




 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 1 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

Manuale tecnico

Uso del servizio α PeS di generazione timbri digitali 2D-Plus da parte di applicativi aziendali



Release	Data	Modifiche effettuate	Redatto (acronimo)	Approvato (acr. Pm)
		Origine: [SE_T-07-0049] T I ALL Manuale appliance [2.3].odt	URS, ESP, ADM	n.a.
1.0	10/03/2009	Prima Emissione	SFN	n.a.
1.1	18/03/2009	Note sulle prestazioni e sul trattamento dei dati binari	SFN	n.a.
2.0	23/03/2009	Modifica dei capitoli Dettagli Sull'Output; XML/XSL; RSA Signature ; Nota sulla distinzione tra DPI e PPI;	SFN, FCR, URS	SFN
2.1	28/07/2009	aggiornamento elenco documentazione; eliminazione del capitolo sui formati dati; inserimento di un capitolo di configurazioni utilizzabili sull'appliance di test	SFN	n.a.
3.0	19/08/2009	Aggiunta di un paragrafo preliminare sull'interfaccia Web Service SOAP/HTTPS; leggera ristrutturazione del Capitolo 4	FCL	n.a.
3.1	25/09/2009	Modifica URL per interfaccia SOAP	FCL	n.a.
3.2	02/02/2010	Correzione nome file TimbroDigitale.jpg Paragrafo 5.1.3	ESP	n.a.
3.3	08/02/2010	Aggiornamento RETCODE, traduzione in italiano	ESP	n.a.
3.4	25/03/2010	Corretto href per interfacciamento SOAP	MNG	MNG
3.5	21/06/2010	Aggiornamento RETCODE, traduzione in italiano	ESP	

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 2 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 3 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		



SOMMARIO

1	DEFINIZIONI E ACRONIMI.....	4
2	DOCUMENTAZIONE DI RIFERIMENTO.....	5
3	SCOPO DEL DOCUMENTO.....	6
3.1	PRIMA DI INIZIARE.....	6
4	INTERFACCIARE L'APPLIANCE PES™.....	8
4.1	PROTOCOLLO-BASE DI COLLOQUIO.....	8
4.2	PROTOCOLLI APPLICATIVI.....	9
4.2.1	<i>Premessa.....</i>	9
4.2.2	<i>Chiamata diretta HTTPS.....</i>	10
4.2.3	<i>Interfaccia preliminare SOAP.....</i>	10
5	OUTPUT DEL SERVIZIO.....	11
5.1	DETTAGLI SULL'OUTPUT.....	12
5.1.1	<i>Caso Image:.....</i>	12
5.1.2	<i>Caso TD:.....</i>	12
5.1.3	<i>Caso PDF.....</i>	13
5.1.4	<i>Caso p7m.....</i>	13
5.2	PARAMETRI OPZIONALI.....	14
5.2.1	<i>Img_DPI (*).....</i>	14
5.2.2	<i>PeS_image_format.....</i>	16
5.2.3	<i>PeS_IMG_MAXWmm e PeS_IMG_MAXHmm.....</i>	16
5.3	RETCODE.....	18
6	CARATTERISTICHE DELLE IMMAGINI E DEI LORO FORMATI.....	22
7	PIATTAFORMA DI TEST ED ESEMPI D'USO.....	24
8	FORMATO DATI DA INVIARE ALL'APPLIANCE.....	25

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 4 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

1 DEFINIZIONI E ACRONIMI

Termine/Sigla	Descrizione
DRT (Dichiarazione per Richiesta Timbro)	Documento preparato dal RAp; contiene le informazioni necessarie affinché il TSC abbia consapevolezza (legale) di ciò che la sua Smart Card firmerà
ICP (Identificativo Configurazione PeS)	Identificativo di un gruppo di informazioni e parametri necessari per generare un timbro digitale per un DT, in modo coerente con quanto indicato
PAdm (PeS Administrator)	amministratore del Software Core Appliance α PeS 2D-Plus™
RAp (Responsabile Applicazione)	persona fisica/ufficio che fornisce le informazioni al Titolare relativamente al contenuto dei documenti che quest'ultimo autorizzerà a firmare in modo automatico, con la smart card di cui risulta intestatario.
SSD	Secure Signature Device; sono gli apparati sicuri di firma, necessari a generare una firma digitale a norma; un caso tipico di SSD è una smart card certificata Common Criteria EAL4+ secondo CWA 14169
Timbro Digitale	rappresentazione convenzionale di informazioni (tutte o una sola parte di esse) contenute in un documento elettronico stampabile, riconoscibile con strumenti elettronici, ottenuta utilizzando una codifica grafica definita. (definizione CNIPA). La codifica grafica qui definita è il codice 2D-Plus®; nel resto del documento si utilizzerà <i>timbro digitale</i> o <i>2D-Plus®</i> indifferentemente;
TSC (Titolare Smart card):	persona fisica, che fa la richiesta ed a cui è assegnata una Smart Card di firma digitale, di cui quindi risulta intestatario e responsabile;
u.v.	ultima versione disponibile

