial Number*. La codifica di tale standard include un quarto campo l'*Header* che garantisce l'unicità nel namespace EPC (tabella 2).
- *versioni serializzate del GS1*: sfruttando le conoscenze e la struttura dei codici a barre formalizzati nel GS1 (*Global Services*), l'EPC codifica i seguenti identificatori:
  - *Global Trade Item Number (SGTIN-96 SGTIN-198)*: il GTIN contribuisce all'automatizzazione del processo commerciale (principalmente nelle fasi di acquisto e vendita di un bene). Questa tipologia di codice viene assegnata agli oggetti (prodotti o servizi) che necessitano di essere prezzati, ordinati o richiamati all'interno di una *supply chain*<sup>3</sup>, ritornando determinate informazioni predefinite inerenti l'oggetto;
  - *GS1 Serial Shipping Container Code (SSCC-96)*: questa codifica viene impiegata per tracciare il trasporto e l'immagazzinamento dei beni da gestire attraverso la supply chain;

<sup>3</sup>*Supply chain*: trad. *catena di distribuzione* dei beni di consumo (Fonte: <http://it.wikipedia.org>).

- *GS1 Global Location Number (SGLN-96 e SGLN-195)*: può essere utilizzato per identificare un luogo fisico od entità legali coinvolte nel processo di comunicazione con la supply chain;
  - *GS1 Global Returnable Asset Identifier (GRAI-96 e GRAI-170)*: è una chiave che consente la tracciabilità di imballaggi riutilizzabili o macchinari di trasporto all'interno dell'asset<sup>4</sup> aziendale;
  - *GS1 Global Individual Asset Identifier (GIAI-96 e GIAI-202)*: viene impiegata per tracciare il ciclo di vita di beni coinvolti nell'asset aziendale;
  - *Global Service Relation Number (GSRN-96)*: viene utilizzato per identificare il destinatario di un servizio in un contesto di collaborazioni aziendali. Permette inoltre di accedere ai database per registrare i servizi di uso ricorrente;
  - *Global Document Type Identifier (GDTI-96)*: identifica le tipologie di documento accessibili nei database aziendali, regolandone quindi l'accesso.
- *DOD Construct (DoD-96)*: identificatori atti a tracciare i beni destinati e provenienti dal Dipartimento della Difesa U.S.A.

### 3.2.2 Classificazione dei tag secondo lo standard EPC

L'*Auto-ID Center* creato nel 1999 si pose come obiettivo quello di creare un EPC, originariamente il centro pianificò di creare un proprio protocollo di comunicazione UHF tale da consentire la comunicazione di classi differenti di tag:

- *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; è essenzialmente un tag Class 2 dotato di una batteria tale da incrementare il raggio operativo di trasmissione/ricezione dei segnali;

---

<sup>4</sup>*Asset*: insieme dei valori materiali e immateriali facenti capo ad una proprietà, in tal caso ad un'azienda (Fonte: <http://it.wikipedia.org>).



- *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.

Nel 2003 con la scissione del centro in due entità distinte e la nascita dell'EPC-global, le Class 0 ed 1 divennero standard EPC; successivamente nel 2004 l'EPC-global cominciò a sviluppare un protocollo di seconda generazione (*Gen 2*), non retro compatibile con le due classi, perseguendo l'obiettivo di creare uno standard globalmente riconosciuto.

Nel Dicembre 2004 Gen 2 è stato approvato come standard ISO (sezione 3.1 a pagina 12) e molti costruttori di dispositivi e tag hanno adottato adottano tale standard, unitamente agli standard ISO [10].

## 4 Normative inerenti l'RFID

In Italia l'utilizzo della tecnologia RFID é stata oggetto di provvedimenti da parte del Garante della Privacy, con il Provvedimento a carattere generale del Garante per la protezione dei dati personali 9 Marzo 2005 [1], ne regola l'utilizzo tale per cui non si vengano a creare situazioni di minaccia alla privacy dei cittadini.

