

D. E.

CENTRO STUDI
DIFESA EUROPA

Via Lazzaretto 3 – 20124 Milano
Tel. 0262699146 – fax. 0262694922
www.bancaeuropa.org

E-GOVERNMENT & SECURITY PER LA DIFESA
E LA PUBBLICA AMMINISTRAZIONE
GIOVEDÌ 26 GIUGNO 2008 DALLE ORE 9 ALLE ORE 13.30 CIRCA
C/O SCUOLA TRASPORTI E MATERIALI – AULA MAGNA
VIALE DELL'ESERCITO 102– CITTÀ MILITARE, CECCHIGNOLA – ROMA

BIBLIOTECA APOSTOLICA VATICANA

Luciano Ammenti

Responsabile Coordinamento dei Sistemi Informatici C.E.D. Director

Ci sono sviluppi in merito allo standard universale di " negativo digitale" DNG- RAW ecc. le cui caratteristiche sono fondamentali nell'ambito della conservazione dei dati e della loro sicurezza di longevità.

Inoltre nell'ambito della tecnologia RF.ID standard [ISO 15693](#) come sono gli sviluppi relativi alla protezione dei dati residenti nel chip .

Esistono in commercio CARD che raggruppano tre tags con standard : [ISO 18000-6](#) [ISO 14443](#) [ISO 15693](#)?

CENTRO MILITARE STUDI STRATEGICI (CE.MI.S.S.)

Ten. Col. (Aeronautica Militare) **Volfango MONACI**

Capo Dipartimento Scienza, Tecnologia, Economia e Politica Industriale (S.T.E.P.I.)

Domanda “discorsiva” :

Il progresso Tecnologico cui gli ultimi decenni ci hanno abituato era stato ampiamente previsto. Negli anni settanta fu coniato il termine “Future shock” — choc da futuro — per esprimere la preoccupazione della difficoltà di adattamento, del cambiamento che le nuove tecnologie avrebbero introdotto nella vita di tutti i giorni.

Fu inventata una scala graduata di 5 Shock Levels:

Shock Level ZERO

identifica quelle tecnologie che la generazione precedente non avrebbe sognato, ma che ora sono di uso comune, e con le quali il “mitico ed inesistente” cittadino medio si sente a suo agio: Telefono cellulare, bancomat, televisore piatto da 30 pollici.

D. E.

CENTRO STUDI
DIFESA EUROPA

Via Lazzaretto 3 – 20124 Milano
Tel. 0262699146 – fax. 0262694922
www.bancaeuropa.org

Identifica pure quelle persone che tipicamente sono a loro agio con quelle tecnologie: giornalisti televisivi, uomini politici, tassisti.

Shock Level ONE

identifica tecnologie che piacciono ai tecnofili, agli ingegneri, agli “early adopters”, ai giovani... ed ai Direttori Commerciali delle Ditte che vogliono aprire un nuovo mercato. Sono tecnologie disponibili oggi, quali: realta' aumentata, biometria, avatar... I piu' anziani non le abbracciano con entusiasmo. ma tra meno di due decenni le considereremo Shock Level Zero.

Siccome il mio interesse professionale e personale e' rivolto a Tecnologie che potranno avere impatti di carattere strategico, la mia domanda alle Ditte e':
Cosa avete nei cassetti dei vostri Uffici Tecnici, in serbo per noi, che sia Shock Level TWO o superiore ?

AERONAUTICA MILITARE

Col. Giuseppe Gimondo

Capo del “Reparto Sistemi Automatizzati”, della 3ª Divisione del Comando Logistico A.M