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 5 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		



2 DOCUMENTAZIONE DI RIFERIMENTO

Smart Card Owner Guide Manuale dell'interfaccia web per il titolare di una Smart Card di firma digitale automatica [SE_T-07-0049] T I MAN Smart Card Owner Guide [u.v].pdf
Procedure Operative Piattaforma PeS 2D-Plus® Procedure operative e policy di sicurezza, nell'integrazione di una piattaforma Appliance α PeS 2D-Plus® [SE_T-07-0049] T I DST proc operative α PeS [u.v].pdf
DRT- Form di richiesta TD Dichiarazione di Richiesta di un Timbro Digitale per uno specifico documento (Policy) [SE_T-07-0049] T E ALL DRT - Form richiesta TD [u.v].pdf
Decoder Plus® - User Guide Manuale utente del software Decoder 2D-Plus® [SE_T-07-0053] T I MAN User Guide [u.v].pdf
Useful Data Structures Strutture dati interpretate e vantaggiose nel codice grafico bidimensionale 2D-Plus® [SE_T-07-0054] DST useful data structures [u.v].pdf
Code Examples Esempi di programmazione in vari linguaggi [SE_T-07-0053] T I ALL CodeExamples [u.v].pdf

La documentazione indicata, può essere liberamente scaricata dall'indirizzo:

http://www.secure-edge.com/Appliance_PeS/doc/

NOTA: nel presente documento, possono essere indicati suffissi di file, in formato maiuscolo o minuscolo. Il formato del suffisso è indifferente, il file sarà comunque riconosciuto e trattato in modo opportuno dai software interessati.

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 6 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

3 SCOPO DEL DOCUMENTO

Il presente manuale definisce le modalità per interfacciare correttamente, a livello applicativo, un Appliance α PeS™, allo scopo di utilizzare il servizio di generazione di codici 2D-Plus®

Vengono quindi indicate le tipologie di codice 2D-Plus® che è possibile generare; in ultimo vengono specificati i formati dati che il software Decoder 2D- Plus® ha la capacità di interpretare direttamente, con una serie di esempi e consigli sulla modalità di progettazione dei dati.

I destinatari di questo documento sono sia i responsabili delle applicazioni software, sia gli stessi sviluppatori di queste applicazioni.

Nel documento, non sono presenti indicazioni relative alle performance dell'Appliance α PeS™, in quanto troppo dipendenti dalla piattaforma hw e del tipo di SSD (Secure Signature Device) utilizzata per la firma automatica.

A puro scopo indicativo si ricorda che una Smart Card utilizzabile per la creazione di una firma digitale a norma legale, riesce ad elaborare una firma in circa un secondo.

L'appliance è capace di gestire più Smart Card contemporaneamente, ovvero HSM dedicati.



In quest'ultimo caso, l'appliance in configurazione standard, potrebbe creare circa 50 timbri digitali al secondo.

§

3.1 PRIMA DI INIZIARE

L'interfacciare un Appliance α PeS™, da parte di una applicazione prevede che siano state effettuate una serie di attività e procedure organizzative; solo a titolo di esempio, ed in breve:

- ♦ l'ufficio responsabile per l'emissione del documento a cui si vuole applicare il timbro digitale, deve aver documentato la sua richiesta, indicando il tipo documento, i dati che verranno firmati, i destinatari del documento e la persona fisica che dovrà fare apporre la propria firma digitale tramite procedura automatica;
- ♦ Esiste una persona fisica (Titolare) che firmerà digitalmente i dati, permettendo la realizzazione del timbro digitale per il documento in questione. Questa persona fisica, dovrà già avere a disposizione, o avrà fatto richiesta, di una smart card con un certificato di firma automatica; inoltre si dovrà essere assicurato, magari tramite dichiarazione formale, che la sua smart card sarà usata solo per firmare i documenti di cui è conoscenza e che questa risiederà in un ambiente controllato;

