

			
<p><u>SICUREZZA E TRUST NELLA CATENA DELLE CERTIFICATION AUTHORITY DELLA FIRMA DIGITALE</u></p> <p>CORRADO GIUSTOZZI, CISM, CRISC, ISO27001 LA</p> <p> <i>Permanent Stakeholders' Group, ENISA</i></p> <p> <i>Security Evangelist, Capgemini</i></p>			
28 febbraio 2012	Corrado Giustozzi	Pag. 1	

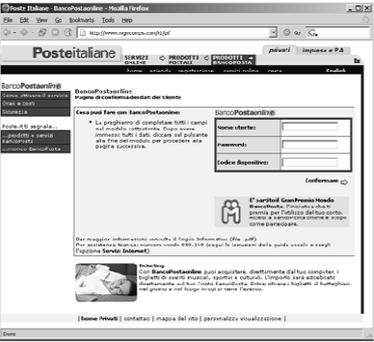
	Indice della presentazione	
<ul style="list-style-type: none"> • Considerazioni generali • Breve ripasso sulla firma digitale • Le autorità di certificazione e i modelli di trust • Il caso Jmicron/Realtek – Stuxnet • Il caso Comodo • Il caso Diginotar • Conclusioni 		
28 febbraio 2012	Corrado Giustozzi	Pag. 2

	Evoluzione del “documento”	
<ul style="list-style-type: none"> • Il documento “classico”: <ul style="list-style-type: none"> – è un oggetto materiale che coincide col suo supporto – è unico e originale, si distingue dalle copie – richiede una modifica fisica per la validazione • Il documento “moderno”: <ul style="list-style-type: none"> – è un oggetto immateriale (contenuto informativo) separato ed indipendente dal particolare supporto che lo ospita – ogni copia è un originale, anche su altro supporto – non ammette modifiche fisiche 		
28 febbraio 2012	Corrado Giustozzi	Pag. 3

	<h3>Le garanzie necessarie</h3>	
<ul style="list-style-type: none"> • Da sempre l'uomo ha chiesto ai documenti alcune importanti certezze: <ul style="list-style-type: none"> - autenticità - integrità - non ripudio - confidenzialità • Per ottenere queste certezze si è sempre fatto ricorso a modifiche fisiche al documento: <ul style="list-style-type: none"> - firme, sigilli, timbri, punzoni, filigrane, ologrammi, ... • ...ma il documento moderno è <i>immateriale!</i> 		
<p>28 febbraio 2012</p>	<p>Corrado Giustozzi</p>	<p>Pag. 4</p>

	<h3>Un altro problema...</h3>	
		
<p>28 febbraio 2012</p>	<p>Corrado Giustozzi</p>	<p>Pag. 5</p>

	<h3>Parliamo di identità digitale...</h3>	
<div style="display: flex; align-items: flex-start;"> <div style="flex: 1;">  </div> <div style="flex: 2;"> <ul style="list-style-type: none"> • Il netizen vive e si esprime sempre più soltanto in Rete • Anche senza chiamare in causa la fantascienza, la Rete tende a mediare e sostituire i contatti sociali (il che non è sempre un male!...) • L'interazione con la società digitale avverrà sempre di più mediante la Rete • Il principale crimine del ciber spazio nel futuro sarà il furto d'identità </div> </div>		
<p>28 febbraio 2012</p>	<p>Corrado Giustozzi</p>	<p>Pag. 6</p>

		<h3>...per non dire del phishing!</h3>			
					
28 febbraio 2012		Corrado Giustozzi		Pag. 7	

		<h3>Nuove forme di garanzia</h3>			
<ul style="list-style-type: none"> • Per fornire garanzie ai documenti digitali si usano tecniche innovative di <i>validazione</i> ottenute come effetto collaterale delle moderne tecniche di <i>protezione</i> delle informazioni • La <i>crittografia a chiave pubblica</i>, nata per proteggere le comunicazioni di massa, consente anche di attribuire <i>certezze</i> ad un documento digitale • Non si valida il <i>supporto</i> del documento bensì il suo <i>contenuto informativo</i> • Nasce così la cosiddetta <i>firma digitale</i> 					
28 febbraio 2012		Corrado Giustozzi		Pag. 8	

