

# La Controversia sul Trusted Computing

*Alessandro Bottoni – Milano – 12 Maggio 2006*

## Slide 1: Introduzione

Questa presentazione illustra brevemente i termini della controversia attualmente in corso riguardo la tecnologia comunemente nota come “Trusted Computing” o “Trustworthy Computing”. Questa presentazione fornisce solamente una visione d'insieme della situazione corrente. Una analisi più dettagliata della controversia in corso (e della documentazione esistente sul TC) è disponibile nell' **e-book** gratuito dello stesso autore (Alessandro Bottoni), reperibile a questo indirizzo:

[http://alessandrobottoni.interfree.it/download/Trusted\\_Computing\\_Rel\\_0-9\\_Beta.pdf](http://alessandrobottoni.interfree.it/download/Trusted_Computing_Rel_0-9_Beta.pdf)

In questo testo potete trovare una discussione dettagliata di molte affermazioni contenute in questa presentazione che possono sembrare, a prima vista, immotivate od esagerate. Vi rimandiamo quindi alla lettura di questo testo per la dimostrazione delle varie tesi presentate in questo documento.

Molti argomenti sono stati esaminati in modo individuale negli articoli dell'autore per la rubrica Untrusted di Punto Informatico (<http://punto-informatico.it>) e per la Spina Nel Fianco (<http://www.laspinanelfianco.it>). Vi rimandiamo a questi articoli per una trattazione dettagliata dei principali aspetti del Trusted Computing.

## Slide 2: I documenti di riferimento (letture consigliate)

Vi raccomandiamo caldamente di leggere almeno una buona parte dei documenti elencati qui di seguito per formarvi una vostra opinione personale sul fenomeno “Trusted Computing”. In questi documenti trovate le fonti di informazione che sono servite per la stesura dell' e-book e per la preparazione di questa presentazione.

“**The need for TCPA**” di David Safford e “**Claryfing misinformation on TCPA**” di David Safford, reperibili presso IBM: <http://www.research.ibm.com/gsal/tcpa/> .

La **documentazione ufficiale del TCG**, reperibile sul loro sito web: <https://www.trustedcomputinggroup.org/home> .

“**LaGrande Technology Overview**” ed altri documenti tecnici reperibili a <http://www.intel.com/technology/security/> .

**Vari documenti tecnici di MS su NGSCB**, reperibili su TechNet (<http://technet.microsoft.com/en-us/default.aspx>)

“**The Controversy over Trusted Computing**” di Catherine Flick (tesi di laurea), reperibile a questa URL:

[http://luddite.cst.usyd.edu.au/~liedra/misc/Controversy\\_Over\\_Trusted\\_Computing.pdf](http://luddite.cst.usyd.edu.au/~liedra/misc/Controversy_Over_Trusted_Computing.pdf) .

La raccolta di documenti reperibile a **L0t3k** : <http://www.l0t3k.org/security/docs/tcpa/> .

**Wikipedia**: [http://en.wikipedia.org/wiki/Trustworthy\\_Computing](http://en.wikipedia.org/wiki/Trustworthy_Computing) .

La raccolta di documenti in italiano presenti a <http://www.no1984.org> .

Gli articoli di Alessandro Bottoni per la rubrica “**Untrusted**” di **Punto Informatico**: <http://punto-informatico.it/cerca.asp?s=bottoni+untrusted&B=CERCA&r=PI> .

Il **forum italiano sul P2P**: <http://www.p2pforum.it/forum/showthread.php?t=88160> .

Gli articoli di Alessandro Bottoni per **La Spina nel Fianco**: <http://www.laspinanelfianco.it> .

## Slide 3: La Versione ufficiale

Più esattamente, si dovrebbe parlare di “versioni ufficiali”, al plurale, visto che il Trusted Computing Group, Intel, AMD, Apple, Microsoft ed altri produttori forniscono visioni diverse della stessa tecnologia. Comunque, la versione ufficiale dell'ente ufficiale di standardizzazione, il Trusted Computing Group, presenta la tecnologia Trusted Computing nel modo seguente.