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 7 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

- ♦ Esiste un responsabile dell'applicazione (colui che è interessato a questo manuale), che dovrà dichiarare quale applicazione genera quale documento ed in che formato e con quale configurazione verrà fatta richiesta di creazione del timbro digitale.
- ♦ Esiste un Amministratore dell'Appliance α PeS™, che dovrà dichiarare che la smart card del Titolare verrà associata alla configurazione in precedenza definita dal responsabile applicativo; inoltre dovrà operare affinché il titolare rimanga l'unico che abbia la possibilità di attivare o disattivare la propria smart card e che quest'ultima sia conservata in modo da non essere disponibile ad altri se non al titolare.

A titolo di suggerimento:

Un formulario di esempio, che riepiloga le informazioni ed i ruoli interessati dalle politiche di sicurezza ed organizzative è presente come:

[SE_T-07-0049] T E ALL DRT - Form richiesta TD [u.v].doc



disponibile all'indirizzo http://www.secure-edge.com/Appliance_PeS/doc/

Una traccia sulle sequenze operative, sui ruoli che ruotano intorno alla generazione di un timbro digitale e sulle attività che vanno svolte, è presente nel documento:

Procedure Operative Piattaforma PeS 2D-Plus®

disponibile all'indirizzo http://www.secure-edge.com/Appliance_PeS/doc/

§

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 8 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

4 INTERFACCIARE L'APPLIANCE α PeS™

Un Appliance α PeS™, è un computer connesso ad una rete locale, al quale si possono richiedere una serie di servizi, in genere dedicati alla creazione di timbri digitali basati sul codice grafico 2D- Plus® ed alla firma digitale.

Le richieste vengono rivolte all'appliance da parte di applicativi software, che possono interfacciarsi alla rete.

§

4.1 PROTOCOLLO-BASE DI COLLOQUIO



Attualmente il protocollo usato tra le applicazioni e l'appliance è HTTPS, una combinazione tra il protocollo HTTP ed un canale di comunicazione sicuro basato su SSL o TLS.

Sarebbe possibile utilizzare anche il semplice protocollo HTTP, ma questa soluzione è da scoraggiare, in quanto tipicamente l'appliance applica una operazione di firma digitale automatica ai dati che gli vengono inviati; se questi dati viaggiassero senza protezione, potrebbero essere modificati durante il percorso applicazione-appliance, con spiacevoli conseguenze.

La generazione di un canale di comunicazione sicuro basato su SSL o TLS prevede l'uso di crittografia asimmetrica RSA e certificati di chiave pubblica X.509.

Prima di poter instaurare un colloquio di questo tipo, il responsabile dell'applicazione dovrà confrontarsi con l'Amministratore dell' Appliance α PeS™ (PAdm).

§

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 9 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

4.2 PROTOCOLLI APPLICATIVI

4.2.1 PREMESSA

L'appliance agisce come un server web; le informazioni che gli sono necessarie per agire sono di tre tipi:

- ✓ **comandi** che esplicitano il tipo di funzione richiesta;
- ✓ **metadati** che completano le informazioni necessarie all'erogazione del servizio;
- ✓ **dati** quanto deve essere gestito;

I comandi ed i metadati necessari al lavoro, sono contenuti in oggetti (strutture dati) definiti **Configurazioni** che possiedono un identificatore univoco (ICP - Identificativo Configurazione PeS) e sono contenuti nell'Appliance.

In una configurazione sono presenti una serie di dati che permettono di verificare se la richiesta fatta all'appliance sia corretta, quale host/applicazione può fruire dei servizi associati alla configurazione richiesta, cosa e come operare sui dati allo scopo di realizzare un timbro digitale, che cosa restituire ed in che formato e così via.



La definizione ed il contenuto di una configurazione è una responsabilità congiunta a diversi livelli, di più ruoli aziendali; l'identificativo ICP viene fornito dal PAdm; si rimanda per i dettagli al documento:

Procedure Operative Piattaforma PeS 2D-Plus®

disponibile all'indirizzo http://www.secure-edge.com/Appliance_PeS/doc/

Dunque, per poter richiedere all'appliance un servizio, l'applicazione dovrà prima di tutto sapere a quale configurazione deve fare riferimento.

Al momento l'interfaccia applicativa principale e stabile messa a disposizione dall'appliance è la chiamata diretta HTTPS; è presente anche una versione preliminare di interfaccia Web Service tramite SOAP/HTTPS, che tuttavia potrà subire modifiche anche significative.