		<h3>Indice della presentazione</h3>			
<ul style="list-style-type: none"> • Considerazioni generali • Breve ripasso sulla firma digitale • Le autorità di certificazione e i modelli di trust • Il caso Jmicron/Realtek – Stuxnet • Il caso Comodo • Il caso Diginotar • Conclusioni 					
28 febbraio 2012		Corrado Giustozzi		Pag. 9	

	La crittografia a chiave pubblica - 1	
<ul style="list-style-type: none"> • È un sistema di codifica basato su una <i>coppia</i> di “chiavi” e su un procedimento di calcolo (cifratura) che fa uso dell'una o dell'altra chiave • Il sistema è tale che: <ul style="list-style-type: none"> – conoscendo una chiave non si può ricavare l'altra – un messaggio cifrato con una chiave si può decifrare solo con l'altra, e viceversa • In un sistema del genere: <ul style="list-style-type: none"> – una delle due chiavi (K_p) viene resa <i>pubblica</i> – l'altra (K_s) rimane <i>segreta</i> ossia è nota al solo proprietario • Il meccanismo sottostante è puramente matematico: <ul style="list-style-type: none"> – le chiavi sono numeri primi molto grandi (>200 cifre) – la codifica implica calcoli molto lunghi e complessi 		
28 febbraio 2012	Corrado Giustozzi	Pag. 10

	La crittografia a chiave pubblica - 2	
<ul style="list-style-type: none"> • Il sistema è fortemente asimmetrico: <ul style="list-style-type: none"> – chiunque può cifrare un testo con la chiave pubblica A_p di un soggetto A appartenente al sistema – tuttavia solo A può decifrare un messaggio cifrato con la sua chiave pubblica A_p, perché egli solo è in possesso della corrispondente chiave inversa A_s (la sua chiave segreta) • Vale anche il viceversa: <ul style="list-style-type: none"> – chiunque può decifrare un testo cifrato da A con la propria chiave segreta A_s perché la chiave inversa corrispondente è la A_p ovvero la chiave pubblica di A • Vigè il principio fondamentale del <i>non ripudio</i>: <ul style="list-style-type: none"> – se nessuno conosce la chiave segreta A_s di A, all'infuori di A stesso, allora ogni testo cifrato con A_s è <i>necessariamente</i> stato prodotto da A, e chiunque può verificarlo facilmente 		
28 febbraio 2012	Corrado Giustozzi	Pag. 11

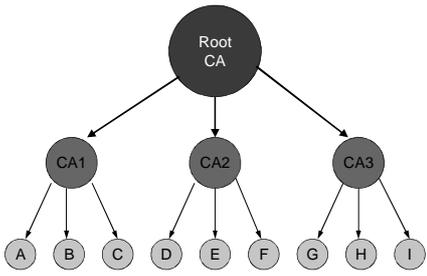
	Perché funziona?	
<ul style="list-style-type: none"> • Il principio su cui si può dare validità “forte” (anche legale) ad un documento sottoscritto con firma digitale si basa su una concatenazione di fatti inequivocabili e di alcune ipotesi ritenute ragionevoli data la natura del sistema • Fatti: <ul style="list-style-type: none"> – l'impronta è un riferimento univoco al documento D originale – l'impronta è stata cifrata con la chiave segreta A_s di A • Ipotesi: <ul style="list-style-type: none"> – solo A conosce e può usare la chiave segreta A_s – il soggetto che possiede la chiave segreta A_s è davvero A • Conclusioni: <ul style="list-style-type: none"> – solo A può aver generato quella firma – essa vale solo per il documento D cui si riferisce con certezza 		
28 febbraio 2012	Corrado Giustozzi	Pag. 12

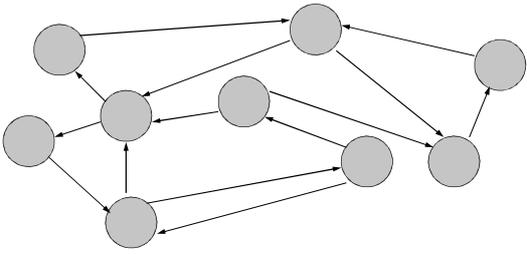
	L'anello debole del sistema	
<ul style="list-style-type: none"> • Affinché tutto funzioni occorre stabilire: <ul style="list-style-type: none"> – chi e come gestisce l'elenco delle chiavi pubbliche – chi e come garantisce la validità dell'elenco – chi e come garantisce sulla effettiva corrispondenza fra identità dei soggetti e relative chiavi pubbliche • Queste certezze fondamentali vengono fornite da un sistema cosiddetto di "certificazione" • La certificazione si attua mediante: <ul style="list-style-type: none"> – entità garanti denominate <i>autorità di certificazione</i> – strumenti tecnologici denominati <i>certificati digitali</i> 		
28 febbraio 2012	Corrado Giustozzi	Pag. 13