### 4.1 Richiami dal D.Lgs 196/2003 (Codice in materia di protezione dei dati personali)

Partendo con il presupposto che l'utilizzo della tecnologia RFID deve rispettare tutti gli articoli del Codice, gli utilizzatori devono porre particolare attenzione sui seguenti articoli:

- *principio di necessità (art. 3 del Codice)*: l'applicazione RFID deve elaborare solo i dati strettamente necessari in relazione alla finalità che persegue;
- *liceità (art. 11, comma 1, lett. a), del Codice)*: l'utilizzo della tecnologia deve svolgersi nel rispetto delle altre leggi e regolamenti che sussistono nel rispettivo settore di impiego: es. in ambito lavorativo, l'uso di tecniche RFID deve in particolare rispettare il divieto di controllo a distanza del lavoratore (art. 4 l. 20 maggio 1970, n. 300; art. 114 del Codice);
- *finalità e qualità dei dati (art. 11, comma 1, lett. b), c), d) e e), del Codice)*: i dati possono essere inoltre utilizzati soltanto in termini compatibili con la finalità per la quale sono stati originariamente raccolti; devono essere conservati per il tempo strettamente necessario a perseguire tale finalità, decorso il quale devono essere cancellati o resi anonimi, il titolare deve altresì curare la pertinenza e non eccedenza, l'esattezza e l'aggiornamento dei dati personali;
- *proporzionalità (art. 11, comma 1, lett. d), del Codice)*: i dati trattati e le modalità del loro trattamento, anche con riferimento alla tipologia delle infrastrutture di rete adoperate, non devono risultare sproporzionati rispetto agli scopi da prefissare: es. non si possono tracciare i tag dei prodotti, dopo la loro vendita, a meno che ciò sia necessario per fornire un servizio specificamente e liberamente richiesto dall'interessato stesso;

- *informativa (art. 13 del Codice)*: il titolare dei servizi deve avvisare gli interessati in modo tale che essi sappiano che i beni od i servizi di cui beneficiano, sono soggetti all'utilizzo di tecnologie tramite cui è possibile raccogliere dati personali;
- *trattamento da parte di privati*: in generale, l'utilizzo di RFID che implichi un trattamento di dati personali da parte di privati può essere effettuato solo con il *consenso dell'interessato*, sottoscritto secondo determinate modalità. Anche in presenza del consenso dell'interessato o di un altro presupposto del trattamento, il trattamento dei dati personali mediante RFID deve comunque svolgersi nel rispetto dei menzionati *principi di finalità, proporzionalità e dignità*;
- *esercizio dei diritti (artt. 7-10 del Codice)*: Il titolare del trattamento deve agevolare l'esercizio, da parte dell'interessato, dei diritti di cui all'art. 7 del Codice, semplificando le modalità e riducendo i tempi per il riscontro al richiedente (art. 10, comma 1 del Codice). Già nella fase di progettazione delle tecnologie, i produttori di sistemi RFID dovrebbero opportunamente predisporre modalità idonee a garantire agli interessati un agevole esercizio dei diritti;
- *disattivazione o rimozione delle etichette*: all'interessato deve essere riconosciuta la possibilità di ottenere, gratuitamente e in maniera agevole, la rimozione o la disattivazione delle etichette RFID al momento dell'acquisto del prodotto su cui è apposta l'etichetta o al termine dell'utilizzo del dispositivo. Le etichette devono essere posizionate in modo tale da risultare, per quanto possibile, facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto o dell'oggetto a cui si riferiscono (ad esempio, disponendone la collocazione sulla sola confezione);
- *impianto sottocutaneo di microchip*: gli impianti sottocutanei di microchip devono ritenersi in via di principio esclusi, in quanto contrastanti, con riferimento alla protezione dei dati, con il principio di dignità (art. 2 del Codice), ferme restando le altre norme dell'ordinamento a garanzia dell'integrità fisica e dell'inviolabilità della dignità della persona, contenute anche nella Carta dei diritti fondamentali dell'Unione europea (artt. 1 e 3).