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 10 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance αPeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

4.2.2 CHIAMATA DIRETTA HTTPS

La richiesta di servizio si può esprimere come segue:

https://<nome appliance | IP Address>/cgi-bin/gateway?cfg=<ICP>&data=<dati>

<ICP> è l'identificativo della configurazione; formato: stringa alfanumerica;

<data> sono i dati da elaborare; formato: *URL Encoded*;

I parametri <ICP> e <data> sono i soli parametri obbligatori.

Successivamente vedremo una serie di altri parametri opzionali, che possono essere inseriti in sostituzione –temporanea– di quanto indicato nella configurazione.

Il passaggio dei parametri può avvenire indifferentemente con metodo POST o GET.

Esempi di codice in linguaggio di programmazione Php, Java e C#, per la richiesta di servizio all'appliance, sono disponibili all'indirizzo:

http://www.secure-edge.com/Appliance_PeS/code/

§

4.2.3 INTERFACCIA PRELIMINARE SOAP



Questa interfaccia Web Service è ancora ad un livello preliminare; di conseguenza, non dispone di tutte le opzioni previste dalla chiamata diretta HTTPS.

Per usare l'interfaccia SOAP, si utilizza la descrizione WSDL presente all'indirizzo:

https://<nome appliance | IP Address>/Admin/Open/SOAP/soap_2dplus_https.wsdl

L'accesso al servizio richiede un'autenticazione tramite certificato PEM completo di chiave privata; richiede inoltre che l'appliance sia stata configurata per accettare connessioni HTTPS dall'indirizzo IP dell'applicazione chiamante.

Il Web Service “**get2DPlusService**” mette a disposizione l'unica chiamata “**get2DPlus1**”.

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 11 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance αPeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

Il metodo **get2DPlus1** ha bisogno di due parametri di input:

‘b64data’ xsd:base64Binary

questa variabile dovrà contenere i dati da codificare nel timbro digitale; i dati dovranno essere prima codificati in Base64 e poi URL-encodati, per mantenere l'integrità tramite HTTPS

‘config_file’ string

questa variabile dovrà contenere il nome della configurazione cui fa riferimento il servizio (vedere paragrafo 4.2.1 e capitolo 7), e dovrà essere URL-encodata

In risposta, si otterranno due parametri di output:

‘image_res’ xsd:base64Binary

questa variabile conterrà, in caso non ci siano stati errori, l'immagine del timbro digitale 2DPlus® codificata in forma Base64. In caso di errore è posta a NULL

‘error_code’ int

codice di errore: se è 0, significa che la generazione è andata a buon fine e ‘image_res’ contiene un timbro digitale 2DPlus® valido. Altri valori:



- 1 problema nell'autenticazione del client. Contattare l'amministratore dell'appliance*
- 1 manca, o è vuota, la struttura dati di input*
- 2 errore interno*
- > 2 errore nella generazione del timbro digitale: fare riferimento al paragrafo 5.3*

5 OUTPUT DEL SERVIZIO

Le caratteristiche di quanto viene restituito dall'Appliance αPeS™, dipende dalla configurazione richiesta.

L'appliance può restituire in alternativa:

- ✓ **Image:** è il codice 2D- Plus®, all'interno del quale ci sono i dati inviati;
- ✓ **TD:** è il codice 2D- Plus®, all'interno del quale ci sono i dati firmati digitalmente;

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 12 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

- ✓ **PDF:** è il file PDF, contenente una rappresentazione del documento leggibile e stampabile, comprensiva di un **TD** (codice 2D- Plus® come timbro digitale);
- ✓ **p7m:** è la busta crittografica contenente i dati firmati digitalmente a norma legale;
- ✓ **RetCode** (viene trattato più avanti): può contenere un codice identificativo di un errore, un malfunzionamento, una incongruenza dei dati;

§

5.1 DETTAGLI SULL'OUTPUT

5.1.1 CASO IMAGE:

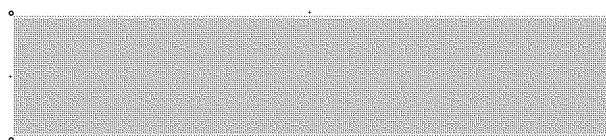
L'appliance restituirà, in caso di successo, l'immagine di un codice 2D- Plus® , strutturato in dipendenza dai parametri contenuti nella configurazione.