### Scopi

1. Fornire all'utente del PC le funzionalità crittografiche tipiche di una Smart Card direttamente sul PC, “di serie”, senza bisogno di acquistare separatamente il lettore e la Smart Card. Questo è stato il motivo che ha inizialmente spinto IBM ad installare sui ThinkPad il chip ESS (Encryption SubSystem), antesignano del TPM (Fritz Chip).
2. Fornire all'utente del PC le funzionalità crittografiche necessarie per cifrare e decifrare “al volo” documenti e comunicazioni.
3. Fornire all'utente le funzionalità necessarie per certificare e verificare in seguito l'identità di documenti, programmi e, indirettamente, utenti.
4. Fornire all'utente le funzionalità necessarie per rilevare cambiamenti sospetti nei programmi o, più in generale, nella piattaforma usata (nel PC).
5. Fornire all'utente le funzionalità necessarie per certificare la propria identità in Rete.
6. Fornire all'utente le funzionalità necessarie per controllare l'accesso di estranei alle risorse della propria rete, del proprio PC o di un suo qualunque elemento.
7. Fornire ai produttori di software una infrastruttura di sicurezza avanzata che potesse essere usata per l'implementazione di sistemi antivirus innovativi e di altri sistemi di sicurezza.
8. Fornire ai produttori di software e di contenuti multimediali le funzionalità crittografiche necessarie per implementare un nuova generazione di sistemi DRM che rendesse finalmente possibile il commercio di materiale digitale sulla Rete senza i problemi di copia abusiva che piagano il mercato al giorno d'oggi.

### Caratteristiche tecniche

Tecnicamente parlando, una piattaforma di Trusted Computing “standard” è composta sostanzialmente da un singolo microchip, chiamato Trusted Platform Module (TPM) o Fritz Chip. Questo chip deve fornire almeno le seguenti funzionalità.

1. Un motore crittografico implementato in hardware (e quindi molto veloce) in grado di cifrare e decifrare dati (documenti) e flussi di dati (comunicazioni) con un algoritmo RSA ed una chiave di cifra lunga fino a 2048 bit.
2. Una coppia di chiavi crittografiche RSA (pubblica e privata) usate per certificare l'identità del Fritz Chip. Questa coppia di chiavi viene generata in fabbrica e non è né modificabile né cancellabile in seguito. La chiave privata non lascia mai il Fritz Chip e non è accessibile in nessun modo. La chiave pubblica viene rilasciata all'esterno ed usata per decifrare i documenti cifrati con la chiave privata. In questo modo è possibile verificare l'identità del TPM senza conoscere la sua chiave privata.
3. Le funzionalità necessarie a generare nuove chiavi RSA a 2048 bit, usate come “identità virtuali” per le comunicazioni in Rete. Queste chiavi vengono usate anche per cifrare e decifrare documenti e flussi di comunicazione.
4. Uno spazio di memoria, interno al Fritz Chip, in cui memorizzare le chiavi. Questo spazio di memoria è inaccessibile dall'esterno.
5. Le funzionalità necessarie a “firmare” un documento con l'algoritmo RSA ed una chiave

lunga fino a 2048 bit.

6. Le funzionalità necessarie per verificare la provenienza e la attendibilità dei documenti sulla base della loro firma digitale.
7. Le funzionalità necessarie a generare certificati digitali RSA con cui “fotografare” documenti e programmi (cioè un “hashing”, secondo l'algoritmo SHA-1).
8. Le funzionalità necessarie a verificare l'identità e l'integrità di documenti e programmi sulla base del loro certificato digitale.

Queste funzionalità possono essere implementate da una circuiteria equivalente a quella del Fritz Chip e ricavata direttamente all'interno della CPU. Ad esempio, i processori VIA Technologies C3 – C7 mettono a disposizione tutte le funzionalità tipiche di un Fritz Chip, tranne l'attestazione remota, all'interno della CPU. I chip prodotti dalla inglese ARM dispongono al loro interno di una tecnologia, chiamata TrustZone, che è sostanzialmente equivalente a quella di un Fritz Chip. Per quello che è possibile saperne, sembra che sia Intel che AMD abbiano in progetto di integrare le funzionalità del Fritz Chip nelle loro CPU della prossima generazione.

La piattaforma (PC o altro dispositivo digitale) deve inoltre fornire le funzionalità del BIOS o del FirmWare necessarie per gestire il Fritz Chip e per verificare che l'avviamento dell'intera macchina avvenga seguendo una sequenza di stati affidabili e certificati (“Secure Boot”).