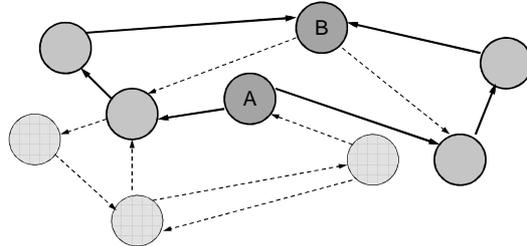
	Indice della presentazione	
<ul style="list-style-type: none"> • Considerazioni generali • Breve ripasso sulla firma digitale • Le autorità di certificazione e i modelli di trust • Il caso Jmicron/Realtek – Stuxnet • Il caso Comodo • Il caso Diginotar • Conclusioni 		
28 febbraio 2012	Corrado Giustozzi	Pag. 14

	Il processo di certificazione	
<ul style="list-style-type: none"> • L'Autorità di Certificazione è un soggetto <i>super partes</i>, affidabile per definizione, il quale: <ul style="list-style-type: none"> – attesta la validità di una chiave – garantisce l'identità del titolare – gestisce l'elenco delle chiavi pubbliche • Il Certificato Digitale da essa emesso contiene: <ul style="list-style-type: none"> – la chiave pubblica del titolare – i dati anagrafici del titolare (identità digitale) – ulteriori dati di servizio: scadenza, limitazioni, ... – il tutto "firmato" dalla CA 		
28 febbraio 2012	Corrado Giustozzi	Pag. 15

	Modelli di certificazione	
<ul style="list-style-type: none">• ISO X.509:<ul style="list-style-type: none">- standard <i>de iure</i> basato sulle Certification Authorities- struttura gerarchica organizzata formalmente- ogni CA certifica quelle al di sotto di lei- l'unico valido a norma di legge• Web of Trust:<ul style="list-style-type: none">- standard <i>de facto</i> affermatosi con PGP- modello cooperativo senza struttura formale- ogni utente certifica agli altri coloro di cui è certo- accettato informalmente ma privo di validità legale		
28 febbraio 2012	Corrado Giustozzi	Pag. 16

	Certificazione secondo X.509	
		
28 febbraio 2012	Corrado Giustozzi	Pag. 17

	Certificazione secondo PGP	
		
28 febbraio 2012	Corrado Giustozzi	Pag. 18

	Web of Trust	
		
28 febbraio 2012	Corrado Giustozzi	Pag. 19

	I certificati digitali	
<ul style="list-style-type: none"> • “Credenziali elettroniche” che autenticano il titolare di una coppia di chiavi di firma • Emessi dalle “Autorità di Certificazione” • Usati ad esempio dai browser per: <ul style="list-style-type: none"> – effettuare transazioni sicure garantendo l'identità del server remoto e attivando una crittografia di sessione (SSL/TLS) – cifrare messaggi di e-mail e/o di altro tipo (VoIP, ...) – garantire della provenienza di software • Danno validità legale ad una firma digitale, quando siano rispettate certe condizioni tecnico-operative 		
28 febbraio 2012	Corrado Giustozzi	Pag. 20

	Tecnologie chiave	
<ul style="list-style-type: none"> • Crittografia a chiave pubblica: <ul style="list-style-type: none"> – infrastruttura di sicurezza globale – prerequisito per la firma digitale • Firma digitale: <ul style="list-style-type: none"> – certezza degli atti e documenti elettronici • Autorità di certificazione: <ul style="list-style-type: none"> – certezza dell'identità e della responsabilità – garanzia di autenticità dei documenti • Certificati digitali: <ul style="list-style-type: none"> – identificazione certa dei titolari – garanzia di identità 		
28 febbraio 2012	Corrado Giustozzi	Pag. 21

	Indice della presentazione	
<ul style="list-style-type: none"> • Considerazioni generali • Breve ripasso sulla firma digitale • Le autorità di certificazione e i modelli di trust • Il caso Jmicron/Realtek – Stuxnet • Il caso Comodo • Il caso Diginotar • Conclusioni 		
28 febbraio 2012	Corrado Giustozzi	Pag. 22