Il codice conterrà l'input fornito, ma di default le configurazioni gestiscono la compressione dei dati; se questa dovesse essere evitata (ad esempio l'applicazione gestisce già una compressione proprietaria), la funzione di compressione deve essere deselezionata dalla configurazione richiesta.

Il formato immagine da restituire è uno dei metadati presenti nella configurazione; attualmente sono previsti i seguenti formati:

- ✓ gif
- ✓ pbm
- ✓ png
- ✓ jpg¹
- ✓ TIFF

Esempio di codice 2D- Plus®



§



5.1.2 CASO TD:

I dati in input vengono firmati digitalmente, creando una struttura PKCS#7 a norma legale che viene poi compressa. Il tutto viene poi trasformato in un codice 2D- Plus® .

Il tutto segue quanto indicato per il *Caso Image*.

§

¹ Lo standard JPEG non consente una elaborazione "non-lossy" se non in estensioni praticamente non supportate. Tuttavia, un'immagine JPEG prodotta con la massima qualità possibile ed i giusti parametri, risulta adeguata anche per una stampa di qualità adeguata alle necessità del codice 2D- Plus® .

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 13 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

5.1.3 CASO PDF

L'appliance restituirà, in caso di successo, un file PDF (application/pdf); a sua volta contenente il timbro digitale rappresentato dal codice bidimensionale 2D- Plus®.

La generazione di un file PDF con l'inclusione del timbro digitale, prevede che la richiesta di servizio fornisca dati nel formato XML, il quale faccia riferimento ad un file XSL per la descrizione del layout finale del documento.

La generazione del file PDF verrà effettuata direttamente dall'appliance; in questo contesto e diversamente dalle altre situazioni, anche il file XSL dovrà essere disponibile ai processi presenti sull'appliance.

Il file XSL deve indicare il rettangolo di contenimento nel quale verrà inserita l'immagine del codice 2D-Plus® (timbro digitale).

NOTA: è importante che nel file XSL, il file immagine del timbro digitale che deve essere inserita nel documento finale, venga referenziata sempre con il nome ***TimbroDigitale.jpg***.

Il file XSL deve essere scritto in modo che la trasformazione XSLT, generi un file di formato FO, con il quale sarà poi possibile produrre il file PDF finale.

§

5.1.4 CASO P7M

L'appliance può restituire il file .p7m, che corrisponde ai dati firmati digitalmente ed inseriti in una busta crittografica a norma legale PKCS#7.



Quando una applicazione ha necessità di ricevere solo un file .p7m, nella configurazione a cui fa riferimento deve essere deselezionata esplicitamente la funzionalità di creazione del codice bidimensionale.

A queste condizioni l'unico output che l'appliance fornirà sarà un file nel formato PKCS#7.

Questo significa utilizzare l'appliance come apparato per la gestione di firme automatiche in remoto; quindi nulla a che fare con la generazione di un timbro digitale.

§

NOTA:

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 14 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

Ci possono essere della applicazioni, sia relative ad una richiesta di un timbro digitale (caso TD), sia relative alla richiesta di un file PDF al cui interno sia presente un timbro digitale (caso PDF), in cui esiste la necessità di gestire una conservazione di quanto firmato.

I dati firmati, cioè il pacchetto PKCS#7, sono presenti all'interno del codice 2D- Plus® (il timbro digitale) generato, ma per avere a disposizione questi dati si dovrebbe decodificare il codice stesso.

In questi casi l'applicazione dovrà effettuare due chiamate all'appliance, fornendo gli stessi dati:

1. una chiamata nella quale chiederà la creazione di un file .p7m (**Caso p7m**);
2. una chiamata nella quale richiederà un timbro digitale (**Caso TD**) ovvero un file PDF (**Caso PDF**);

La gestione delle configurazioni è realizzata operativamente dal PAdm; i dettagli relativi alle configurazioni sono trattati nei documenti:

*- **Procedure Operative Piattaforma PeS 2D-Plus®***

*- **DRT- Form di richiesta TD***

disponibili all'indirizzo http://www.secure-edge.com/Appliance_PeS/doc/

§

5.2 PARAMETRI OPZIONALI

***NOTA:** questo paragrafo non è applicabile all'interfaccia preliminare SOAP, ma solo alla chiamata diretta HTTPS.*

Oltre ai parametri obbligatori altri, tra quelli presenti nella configurazione, possono essere variati dal chiamante. Tale variazione varrà per la sola elaborazione in oggetto, mentre la configurazione nel sistema non viene sovrascritta.