- 1) **PREMESSA:** Le metodologie contrattuali attualmente adottate nell'ambito della pubblica amministrazione per l'esecuzione di imprese aventi per oggetto lo sviluppo di software sono fortemente vincolate ai processi “tradizionali” secondo i quali il fornitore sviluppa il software richiesto sulla base di requisiti tecnici specificati in appositi capitolati redatti dalla P.A.. Tale processo risulta poco efficace in termini di qualità dei risultati ottenuti. Infatti, considerati i costi di sviluppo che tipicamente sono molto elevati, se i capitolati tecnici prodotti per la gara, pur identificando nel dettaglio le funzioni da automatizzare, sono generici in termini di indicazioni su come tali funzioni dovranno essere svolte dal software (con particolare riferimento all'usabilità del software e all'efficienza dei processi automatizzati), la ditta si limiterà a sviluppare le funzioni richieste nel modo meno dispendioso possibile che non è mai quello migliore che è in genere il risultato dall'analisi comparativa di diversi approcci. Di contro, è evidente la scelta di redigere capitolati tecnici estremamente approfonditi nelle fasi preliminari del progetto è discutibile, sia perché le competenze richieste sono molto simili a quelle necessarie a sviluppare il successivo software (che se fossero presenti nella P.A. non richiederebbero l'outsourcing delle risorse), sia perché tali requisiti potrebbero risultare troppo stringenti e quindi limitare le possibilità offerte dalla tecnologia oppure dettare esigenze non ottenibili dalla stessa.

DOMANDA: quale approccio innovativo propone l'industria per ovviare a tali problematiche garantendo nel contempo la conformità dei processi tecnico amministrativi a quanto previsto dalla normativa vigente in materia di gare e appalti?

D. E.

CENTRO STUDI
DIFESA EUROPA

Via Lazzaretto 3 – 20124 Milano
Tel. 0262699146 – fax. 0262694922
www.bancaeuropa.org

- 2) **PREMESSA:** In materia di sicurezza nell'ambito dei sistemi informativi di grandi dimensioni è da sempre stata data grande importanza alla protezione dell'informazione da accessi non autorizzati sia in lettura sia in scrittura. Tale obiettivo è raggiunto proteggendo con crittografia i canali di comunicazione ed identificando e profilando gli utenti che accedono al sistema. In ambiente caratterizzato da numerosi utenti concorrenti assume inoltre particolare rilevanza la necessità di storicizzare i dati variabili in modo da potere ascrivere con certezza ogni modifica apportata al dato variabile ad uno specifico utente. La garanzia che il dato sia valido (cioè sia stato trattato nel modo corretto dal personale corretto) è fornita dal sistema nel quale è gestito.

DOMANDA: Nell'ambito delle nuove architetture SOA (Service Oriented Architecture) dove le informazioni gestite da una data applicazione non sono più fruite solo all'interno della stessa ma possono essere esposte mediante appositi servizi per essere utilizzati da altre applicazioni, quale è l'approccio più conveniente per garantire la sicurezza dei dati sia in termini di autorizzazione? Quale strategia può essere implementare per consentire che il dato esportato verso altri sistemi con i moderni meccanismi di interoperabilità mantenga inalterate le caratteristiche di validità/integrità (in pratica è possibile certificarne l'origine) anche dopo essere stato decontestualizzato dal sistema di origine?

STATO MAGGIORE DELL'ESERCITO

Ten. Col. **Marco Piantoni**

Reparto Logistico Ufficio Comunicazioni e Sistemi

I fattori di crescita ed evoluzione dell' IT e la sua diffusione in diversi settori di applicazione hanno portato ad accrescere le soluzioni tecnologiche portando alla definizione di nuovi standard e di nuovi sistemi. Si ritiene fondamentale per tanto realizzare una convergenza che si concretizza con la piena interoperabilità dei sistemi di comunicazione. Pertanto è necessario nell'implementazione delle nuove tecnologie salvaguardare l'interoperabilità con i sistemi in esercizio e contemporaneamente quella con analoghi sviluppi condotti dalle altre nazioni della NATO.

In questo ambito si inserisce la realizzazione per la F.A. di un Integrated Test Bed, come aspetto cruciale del progetto per la Trasformazione Terrestre in atto, che consentirà attraverso un sistema di Modelling & Simulation di testare i nuovi sistemi o più in generale nove.

Bisogna in merito sottolineare la necessità di individuare delle soluzioni o degli strumenti che possono salvaguardare gli aspetti peculiari della sicurezza, che nell'ambito Difesa hanno una elevata rilevanza.

Veniamo quindi alla domanda: “come vengono testate le vostre soluzioni e quali possono essere degli strumenti validi al fine di “stressare” i nuovi sistemi per verificarne la validità ai fine della sicurezza EAD?”