	Stuxnet, un virus “firmato”	
<ul style="list-style-type: none"> • Nel giugno 2010 i ricercatori di VirusBlokAda identificano un nuovo worm che si propaga sfruttando ben quattro vulnerabilità zero-day di Windows • La diffusione iniziale avviene mediante chiavette USB da cui vengono installati <i>device driver validamente firmati</i> • Nelle settimane successive apparirà chiaro che si tratta di un prodotto estremamente sofisticato, il quale ha come bersaglio specifici sistemi SCADA prodotti dalla Siemens • Il 60% dei sistemi colpiti si trova in Iran, il che ha fatto ritenere trattarsi di un attacco mirato contro i sistemi industriali degli impianti di arricchimento dell'uranio • Si scoprono successivamente diverse versioni di Stuxnet, alcune risalenti addirittura al giugno 2009 		
28 febbraio 2012	Corrado Giustozzi	Pag. 23

	Furto di certificati validi	
<ul style="list-style-type: none"> • Stuxnet installa sui sistemi Windows un <i>rootkit</i> i cui device driver sono firmati digitalmente con certificati validi, e ciò ha fatto sì che la minaccia rimanesse a lungo nascosta • I certificati, emessi da Verisign, appartengono a due note aziende elettroniche taiwanesi: Jmicron e Realtek • Entrambe le aziende hanno sede nello Hsinchu Science Park, grande complesso industriale di Taiwan, e ciò ha fatto pensare che i certificati siano stati trafugati mediante accesso fisico alle rispettive sedi; tuttavia ancora non è stato chiarito il modo in cui ciò è effettivamente avvenuto • Verisign ha prontamente revocato i certificati, ma è stato necessario un aggiornamento di Windows per distribuire efficacemente la revoca su tutti i sistemi del mondo 		
28 febbraio 2012	Corrado Giustozzi	Pag. 24

	Indice della presentazione	
<ul style="list-style-type: none"> • Considerazioni generali • Breve ripasso sulla firma digitale • Le autorità di certificazione e i modelli di trust • Il caso Jmicron/Realtek – Stuxnet • Il caso Comodo • Il caso Diginotar • Conclusioni 		
28 febbraio 2012	Corrado Giustozzi	Pag. 25

	Emissione fraudolenta	
<ul style="list-style-type: none"> • Comodo è un gruppo di aziende americane che produce software di sicurezza; tra di esse vi è Comodo CA, una certification authority regolarmente accreditata che vende molti tipi di certificati digitali (OV, DV, EV SSL, ...) • Nel marzo 2011 Comodo ha reso noto che, in seguito alla compromissione di un account in una Registration Authority affiliata, aveva emesso nove certificati validi ma fraudolenti intestati a sette noti domini commerciali tra cui: <ul style="list-style-type: none"> – mail.google.com, www.google.com – login.yahoo.com (tre certificati) – login.skype.com – addons.mozilla.org • Il certificato intestato a Yahoo ha svolto attività su Internet 		
28 febbraio 2012	Corrado Giustozzi	Pag. 26

	Analisi dell'incidente	
<ul style="list-style-type: none"> • Comodo ha provveduto a revocare i certificati non appena si è accorta della loro emissione fraudolenta • I produttori di browser sono stati avvertiti immediatamente ed hanno provveduto ad eliminare i certificati dai propri prodotti mediante aggiornamenti coordinati • I risultati pubblicati da Comodo in seguito all'analisi dell'incidente occorso affermano che: <ul style="list-style-type: none"> – l'attacco ha riguardato e compromesso la sola RA periferica – né i sistemi della CA né le chiavi nell'HSM sono stati compromessi – l'attacco era stato pianificato da tempo e svolto con cura chirurgica – l'attacco proveniva da un IP allocato in Iran (212.95.136.18) – l'attaccante aveva controllo sull'infrastruttura DNS • Comodo ritiene pertanto che l'attacco fosse governativo 		
28 febbraio 2012	Corrado Giustozzi	Pag. 27

	Indice della presentazione	
<ul style="list-style-type: none"> • Considerazioni generali • Breve ripasso sulla firma digitale • Le autorità di certificazione e i modelli di trust • Il caso Jmicron/Realtek – Stuxnet • Il caso Comodo • Il caso Diginotar • Conclusioni 		
28 febbraio 2012	Corrado Giustozzi	Pag. 28