L'impiego di microchip sottocutaneo può essere quindi ammesso solo in casi eccezionali, per comprovate e giustificate esigenze a tutela della salute

delle persone, in stretta aderenza al principio di proporzionalità (art. 11 del Codice), e nel rigoroso rispetto della dignità dell'interessato (art. 2, comma 1). L'interessato dovrebbe poter essere in grado di ottenere di regola, in qualunque momento e senza oneri, la rimozione del microchip e l'interruzione del relativo trattamento dei dati che lo riguardano.

I titolari del trattamento devono inoltre predisporre modalità di impianto e di impiego delle etichette sottocutanee tali da garantire la riservatezza circa la presenza delle stesse etichette nel corpo dell'interessato.

- *ulteriori prescrizioni:* in aggiunta alla prescrizioni fin qui illustrate, è necessario che il titolare del trattamento notifichi al Garante:
  - l'attività di raccolta ed elaborazione dei dati personali nel caso in cui:
    - \* i dati indichino la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. a))
    - \* le operazioni vengano effettuate con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzarne abitudini e scelte in ordine ai prodotti acquistati (artt. 37, comma 1, lett. d));
  - le misure di sicurezza (artt. 31-36 e Allegato B) del Codice), affinché siano ridotti al minimo i rischi di distruzione o perdita anche accidentale dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
  - la selezione dei soggetti che, in qualità di incaricati o responsabili del trattamento, sono autorizzati a compiere operazioni di trattamento sulla base dei compiti assegnati e delle istruzioni impartite (artt. 29 e 30 del Codice).

## 5 Minacce alla sicurezza ed alla privacy

La tecnologia RFId è di tipo *wireless* questo fattore incide pesantemente sulla sicurezza nei processi di comunicazione, inoltre data la scalabilità del sistema (sezione 2 a pagina 9), i costi relativamente contenuti dei tag, nonché il grado di pervasività/integrazione degli stessi nella vita quotidiana, essa sta sempre di più aumentando il suo grado di impiego nei vari campi applicativi, tra cui ricordiamo i sistemi di accesso ed i sistemi volti alle operazioni di tipo economico. Di seguito vengono riportate le principali tipologie di attacco a cui i sistemi RFId sono soggetti, e le possibili contromisure e reazioni atte a salvaguardare la sicurezza e la confidenzialità del sistema e dei dati elaborati [7].

- *attacco fisico*: consiste nell'attaccare fisicamente un tag RFId in modo tale da acquisire o modificare i dati in esso contenuti: l'attacco sul tag può avvenire modificandone l'energia di alimentazione, modificandone il circuito, accedendo ai dati tramite l'utilizzo di un laser, etc.

Contromisure: realizzare tag anti manomissione o rivestire gli stessi con particolari schermature (banalmente un foglio di alluminio per alimenti).

- *skimming* (trad. *strisciare*): questa tipologia di attacco prevede che un attaccante detto *skimmer* utilizzi un dispositivo hardware in modo tale da acquisire i dati personali contenuti nei tag RFId presenti nei documenti delle vittime (es. carta di credito, passaporto, tessera sanitaria, ect...). Il dispositivo hardware consiste in un lettore, tipicamente un PDA, dotato di un'apposita antenna il cui raggio di ricezione può variare da pochi metri a qualche chilometro.

Contromisure: richiedere l'autenticazione da parte del lettore prima che il tag possa inviare i propri dati, adottare schermature, blocker tag o RFId Guardian.