D. E.

CENTRO STUDI
DIFESA EUROPA

Via Lazzaretto 3 – 20124 Milano
Tel. 0262699146 – fax. 0262694922
www.bancaeuropa.org

MINISTERO DELLA DIFESA

Ten. Col. Vincenzo Iscaro

Sezione Sicurezza Sistemi Ufficio Sistemi Integrati NEC

I fattori di crescita ed evoluzione dell'ICT, con particolare riguardo allo sviluppo di reti di interconnessione tra i sistemi informativi che hanno uno spettro di applicazione sempre più ampio, impongono una rigorosa attenzione agli aspetti legati alla sicurezza. In tal senso è importante che le federazioni di reti siano adeguatamente supervisionate e si attui un rigoroso rispetto di procedure, regole e standard.

Questo fattore vale per tutto lo scenario delle applicazioni informatiche e di telecomunicazioni, in particolare per l'Amministrazione Difesa in considerazione delle interconnessioni che si realizzano con altri paesi appartenenti ad alleanze o coalizioni. Parallelamente la diffusione dell'utilizzo delle reti presenta ormai fattori di crescita esponenziali e le applicazioni su reti aperte sono diventate una realtà non più esclusiva del mondo imprenditoriale. Internet sta divenendo sempre più un sistema di scambio di informazioni. Chiaramente questa realtà ha i suoi fattori di rischio pertanto l'Information Assurance deve essere un elemento fondamentale e trasversale di cui tenere conto anche alla luce che lo spettro della minaccia assume caratteristiche di sempre maggiore sofisticazione in funzione all'evoluzione tecnologica dei meccanismi di sicurezza difensivi adottati. In tale contesto gli attacchi informatici possono essere diretti come nel caso dell'Estonia all'intero sistema informatico dello Stato coinvolgendo contemporaneamente Network di diverse Amministrazioni.

Per rispondere a queste minacce quali sono le soluzioni vincenti costo efficacia che ci consentirebbero di ridurre il rischio e avere una adeguata supervisione dell'Information Assurance nel suo complesso?

MINISTERO DELLA DIFESA/TELEDIFE

C. Amm. Giuseppe Ilacqua

Capo I° Reparto

TELEDIFE è la D.G. dell'Area T-A della Difesa competente per le forniture di progettazione, acquisizione e gestione dei sistemi informatici e telematici classificati e non classificati (a vario livello di sicurezza), dei sistemi di comando e controllo, intelligence, osservazione e riconoscimento e dei sistemi di telecomunicazione radio e satellitari; in pratica di tutti i sistemi-tecnologie compresi nella sigla C4ISTAR.

La Difesa da sempre progetta, realizza e certifica a sicurezza i sistemi classificati secondo le leggi-normative in vigore che prevedono la certificazione obbligatoria e dal 2006 ha iniziato a prevedere la certificazione a sicurezza anche dei sistemi informatici non classificati, come previsto dal D.M. del 30.10.2003 (ma senza sua obbligatorietà) in funzione delle relative funzioni e caratteristiche dei dati gestiti, sia per adempiere alla prescrizioni di legge relative alla tipologia di tali dati (finanziari, anagrafici, sanitari, logistici, ecc).

La sempre maggiore diffusione, per ragioni di costo-efficacia di gestione e di sicurezza, dei

D. E.

CENTRO STUDI
DIFESA EUROPA

Via Lazzaretto 3 – 20124 Milano
Tel. 0262699146 – fax. 0262694922
www.bancaeuropa.org

sistemi informatici a configurazione WEB BASED e le sempre maggiori esigenze di integrazione ed interfaccia tra i vari sistemi e database ICT e tra questi ed i sistemi-database classificati, come previsto dalle nuove architetture netcentriche, anche con configurazione "a servizi", rendono sempre più critiche le esigenze di disponibilità di: dispositivi di "multi level security", per l'interconnessione di sistemi e database delle suddette diverse tipologie;

sistemi di gestione integrata dell'efficienza e della sicurezza di CELD di alta complessità e di reti telematiche geografiche e locali;

sistemi di "identity management", con l'uso di smart card e biometria, per la "profilazione" degli utenti all'accesso ai vari tipi di sistemi e database.

Potete fornirci indicazioni sulle vostre capacità di fornire tali sistemi-dispositivi e sui relativi requisiti di certificazione.