Le funzionalità del Fritz Chip sono una condizione necessaria per poter considerare un PC (od un altro dispositivo digitale) come “TC-compliant” ma non sono necessariamente le sole funzionalità riconducibili a questa tecnologia che possano essere implementate dal produttore. All'interno della sua architettura “LaGrande Technology”, Intel usa un Fritz Chip standard e vi aggiunge diversi elementi hardware e diverse funzionalità originariamente non previste dallo standard TCG. Lo stesso dovrebbe fare anche AMD (per restare compatibile con il suo concorrente).

### **Promesse**

Le funzionalità del Fritz Chip (sommate a quelle degli altri elementi eventualmente presenti) dovrebbero garantire all'utente i seguenti vantaggi.

1. Protezione crittografica dei dati dell'utente
2. Verifica della identità e integrità dei programmi
3. Verifica della identità e affidabilità dei Siti
4. Immunità dai Virus, Worm, Trojan, etc.
5. Pagamenti sicuri in Rete
6. Comunicazioni sicure in Rete
7. Sicurezza della propria Identità di Rete

### **Slide 4: La Realtà**

Come molti commentatori indipendenti hanno fatto notare, la realtà è piuttosto diversa.

1. Il TC può essere considerato un sistema DRM di seconda generazione già nella sua forma base e sicuramente può essere usato per creare sistemi DRM veri e propri. In entrambi i casi, questi sistemi DRM sono sostanzialmente inviolabili. In entrambi i casi, questi sistemi DRM consentono un livello di controllo molto superiore a quello a cui siamo abituati, al punto da poter essere usati efficacemente per imporre la censura su determinati documenti.
2. Il TC permette ai fornitori di software e di contenuti multimediali di esaminare e verificare la piattaforma (PC + software) dell'utente con un livello di dettaglio mai visto prima. Tecnicamente, è impossibile mentire o nascondere informazioni durante questa operazione di analisi (Remote attestation), cosa che crea degli enormi problemi di privacy.

3. Il TC permette (anche se indirettamente) di identificare l'utente, creando altri problemi di privacy.
4. Il TC permette di fornire beni digitali e servizi in modo diverso a utenti diversi od a piattaforme diverse, creando i presupposti per una emarginazione degli utenti “indesiderati” e per un “digital divide” mai visto prima.
5. Il TC permette di legare il consumo di contenuti multimediali e di servizi all'uso di software “certificato”, creando i presupposti per una emarginazione dal mercato dei concorrenti commerciali scomodi. Questo rappresenta un grosso rischio per la libera concorrenza ed il mercato.
6. Il TC crea dei seri problemi di sicurezza per gli enti istituzionali (governi, amministrazioni pubbliche, etc.) e per la Sicurezza Nazionale. Non solo non è possibile sapere cosa realmente facciano l'HW ed il SW crittografici di una piattaforma “trusted” ma, anche quando si attengono scrupolosamente allo standard TCG, sono già impossibili da verificare e da controllare. Chi produce questa tecnologia si trova in una posizione di forza mai vista prima rispetto agli utilizzatori, siano essi privati cittadini o interi governi.

A queste contestazioni bisogna aggiungere il fatto che il TC, di per sé, non fornisce nessun miglioramento nella difesa da virus, worm, Trojan, programmi spia ed “hacker”. In realtà, il TC non fornisce niente che non possa essere facilmente ottenuto già adesso con strumenti molto meno discutibili e molto meno invasivi, spesso addirittura con strumenti gratuiti già presenti su qualunque piattaforma.

La realtà è che il TC mette a disposizione dei fornitori di software e di contenuti multimediali quella piattaforma “sicura” per il commercio elettronico che chiedono da anni. In particolare, questa piattaforma permette ai fornitori di controllare il comportamento dei clienti e di difendersi da essi. In altri termini, il TC è una piattaforma concepita chiaramente per permettere ai fornitori di difendersi dagli utenti, non per permettere agli utenti di difendersi dai molti rischi di Internet.

## Slide 5 : Garanzie Apparenti

Nel tentativo di rassicurare gli utenti, le aziende si sforzano di fornire delle garanzie credibili riguardo alla protezione della privacy e riguardo al rispetto della libertà di scelta dell'utente. Le garanzie che vengono più spesso citate sono le seguenti.