- *blocker tag* (*RSA bloker tag* o *RSA tag*): è un tag RFId atto a proteggere la privacy dei dati contenuti negli RFId di un sistema, e che in caso di richieste non autorizzate risponde in modo positivo alle stesse, impedendo agli scanner di leggere i tag RFId ad esso circostanti [15];
- *RFId Guardian*: è un dispositivo portatile a batteria che regola e monitorizza l'utilizzo della tecnologia RFId, integrando le funzionalità di auditing, key management, controllo degli accessi ed autenticazione [13];

- *autenticazione simmetrica*: il processo consiste nello scambio di token criptati  $T_n$  tra il lettore ed il tag, esso funziona poiché il/i tag sanno che solo lettori autorizzati possono generare un  $T_1$  valido, viceversa il lettore sa che solo tag autorizzati possono generare un  $T_2$  valido.
  - *Hash lock*: in questo meccanismo di sicurezza i tag sono normalmente in modalità “chiusa”, ossia non comunicano dati al lettore richiedente, ma solo un *metaID*, una rappresentazione hash del loro ID. Il lettore autorizzato consultando il database di riferimento può rintracciare l’ID del tag attraverso il *metaID*, ed inviarlo al tag stesso: se l’associazione è corretta il tag entra in modalità “aperta”, consentendo la lettura dei propri dati. Per ovviare a possibili tracciature o eavesdropping dei *metaID* si sono sviluppati inoltre il *Randomized Hash-Lock* ed il *Double Randomized Hash-Lock*, che consistono nel hashare i *metaID* utilizzando numeri casuali, rendendo il processo di comunicazione più complesso.
- *spoofing* (trad. *imbrogliare*): l’attaccante può creare tag “autentici” scrivendovi dati “corretti” utilizzando tag RFID vergini o riscrivibili, in modo tale da accedere ad un sistema utilizzando i dati di una vittima, che ne detiene i diritti d’accesso.  
Contromisure: tali attacchi vengono cauterizzati restringendo l’accesso ai dati, richiedendo nel processo di autenticazione l’utilizzo di una chiave segreta conservata all’interno di un’area di memoria protetta che non deve mai essere né letta né trasmessa da parte del tag, facente quindi parte dei dati ad accesso ristretto.
  - *Denial of Service (DoS)* (trad. *interruzione del servizio*): questo tipo di attacco mira a modificare il normale funzionamento del sistema RFID. Poiché tale tecnologia è wireless il DoS può essere facilmente realizzato effettuando il *jamming* della frequenza operativa. L’attacco può essere perpetrato anche rispondendo ad ogni richiesta effettuata durante il processo di comunicazione, simulando il comportamento di un *blocker tag*. Una terza modalità di attacco DoS consiste nel disattivare o distruggere i tag coinvolti nel processo di comunicazione.  
Contromisure: gli attacchi DoS, sebbene non esistano meccanismi validi tramite cui proteggersi, possono essere facilmente rilevati e bloccati prima che possano causare gravi danni. Meccanismi quali il monitoraggio

della frequenza operativa del sistema RFId ed istituzione di routine di controllo possono essere valide contromisure al problema.

- *eavesdropping* (trad. *origliare*): consiste nell'ascoltare in modo passivo e non autorizzato la comunicazione RFId.

Contromisure: il metodo più semplice per ovviare a questo tipo di attacco consiste nel crittografare le comunicazioni, prima di inviare i dati via wireless: in questo modo l'attaccante può sì ascoltare la comunicazione, ma (in teoria) non può "comprendere" i dati trasmessi.

- *tracking* (trad. *monitoraggio*): la tecnologia RFId si basa sulla scelta implementativa che ogni tag è dotato di un ID: l'attaccante riuscendo ad identificare l'ID di un particolare tag, può tenerne traccia degli spostamenti nel tempo e nello spazio.

Contromisure: è possibile adottare l'impiego di schermature del tag, dell'RFId Guardian od utilizzare pseudonimi (aggiornati ogni quanto di tempo) da associare al tag, in modo tale che l'attaccante debba effettuare più scansioni di tali identificatori per poter rintracciare l'oggetto voluto.