Tutti i parametri sono riferiti alla immagine del codice bidimensionale 2D- Plus®:



- ✓ **Img_DPI:** Dot Per Inch; numero di punti per pollice per il quale l'immagine è stata creata;
- ✓ **PeS_image_format:** formato dell'immagine del codice;
- ✓ **PeS_IMG_MAXWmm:** larghezza massima (mm) occupata dal codice;
- ✓ **PeS_IMG_MAXHmm:** altezza massima (mm) occupata dal codice;

I valori ammessi per tali parametri sono i seguenti:

5.2.1 IMG DPI(*)

Valore numerico intero tra 50 e 1200. Indica i PPI dell'immagine da produrre.

() per ragioni storiche l'etichetta del parametro è **Img_DPI** invece di **Img_PPI**.*

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™	
	Nome del file di riferimento	
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc	
		pag. 15 di 25

Per alcuni formati grafici, quest'informazione è anche riportata nel file prodotto, altrimenti viene utilizzata esclusivamente per il calcolo delle dimensioni del timbro digitale.

NOTA1: il codice 2D- Plus® è un codice composto di piccoli simboli; una stampa di una immagine a 300PPI è consigliabile solo quando si abbia la certezza che il codice verrà stampato utilizzando una stampante laser.

In caso di utilizzo di stampante a getto d'inchiostro (inkJet) è consigliabile impostare il parametro non oltre i 200PPI.

I valori 50PPI e 100PPI sono indicati su supporti industriali plastificati, che non possono essere lavorati a densità maggiori.

I valori 600PPI e 1200PPI sono indicati, quando vengano utilizzate stampe su pellicola.

NOTA2: Differenza tra PPI e DPI

Il termine DPI (dot-per-inch) indica la risoluzione utilizzata dalla stampante per imprimere l'immagine su carta, ovvero il *passo* del retino di stampa.



E' quindi legato alla qualità di stampa: una stampante che lavori con un valore elevato di DPI avrà a disposizione una griglia di elementi ("dot") più fitta, e quindi più precisa, per rappresentare un'immagine.

Il termine PPI (pixel-per-inch) indica la densità (di stampa/visualizzazione) di un'immagine e rappresenta il numero di punti-grafici per pollice con il quale l'immagine viene stampata.

Questo significa che una immagine di 600 pixel di larghezza e 150 pixel di altezza, se venisse stampata a 300PPI, occuperebbe sul foglio di stampa 2inch di larghezza e 0,5inch di altezza; questo risultato è indifferente al numero di DPI a cui è impostata la stampante: se quest'ultima fosse impostata a 600DPI, verrebbe utilizzata una griglia di 2x2 dot per rappresentare un singolo pixel; se fosse impostata a 1200DPI la griglia utilizzata sarebbe di 4x4 dot e così via crescendo nella qualità.

Al contrario, se la stampante fosse stata impostata a 150DPI, l'immagine stampata, risulterebbe graficamente degradata (compressa), dovendo la stampante rappresentare 4 pixel (2x2) con un solo dot!

§

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 16 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

5.2.2 PES IMAGE FORMAT

Il parametro che indica il formato grafico, nel quale è configurata l'immagine del codice 2D- Plus® che viene restituita dall'appliance può avere i seguenti valori:

- 1:** indica il formato **gif**
- 2:** indica il formato **pbm**
- 7:** indica il formato **png**
- 8:** indica il formato **jpg**
- 10:** indica il formato **TIFF**

§

5.2.3 PES IMG MAXWMM E PES IMG MAXHMM

Valori numerici relativi alle dimensioni massime, espresse in mm, dell'area riservata al timbro digitale (codice 2D- Plus®) nel documento da stampare.



Viene indicata l'area riservata al codice 2D- Plus® e non la grandezza del codice, per la ragione che viene di seguito spiegata:

Il codice 2D- Plus® ha una grandezza (larghezza ed altezza) che è dipendente dalla quantità di dati da codificare.

Tuttavia, anche a parità di tipo documento da stampare, di volta in volta potrebbero essere generati codici 2D- Plus® di dimensioni diverse; ad esempio, un cedolino stipendio, potrebbe essere costituito da una sola pagina per un dipendente e costituito da tre pagine per un dipendente diverso; il codice 2D- Plus® risultante sarebbe di dimensioni quindi diverse e la stampa dei due cedolini, risulterebbe graficamente non omogenea.