	Infrastruttura critica di e-gov	
<ul style="list-style-type: none"> • DigiNotar è (era...) una CA olandese: <ul style="list-style-type: none"> – fondata nel 1997 dal notaio Dick Batenburg e dal Koninklijke Notariële Beroepsorganisatie (Notariato olandese) – nasce per fornire ai notai servizi di Trusted Third Party – acquistata nel 2010 da VASCO Data Security International – posta in liquidazione volontaria il 20 settembre 2011 a seguito della scoperta di un'estesa compromissione dei propri sistemi critici • Forniva certificati general purpose ma anche certificati per l'infrastruttura di firma digitale nell'ambito del programma di e-government del Governo olandese (PKloverheid) • Era soprattutto la Root CA per molti enti governativi tra cui: <ul style="list-style-type: none"> – "Staat der Nederlanden" root CA – DigiD, piattaforma centralizzata di autenticazione per e-government – Rijksdienst voor het Wegverkeer (registro automobilistico) 		
28 febbraio 2012	Corrado Giustozzi	Pag. 29

	Compromissione totale (1/2)	
<ul style="list-style-type: none"> • Il 27 agosto 2011 uno studente iraniano segnala su un forum di Google che il suo browser Chrome gli indica come non valido il certificato SSL usato dal server di Gmail • Si tratta di un certificato fraudolento emesso da DigiNotar il 10 luglio, a seguito di un'intrusione nella sua CA; esso viene usato nell'ambito di un ampio attacco di tipo "man-in-the-middle" condotto verso utenti di posta Gmail in Iran • Il 29 agosto, su pressioni del GOVCERT-NL, DigiNotar revoca quel certificato; nei giorni successivi tuttavia si scoprono molti altri certificati analoghi "in the wild" • Il 30 agosto DigiNotar rivela di essersi accorta sin dal 19 luglio di un'intrusione sui propri sistemi, ma afferma che l'infrastruttura PKloverheid non è stata compromessa 		
28 febbraio 2012	Corrado Giustozzi	Pag. 30

	Compromissione totale (2/2)	
<ul style="list-style-type: none"> • Il 30 agosto 2011 DigiNotar commissiona alla società Fox-IT un audit approfondito su tutti i propri sistemi • Il 2 settembre il Governo olandese ritira la fiducia a DigiNotar ma non revoca ancora i certificati di PKloverheid; tuttavia afferma di non poter garantire l'affidabilità della piattaforma di e-gov ed invita i cittadini a non servirsene • Il 3 settembre il Governo olandese assume il controllo delle operazioni di DigiNotar, revoca i certificati di DigiD e PKloverheid e li rimpiazza con certificati Getronics • Il 5 settembre viene pubblicato il report preliminare di Fox-IT che dimostra come la compromissione sia totale • Fra il 2 e il 9 settembre Windows e tutti i browser vengono aggiornati eliminando DigiNotar dalla lista delle Root CA 		
28 febbraio 2012	Corrado Giustozzi	Pag. 31

	Analisi dell'incidente (1/2)	
<ul style="list-style-type: none"> • Non è stato possibile determinare il numero esatto di certificati emessi fraudolentemente: <ul style="list-style-type: none"> – vi sono indicazioni sul fatto che siano certamente più di 531 – DigiNotar non ha potuto garantire che tutti siano stati revocati – soltanto Google ne ha posti in blacklist 247 • I certificati erano intestati ad oltre 300 domini tra cui: <ul style="list-style-type: none"> – aziende ed organizzazioni: Aol, Android, Google, Microsoft, Mozilla, Skype, Twitter, Yahoo, Facebook, Torproject – servizi: Windows Update e Wordpress – CA: Digicert, GlobalSign, Thawte, Comodo, VeriSign, CyberTrust – enti governativi e servizi di intelligence: Mossad, Cia, MI5 		
28 febbraio 2012	Corrado Giustozzi	Pag. 32