- *relay attacks* (trad. *attacchi a staffetta*): le moderne carte di credito ed i sistemi d'accesso sono dotati di tag RFId, il cui processo di autenticazione è spesso basato su un protocollo challenge-response che necessita di una chiave segreta condivisa il cui accesso è consentito solamente se l'utente richiedente è in possesso di un determinato "segreto" relativo al tag RFId. Il normale funzionamento in questo tipo di comunicazione presuppone che sia il tag che il lettore siano "genuini". Il relay attack stravolge questo presupposto: puntando al sistema di controllo, l'attaccante utilizza le credenziali di una vittima per guadagnarsi l'accesso ad un sistema protetto o riservato. Il tag della vittima ed il lettore vengono ingannati, poiché l'attaccante interponendosi nella comunicazione (*man-in-the-middle*) acquisisce i dati voluti.

Contromisure: anche in questo caso è possibile utilizzare meccanismi di schermatura o l'RFId Guardian. I relay attacks generano ritardi nei processi di comunicazione, fattore che può introdurre da parte della vittima, l'adozione di protocolli che introducano vincoli sulla temporizzazione dell'intero processo. È infine possibile introdurre l'*autenticazione a due fattori* (*Two-Factor Authentication*) aggiungendo al processo di comunicazione la condivisione da parte dei due attori, di un segreto (ad esempio

un PIN); l'attaccante che si interpone nella comunicazione deve acquisire questo "segreto" per poter accedere al sistema obiettivo.

- *virus RFId*: sebbene le risorse dei tag RFId siano limitate, si é riuscito utilizzando solamente 127 caratteri, ad inserirvi malicious code (worm e virus), effettuare attacchi SQL injection, buffer overflow ed inserimenti di codice, in grado di aggredire il back-end ed il sistema RFId stesso.  
Contromisure: é possibile preventivare questi attacchi disabilitando lo scripting lato back-end, limitando l'accesso ai database, ed introducendo vincoli sul tipo di parametri e dati elaborati nel processo di comunicazione.



## 6 VeriChip

Concludiamo questo elaborato presentando un caso applicativo che negli ultimi anni ha suscitato particolare scalpore: *VeriChip* è un dispositivo applicato sotto pelle, ed utilizza l'identificazione a radiofrequenza (RFID) il cui segnale operativo si aggira intorno ai 125 kHz, che può essere usato in vari campi (sicurezza, finanza, identificazione di emergenza, etc.).

Delle dimensioni di un chicco di riso (figura 5), ogni dispositivo VeriChip consiste in un tag passivo racchiuso in una capsula di vetro, parzialmente ricoperta da una sostanza porosa a base di polipropilene (*Biobond*), la quale impedisce che il dispositivo “viaggi” per il corpo in cui è stato impiantato. Il numero di identificazione contenuto nel tag è univoco ed a 16 cifre simile al *Social Security Number* in vigore negli U.S.A. o ad un *codice a barre* che viene memorizzato nei relativi database [3].

L'ubicazione standard del microchip è nell'area del tricipite tra il gomito e la spalla del braccio destro, la breve procedura di *chipping* del paziente dura solo alcuni minuti e utilizza solamente un'anestesia locale seguita da un'iniezione rapida e indolore del VeriChip. Una volta inserito sotto pelle, il VeriChip non è visibile ad occhio nudo.

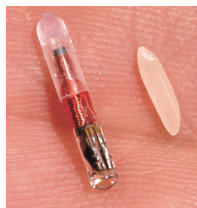


Figura 5: tag VeriChip.

L'obiettivo di tale dispositivo è quello di consentire l'accesso da parte del personale medico, ai dati relativi ai pazienti in cura.