1. Il Fritz Chip può essere completamente disabilitato.
2. La Endorsement Key (EK) che identifica il Fritz Chip non viene (quasi) mai usata e comunque può essere disabilitata.
3. La piattaforma (e quindi l'utente) non viene mai identificata dalla Endorsement Key ma sempre e solo da apposite Attestation Key (AK) generate ad hoc dall'utente.
4. Ci sono delle regole da rispettare (le “Best Practices”).

In sostanza, il TC viene presentato al pubblico come una tecnologia su cui si è riflettuto a lungo, alla ricerca del miglior compromesso tra sicurezza e libertà, e, soprattutto, viene presentato come uno standard rispettato da tutti.

## Slide 6: Rischi reali

In realtà, le garanzie fornite dal TCG e dalle aziende coinvolte nel progetto TC sono solo apparenti.

1. Innanzitutto, la possibilità di disabilitare il Fritz Chip, in tutto od in parte, è quasi solo teorica. Non appena questa tecnologia sarà abbastanza diffusa, sarà semplicemente impossibile accedere a software, contenuti multimediali, servizi di Rete e reti digitali protette da questa tecnologia senza avere un TPM attivo sulla macchina. Tra qualche anno, disabilitare in tutto od in parte il TPM sarà concettualmente equivalente a tagliarsi fuori dal mondo con le proprie mani.

2. Risalire alla identità dell'utente rimane comunque possibile, sia perchè il software che gira localmente alla macchina può comunque avere accesso alla EK, in certe condizioni, sia perchè la AK può essere “tracciata” come un normale cookie in Rete.
3. Il TCG definisce solo alcuni elementi di base di questa tecnologia. Ogni produttore è libero di utilizzare questi elementi come crede e, soprattutto, è libero di aggiungere altri elementi HW ed altre funzionalità. Questi “add-on” possono cambiare radicalmente la natura della piattaforma, trasformandola in una vera fortezza digitale o, più esattamente, in una prigione digitale per l'utente. Questo è quanto stanno facendo Intel, con il progetto LaGrande Technology, e AMD con l'equivalente progetto “Presidio”. Entrambe queste implementazioni proprietarie del TC ampliano di molto lo spettro di funzionalità del TC e lo rendono adatto ad applicazioni, come il DRM, per le quali il TC non era stato concepito in origine.
4. Il TC non è uno standard rispettato da tutti. Esistono diverse implementazioni proprietarie che non si attengono allo standard TCG, come quelle previste dall'inglese ARM (“TrustZone”) e da VIA Technologies (“Padlock”).
5. Non sono previste sanzioni per chi trasgredisce le regole di “bon ton” previste dal TCG (Le “Best Practices”). Di conseguenza, ogni produttore è libero di fare ciò che vuole.

## Slide 7: La comunicazione aziendale

Le aziende coinvolte nel progetto TC, ed il TCG stesso, hanno utilizzato strategie comunicative diverse nel corso di questi anni.

Il **TCG**, soprattutto per bocca di David Safford, si barriera dietro lo standard per difendersi dalle critiche. Le tesi che sostiene sono sostanzialmente due:

1. Lo scopo per cui è stato sviluppato il TC è quello di migliorare la sicurezza dell'utente.
2. Il TCG non è responsabile dell'uso “malvagio” di questa tecnologia, soprattutto non è responsabile dell'uso del TC come sistema DRM.

Inutile dire che all'utente finale interessa poco sapere per quale scopo sia stato concepito il TC e quanto il TCG sia responsabile dell'uso malvagio che ne verrà fatto. Se questa tecnologia verrà utilizzata per i fini che abbiamo accennato nella Slide 4, l'utente ne rimarrà comunque vittima.

**Apple**, che è stata la prima azienda ad avvalersi di questa tecnologia, ha scelto una strategia comunicazionale ancora più rudimentale: il silenzio.

Nella documentazione dei nuovi Mac basati su processori Intel non viene mai citata la presenza del TPM che, tuttavia, è stato identificato da utenti e sviluppatori. Non contenta della sua omertà aziendale, Apple ha persino fatto causa a diversi siti web che pubblicavano informazioni su questo aspetto dei MacIntel. Nonostante questo atteggiamento omertoso, Apple non ha mai smentito che il TPM sia installato su tutte le macchine di serie basate su processori Intel.