	Analisi dell'incidente (2/2)	
<ul style="list-style-type: none"> • Il report di Fox-IT dipinge uno scenario drammatico di incuria ed inadeguatezza nella gestione di DigiNotar: <ul style="list-style-type: none"> – assenza di separazione tra le componenti critiche della CA – tutti i server della CA, benché posti in locali anti-tempest, erano accessibili tramite la LAN di management – tutti i server facevano parte di uno stesso dominio Windows ed erano accessibili mediante un'unica coppia userid/password – la password era assai debole e quindi facilmente craccabile – sui server non erano installati antivirus/antimalware – mancava un sistema di raccolta centralizzata e di analisi dei log • È emerso inoltre che: <ul style="list-style-type: none"> – sui server critici erano presenti molteplici malware – i prodotti di front-end sui server Web non erano aggiornati/patchati 		
28 febbraio 2012	Corrado Giustozzi	Pag. 33

	Ulteriori considerazioni	
<ul style="list-style-type: none"> • L'analisi ha tra l'altro evidenziato che prime tracce dell'attacco risalivano addirittura al 17 giugno, cioè più di un mese prima di quanto DigiNotar sospettasse • È successivamente stato reso noto da F-secure che già nel 2009 DigiNotar era caduta vittima di diversi attacchi di tipo <i>defacement</i> provenienti dall'Iran e dalla Turchia • L'analisi delle richieste dimostra che l'area di utilizzo dei certificati fosse concentrata quasi esclusivamente in Iran: <ul style="list-style-type: none"> – fra il 4 ed il 29 agosto il certificato intestato a Google è stato acceduto per verifica da oltre 300.000 IP diversi, per il 99% iraniani – ciò porta a ritenere che si sia trattato di una azione governativa finalizzata all'intercettazione della posta scambiata su Gmail – si ritiene che in seguito all'attacco siano state compromesse oltre 300.000 caselle di posta di Gmail appartenenti a cittadini iraniani 		
28 febbraio 2012	Corrado Giustozzi	Pag. 34

	Provenienza delle richieste	
		
28 febbraio 2012	Corrado Giustozzi	Pag. 35

	Indice della presentazione	
<ul style="list-style-type: none"> • Considerazioni generali • Breve ripasso sulla firma digitale • Le autorità di certificazione e i modelli di trust • Il caso Jmicron/Realtek – Stuxnet • Il caso Comodo • Il caso Diginotar • Conclusioni 		
28 febbraio 2012	Corrado Giustozzi	Pag. 36

	Considerazioni finali (1/2)	
<ul style="list-style-type: none"> • <i>"This is a nightmare scenario. You have to trust the companies selling these certificates and if we can't, then all bets are off."</i> (Mikko Hyppönen, responsabile della ricerca di F-secure, sul caso Comodo) • Il futuro della società digitale si basa sulla possibilità di attribuire certezze all'interazione non in presenza: <ul style="list-style-type: none"> - sull'identità dei partecipanti - sui loro diritti a partecipare all'interazione - sull'integrità della comunicazione - sulla riservatezza dell'accaduto • Le CA svolgono un ruolo chiave in questo scenario, perché da esse dipende la fiducia di tutti nel corretto funzionamento dell'intero sistema della società digitale 		
28 febbraio 2012	Corrado Giustozzi	Pag. 37

	Considerazioni finali (2/2)	
<ul style="list-style-type: none"> • I recenti episodi di attacchi alle CA dimostrano che esse sono un'infrastruttura critica estremamente appetibile per i malintenzionati, in quanto da esse dipende la possibilità di condurre con successo azioni malevole su grande scala • Tali episodi suggeriscono altresì che il problema dell'integrità della catena del trust sia troppo sottovalutato: <ul style="list-style-type: none"> - quasi nessun browser verifica i certificati sulle liste di revoca - molti root certificates sono cablati nei sistemi utente - molte CA rilasciano certificati senza troppi controlli • Le CA rischiano quindi di diventare l'anello più debole nella catena del trust! • Vale sempre l'antico dubbio di Giovenale: <i>"quis custodiet ipsos custodes?"</i> 		
28 febbraio 2012	Corrado Giustozzi	Pag. 38

	Evviva, abbiamo finito!	
<p style="text-align: center;">GRAZIE PER L'ATTENZIONE</p> <div style="display: flex; justify-content: space-around; align-items: center;">  <div style="text-align: center;"> <p>SICUREZZA E TRUST NELLA CATENA DELLE CERTIFICATION AUTHORITY DELLA FIRMA DIGITALE</p> </div> </div>		
28 febbraio 2012	Corrado Giustozzi	Pag. 39