**Privacy:** i sostenitori della privacy hanno contestato il VeriChip, avvisando il potenziale abuso che ne può essere fatto definendo questo tipo di chip RFID come *spychip* contestando l'uso di questi dispositivi da parte dello stato perché possono portare a una limitazione delle libertà civili. Essendo leggibile da chiunque possieda un lettore di chip RFID l'utilizzo di questo dispositivo faciliterebbe il furto di informazioni personali.

**Sicurezza:** i dati contenuti nel dispositivo non sono criptati e VeriChip non ha la funzionalità di autorizzazione selettiva del lettore. Essendo un chip RFID passivo chiunque abbastanza vicino può leggerlo. Questo difetto può essere parzialmente risolto inserendo il dispositivo ad esempio nel cinturino dell'orologio che può essere rimosso a piacere.

Il database a cui è associato il dispositivo ad ora contiene solo informazioni mediche, e in nessun caso sono disponibili informazioni finanziarie, o di previdenza sociale, l'accesso al database inoltre è garantito solo a strutture mediche autorizzate e ogni accesso viene registrato e le informazioni contenute sono redatte direttamente dall'utilizzatore.

Nel 2006 è stato clonato l'identificatore contenuto in un VeriChip e sul web sono pubblicate le istruzioni per la clonazione (Fonte: <http://cq.cx/vchdiy.p1>).

**VeriChip in Italia:** pur essendo stato oggetto ad un'ampia campagna di informazione più o meno a favore del suo utilizzo, nel nostro paese il VeriChip è regolamentato dal Garante della Privacy ( 4.1 a pagina 18) che ne regola l'utilizzo ai soli *"...casi eccezionali, per comprovate e giustificate esigenze a tutela della salute delle persone..."*.

Il progetto è stato recentemente (nel 2008) abbandonato a causa di mancanza di volontari nell'ambito del progetto *Health Link*, soprattutto dopo le polemiche che già in passato avevano investito tale società, e che non ha portato il successo sperato [9].

## **Riferimenti bibliografici**

- [1] Provvedimenti a carattere generale del 9 Marzo 2005. Etichette intelligenti (Rfid): il Garante individua le garanzie per il loro uso.
- [2] High Tech Aid. ISO/IEC SC31 RFID Related Standards. 2008.
- [3] K. Albrecht. Microchip implants: Answers to Frequently Asked Questions. 2010.
- [4] Fondazione Ugo Bordoni. Tecnologia RFId (presentazione). 2008.
- [5] EPC. FAQ on EPC and RFID. 2010.
- [6] EPCLab. L'Architettura Tecnologica RFId di EPCglobal. 2008.
- [7] T. Haver. Security and Privacy in RFID Applications. 2006.
- [8] ISO. International Organization for Standardization. 2010.
- [9] newsrfid.com. 23 Maggio 2008 - L'RFID sottocutaneo non decolla: VeriChip perde la sua sfida ed è costretta a vendere. 2008.
- [10] RFIDjournal.com. A Summary of RFID Standards. 2010.
- [11] RFIDjournal.com. Glossary of RFID terms. 2010.
- [12] RFID.net. ISO RFID Standards: A Complete List. 2010.
- [13] M. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, and A.S. Tanenbaum. A Platform for RFID Security and Privacy Administration. 2006.
- [14] Technovelgy.com. RFID tag. 2010.
- [15] Wikipedia. RSA blocker tag — Wikipedia, The Free Encyclopedia, 2009. [Online; accessed 14-July-2010].
- [16] Wikipedia. ISO 11784 & 11785 — Wikipedia, The Free Encyclopedia, 2010. [Online; accessed 15-July-2010].
- [17] Wikipedia. ISO/IEC 14443 — Wikipedia, The Free Encyclopedia, 2010. [Online; accessed 15-July-2010].
- [18] Wikipedia. ISO/IEC 15693 — Wikipedia, The Free Encyclopedia, 2010. [Online; accessed 15-July-2010].

- [19] Wikipedia. Radio Frequency IDentification — Wikipedia, L'enciclopedia libera, 2010. [Online; in data 1-luglio-2010].