La configurazione disponibile nell'appliance e dichiarata nel comando inviato a quest'ultimo, prevede due casi in modo da poter ovviare a questo fatto:

- a) il codice 2D- Plus® viene generato senza elaborazioni speciali; la sua grandezza è quindi semplicemente proporzionale ai dati che contiene; la sua immagine, se più piccola dell'area riservata, si posiziona al centro di questa;
- b) al codice 2D- Plus® si aggiunge un "riempimento" (filling) tale che la sua grandezza finale, risulterà sempre essere equivalente all'area riservata, che quindi riempirà completamente; questo renderà l'aspetto esteriore di tutti i codici 2D- Plus® generati, uguale;



 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 17 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

Il timbro digitale necessita di un numero minimo di pixel in verticale e in orizzontale; si faccia attenzione al fatto che il valore minimo ammesso per PeS_IMG_MAXWmm e PeS_IMG_MAXHmm è dipendente dal valore Img_DPI.

Nel caso $Img_DPI = 300$, i valori minimi da rispettare sono:

- ☞ PeS_IMG_MAXW = 35 mm
- ☞ PeS_IMG_MAXH = 4 mm

§

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 18 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance αPeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

5.3 RETCODE

Nel caso che l'appliance riscontrasse qualche problema, è possibile che la risposta consista di un un testo (MIME type text/txt) contenente un codice d'errore numerico.

Nota: il valore dei codici d'errore può variare nel tempo; la presente tabella potrebbe non essere aggiornata in tutte le sue parti.



Appendice A: Errori restituiti dal gateway Paper e-Sign (main)

range 10100 - 10500

- 10101: errore CGI (problema con metodi POST/GET?)
- 10103: sono presenti sia i parametri "data" che "infile"
- 10104: impossibile leggere il file con i dati
- 10105: manca il parametro "data" missing (eventualmente anche "infile")
- 10125: manca il parametro "passwd"
- 10126: il parametro "passwd" e' errato
- 10130: manca il parametro "cfg"
- 10131: il contenuto del parametro "data" e' troppo lungo
- 10132: il parametro "data" e' vuoto
- 10134: impossibile leggere la configurazione PeS
- 10135: configurazione PeS incongruente / illeggibile /incompleta
- 10142: errore di sintassi in un parametro (in sovrascrittura)
- 10150: modo "a riga di comando" non supportato
- 10151: errore nei parametri (modalita' "a riga di comando")
- 10201: impossibile determinare il profilo del chiamante (certificato SSL assente? Sconosciuto?)
- 10202: il chiamante cerca di accedere ad una risorsa che non gli appartiene
- 10220: errore nel processamento dei dati
- 1030x: errore nel (post-)processamento PDF
- 10302: impossibile acquisire la configurazione XSL
- 10303: impossibile scrivere un file temporaneo necessario all'elaborazione PDF
- 10305: errore nel processamento PDF
- 10350: impossibile scrivere/copiare il PDF finale su disco/su stdout
- 10400: errore nel numero di parametri a riga di comando

Appendice B: Errori SOAP server

Nota: fino alla versione 20091123, la sezione SOAP restituiva codici numerici molto bassi e non intercettava gli errori del "core"

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance αPeS™	
	Nome del file di riferimento	
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc	
		pag. 19 di 25

range 20000 - 25000

- 20010: (ex 10) nella struttura SOAP, manca cfg o data
- 20011: cfg e/o data e' vuoto
- 20012: (ex 15?) impossibile stabilire ID del profilo del chiamante
- 20013: (ex 15?) il client non ha presentato un certificato
- 20015: (ex 15) il profilo non ha il permesso di accedere alla configurazione
- 20025: (ex 25) errore generico nel gateway (il server SOAP non trova il timbro digitale dopo l'elaborazione)
- 20030: (ex 20) impossibile scrivere un file di input temporaneo per il gateway

Appendice C: Errori PeS core

range 300000 – 500000

- 310000-319999: configurazione
- 320000-329999: verifiche
- 350000-359999: acquisizione dati
- 360000-369999: elaborazione fingerprint
- 370000-379999: firma
- 380000-389999: compressione part / pre-barcode
 - 381000 +/- 10: OBSOLETO: parte 2D Plus barcode
- 390000-395999: generazione barcode
 - 393000 - 393128 OBSOLETO: parte 2D Plus barcode
- 396000-499999: finale

- 300001: (puo' essere un errore interno) il core ha ricevuto un parametro nullo / manca un parametro
- 310100: (puo' essere un errore interno) configurazione nulla/assente

- 310121: tipo di barcode non supportato
- 310126: impossibile eseguire la conversione al formato immagine richiesto



- 310150: errore nella computazione della lunghezza del PeS header (al 2010, si applica soltanto al PDF417)
- 310152: errore nella computazione del PeS header (al 2010, si applica soltanto al PDF417)

- 310180: errore nella configurazione di accounting
- 310181: errore di accounting (esauriti i timbri a disposizione?)