A quanto pare, Apple cerca di lasciar passare la convinzione, profondamente sbagliata, che il TPM presente sui nuovi MacIntel sia in qualche modo “castrato” o “limitato” nelle sue potenzialità e che, di conseguenza, non possa essere usato per gli scopi più inconfessabili del TC. In realtà, il TPM delle macchine Apple è un TPM pienamente funzionante e pienamente utilizzabile, sia da Apple che da qualunque altro fornitore, per qualunque scopo.

L'azienda che ha affrontato il tema della comunicazione aziendale con la maggiore goffaggine è stata sicuramente **Microsoft**. Non soltanto MS ha dovuto cambiare nome al suo progetto da “Palladium” a NGSCB per sottrarsi alle velenose critiche che avevano investito il progetto, MS ha anche dovuto ritardare più volte l'adozione di questa tecnologia, al punto che nemmeno ora, a distanza di oltre 6 anni dall'avvio del progetto, si sa con certezza quando arriverà sul mercato.

Come se non bastasse, il team di documentatori di MS è incorso in una serie di imbarazzanti

ammissioni sul sito dell'azienda, al punto che MS è stata costretta ad “archiviare” gran parte della documentazione esistente e rimpiazzarla con versioni più accettabili dal pubblico. Questa “archiviazione” è ben descritta da Catherine Flick nella sua tesi di laurea. Ad onore del vero, tuttavia, v'è riconosciuto che MS ha sempre avuto un atteggiamento abbastanza onesto ed esplicito riguardo a questa tecnologia.

**AMD**, come Apple, ha scelto la strada di un impossibile silenzio. Il suo progetto “Presidio” è avvolto da una nuvola di segreto del tutto risibile. Se AMD vuole avere qualche possibilità di vendere i suoi processori a qualcuno, dovrà per forza renderli compatibili con l'architettura Intel LaGrande su cui si basa MS per NGSCB. Di conseguenza, Presidio dovrà essere sostanzialmente un clone di Intel LaGrande.

L'unica azienda che sembra non essersi barricata dietro un imbarazzato silenzio o dietro una barriera di mezze verità è **Intel**. Intel descrive dettagliatamente la sua piattaforma LaGrande Technology e dichiara esplicitamente quali usi vuole farne, incluso gli usi come DRM. In questo è decisamente ammirevole ma, nello stesso tempo, mette in serio imbarazzo i suoi partner.

## Slide 8: Le critiche al TC

Sin dalla sua prima apparizione, nel 1999, il TC si è guadagnato una interminabile serie di critiche molto aspre. Ancora oggi è quasi impossibile trovare un osservatore indipendente che sia disposto a difendere pubblicamente questa tecnologia. Gli unici articoli non aziendali a difesa del TC sono quelli scritti tra il 2001 ed il 2003 da David Safford, un ricercatore dell'IBM che lavora sul progetto TC all'interno del TCG. Le principali critiche che vengono mosse al TC sono le seguenti.

1. Il TC non fornisce sicurezza agli utenti. Tutti i vantaggi offerti dal TC all'utente in termini di sicurezza sono facilmente ottenibili con tecnologie molto meno invasive e molto meno discutibili, come normali programmi di crittografia, firewall e Smart Card. Per esplicita ammissione di MS, il TC, di per sé, non porta nessun miglioramento alla difesa nei confronti di infezioni (virus e simili) e di “hacker”.
2. Il TC minaccia o viola apertamente la privacy dell'utente e ne consente il tracciamento in rete.
3. Il TC è un sistema DRM di seconda generazione. Lo è già nella sua forma base ma li diventa in modo ancora più evidente e pericoloso se combinato con software DRM vero e proprio.
4. Il TC può essere usato per la censura. Grazie alle sue caratteristiche di sistema DRM ed ERM di seconda generazione, il TC può essere usato per imporre una censura di tipo e di livello mai visti prima nella storia dell'uomo.
5. Il TC limita la libertà dell'utente e gli impone di usare solo determinati programmi. Il TC può essere usato per imporre all'utente l'uso di programmi e dispositivi hardware graditi al produttore dei contenuti e del software. MS ha già detto che su Windows Vista potranno essere usati solo driver software “certificati” e, quindi, solo l'hardware “certificato” che essi pilotano. Fine dei mod chip. Punto. Fine dei sistemi per clonare CD e DVD. Punto.
6. Il TC è una minaccia per il mercato e la concorrenza. Per i motivi appena esposti, il TC non è solo una minaccia per la libertà individuale ma anche per la libera concorrenza ed il mercato. Il TC può essere usato per estromettere dal mercato concorrenti scomodi e partner non disposti a pagare le royalties a chi detiene il controllo di questa tecnologia (in pratica, MS ed Intel).
7. Il TC dà ai fornitori l'accesso al PC dell'utente e viola la privacy. Il TC permette ad un fornitore di software, di contenuti multimediali o di servizi di rovistare nella macchina dell'utente per verificare cosa egli usi per accedere ai beni o servizi che sono oggetto della transazione. Di fatto, l'utente non può sottrarsi a questa perquisizione e non può mentire. In pratica, l'utente si trova inerme di fronte ad una azione poliziesca condotta, senza alcun mandato, da una azienda privata.
8. Il TC è una minaccia per la Sicurezza Nazionale. Dato che il TC viene proposto come una tecnologia destinata a diventare standard su ogni dispositivo digitale, PC o altro, che verrà

prodotto nei prossimi anni, è inevitabile che finisca per “infettare” anche i sistemi usati per applicazioni governative, istituzionali, amministrative e militari. Il pericolo che questa tecnologia rappresenta è evidente ma diventa ancora più inquietante se si riflette sul fatto che non è possibile, tecnicamente parlando, mettere in atto nessuna forma di controllo credibile, e nemmeno nessuna contromisura efficace, contro un sistema crittografico implementato in hardware come questo.

## Slide 9: Il Lessico del TC

Da più parti viene denunciata una sostanziale “oscurità” della documentazione dei produttori riguardo al TC, soprattutto quella destinata al grande pubblico ed agli “executive” delle aziende clienti. Catherine Flick, nella sua tesi di laurea, sottolinea questo problema con decisione e lo analizza con notevole chiarezza. A titolo di esempio, vengono spesso citati tre casi di deliberato equivoco sui reali significati dei termini usati. I tre termini incriminati sono “fidato”, “utente” e “proprietario”.

### Fidato, Cruciale e Affidabile

Nella documentazione del TC viene spiegato che il termine “Trusted” non viene inteso nel senso abituale. Il termine “Trusted” viene usato per riferirsi a qualcosa di cui si è costretti a fidarsi in quanto cruciale per la sicurezza dell'intero sistema, di solito qualcosa che conserva informazioni necessarie per l'accesso al sistema ed alle informazioni che esso contiene. Si tratta quindi di un elemento “Cruciale” (nel senso di “nodo centrale della croce”, sciolto il quale la croce si smonta), non di un elemento “Affidabile” (“Trustworthy”). Per questo motivo, da qualche tempo Microsoft ha cambiato la sua documentazione tecnica e si riferisce al TC come ad una tecnologia di “Trustworthy Computing”. La sostanza, tuttavia, rimane la stessa: il sistema è “Trusted” per l'utente perchè è costretto a fidarsi di esso, mentre è “Trustworthy” per i fornitori perchè, grazie ad esso, si mettono al riparo dai comportamenti illegali (od anche solo sgraditi) dei loro clienti.

### Utente

Uno degli elementi che induce maggiormente in errore è il fatto che l'utente della piattaforma Trusted Computing, cioè l'utente del TPM, non è l'utente del PC. L'utente del sistema TC è solitamente un perfetto estraneo che usa, attraverso la rete, i servizi del TPM per difendersi dall'utente del PC. In altri termini, spesso e volentieri il TPM lavora per qualcuno che considera l'utente come un avversario da cui difendersi o persino come una persona a cui imporre la propria volontà, a dispetto del fatto che è l'utente del PC ad avere acquistato e pagato il TPM. Francamente mi è difficile pensare a qualcosa di più diabolico sul piano comunicazionale.

### Proprietario

La diabolica situazione che si presenta nel caso del termine “Utente”, si ripete nel caso del termine “Proprietario”: il proprietario di un documento è la persona che detiene i diritti di controllo su di esso (grazie alle tecnologie di cifra del TC). Di solito questa persona è in realtà una azienda che detiene i diritti di copia (copyright) su questo documento. In modo simile, il proprietario del sistema TC (del TPM) è la persona che ha eseguito la procedura di inizializzazione del TPM (La “Take\_Ownership”). Questa persona non necessariamente coincide con chi ha pagato il PC o con chi lo usa. Potrebbe persino essere l'azienda che ha fornito il dispositivo. Infine, il proprietario di una comunicazione TC (ad esempio di una conversazione VoIP) è la persona che detiene il controllo su di essa attraverso il possesso delle relative chiavi crittografiche, di solito chi ha iniziato la conversazione. Queste sottili risemantizzazioni dei termini non saranno mai comprese appieno dall'uomo della strada e produrranno sicuramente degli effetti devastanti su molti aspetti delle relazioni umane, sociali ed aziendali.

## Slide 10: Le modifiche al TC

Per non essere tacciati di sterile lamentosità, molti osservatori si sono sforzati di individuare dei modi per rendere accettabile, da un punto di vista sociale, politico e legale, il TC. Il primo di questi

volonterosi ricercatori è stato Seth Schoen di EFF, che ha proposto la famosa “Owner Override”. Sulla sua scia anche altri hanno proposto modifiche più o meno estese alla tecnologia TC, tutte prontamente bocciate dalle aziende o semplicemente ignorate.

Il motivo di tanta freddezza è che ognuna di queste modifiche implica, in un modo o nell'altro, che l'utente sia messo in condizione di tacere o di mentire su aspetti cruciali della sua piattaforma di fronte ad una investigazione esterna. Questo vanifica completamente l'utilità del TC come strumento di “sicurezza” per il commercio elettronico e non è quindi accettabile per gli operatori del settore.

Personalmente, credo che sarebbe già stato un serio passo avanti prevedere l'esistenza di un Fritz Chip rimovibile e rimpiazzabile, in pratica una banale Smart Card. Questo avrebbe restituito al processo di gestione delle identità digitali la sua natura fisica, rendendo l'intero processo più comprensibile all'utente occasionale. Anche questa ipotesi, naturalmente, è stata sempre silenziosamente ignorata dalle aziende coinvolte in questo progetto.

## **Slide 11: Alcune modeste proposte**

Alla luce di questa analisi, ci sembra opportuno fornire alcune proposte.

1. Autorizzare l'uso del TC solo in ambiti Militari, di Intelligence, Governativi e Bancari. Il TC può essere una tecnologia cruciale in questi ambiti e non ha senso impedirsi di utilizzarla per questi scopi.
2. Vietare l'uso del TC nell' e-commerce e su Internet. Questo per evitare che il TC venga utilizzato per creare schemi di marketing (aka “politiche commerciali”) basati sul cliente e/o sulla piattaforma utilizzata. Schemi di questo tipo potrebbero facilmente trasformarsi in una vera trappola per l'utente e portare ad un suo progressivo asservimento alla volontà delle aziende.
3. Vietare l'identificazione Utente sulle reti pubbliche. Si tratta di una evidente violazione della privacy e non ha nessuna reale giustificazione tecnica. Il fornitore di un bene o di un servizio deve preoccuparsi di ottenere il pagamento del suo lavoro, non di determinare chi sia il suo cliente. Casi specifici, come quello di accessi a siti per adulti, possono essere affrontati in altro modo.
4. Vietare la Remote Attestation sulle reti pubbliche. Si tratta di una evidente violazione della privacy e non ha nessuna giustificazione tecnica. Cosa stia usando l'utente per accedere ai beni ed ai servizi messi a disposizione del fornitore deve essere un problema del cliente/utente e di nessun altro.
5. Vietare l'installazione di dispositivi TC non rimovibili (Fritz Chip) e favorire invece l'uso di Smart Card. Questo è l'unico modo di impedire che tutta la prossima generazione di hardware venga legata a questa tecnologia in maniera indissolubile, con tutti i rischi che questo comporta. Basti pensare a cosa succederebbe se i produttori decidessero di creare delle piattaforme (cioè dei PC) che “scadono” a date prefissate.
6. Favorire lo sviluppo di una industria europea dei chip per svincolarsi dalla „dittatura“ tecnologica USA. Ormai è evidente che per poter garantire la sicurezza delle nostre istituzioni e dei nostri cittadini è necessario guadagnare il controllo su questi elementi cruciali del sistema nervoso delle nostre società e delle nostre aziende.