- 320200: errore nella password (per configurazione con PIN/pass check)

- 350200: errore nella decodifica in Base64
- 3503XX: (puo' essere un errore interno) errore nel data processing

- 360175: impossibile produrre il fingerprint del certificato di firma

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 20 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

370100: errore (di configurazione) sulla composizione del contenuto da firmare

370185: impossibile creare il file col contenuto da firmare

370195: impossibile leggere il file con la firma

370197: errore nel formato della firma

370200: la firma non e' della lunghezza attesa(?!)

370300: supporto LunaSA non disponibile

370302: supporto OpenSSL non disponibile

370400: fallimento della firma, oppure la configurazione non ha un meccanismo di firma assegnato

370401: errore di configurazione nei parametri di firma

370403: impossibile eseguire il parse del file con il certificato di firma

370405: e' sorto un problema nel setup del meccanismo di firma

370500: sistema di firma non supportato / errato

370600: overload del meccanismo di firma

380105: errore nella configurazione (parametro signature_use)

380200: errore nella compressione

380205: impossibile allocare memoria per la compressione

380300: tipo di compressione errato/non supportato

389010: errore nell'assemblaggio del contenuto del barcode

389050: errore nell'output dei dati del barcode

ATTENZIONE! POSSIBILI ERRORI NEL RANGE D'ERRORE

381xxx: errore nella creazione del barcode

381010: in genere, significa che le dimensioni del timbro (dell'immagine) sono insufficienti per contenere i dati

390100: impossibile allocare memoria durante l'assemblaggio

390150: impossibile determinare un formato immagine temporaneo. Probabile errore nel mix di opzioni della configurazione PeS

390190: errore nella validazione del PDF417

390200: 2D-Plus: errore durante la generazione del codice a correzione d'errore



390290: il formato temporaneo dell'immagine e' inadatto al tipo di barcode

390300: tipo di barcode sconosciuto o non supportato

393065: (2DPlus barcode) array del bytestream nullo

393066: (2DPlus barcode) array di output nullo

393067: (2DPlus barcode) parametri errati passati al modulo 2D Plus

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 21 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

393068: (2DPlus barcode) spazio insufficiente per il contenuto: bisogna aumentare la dimensione del timbro

393069: (2DPlus barcode) errore durante il fill dell'header

393010: (2DPlus barcode) problema nel calcolo del padding "estetico"

393011: (2DPlus barcode) problema di allocazione memoria array simboli (memoria esaurita?!)

393012: (2DPlus barcode) problema nella segmentazione del file per "alfabeto 39"

393013: (2DPlus barcode) problema codifica ECC

393014: (2DPlus barcode) problema malloc array dati con ECC

396105: impossibile eseguire il dump da memoria al file dell'immagine (era: 397005-397009, forse fuori range)

397001: errore di conversione a immagine nel formato dato (post-barcode)

397002: impossibile generare JPEG

397003: errore (intermo) nella generazione del JPEG

397009: impossibile/non permesso convertire nel formato immagine previsto

397005-397009: (obsoleto, forse fuori range) impossibile eseguire il dump da memoria al file dell'immagine

397010: errore in accounting

397009: conversione a formato immagine non supportato

397020: comando esterno di conversione dell'immagine non trovato

397030: errore interno: impossibile trovare tipo di locazione immagine (mix di parametri della configurazione non supportato?)



398xxx: errore interno nello spostamento dei dati da memoria a file

398080: tipo di locazione immagine errato

398110: impossibile trasferire dati da file a memoria

499990: impossibile aprire il file (con l'immagine) per il MIME-output

§

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 22 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

6 CARATTERISTICHE DELLE IMMAGINI E DEI LORO FORMATI

Le applicazioni che fanno richiesta di timbri digitali all'appliance, si vedranno restituire un'immagine, nel formato desiderato, che deve essere inserita in un documento.

Probabilmente il documento stesso dovrà essere stampato con un aspetto grafico prevedibile e coerente con le specifiche richieste all'applicazione.

A tal fine, è utile leggere con attenzione quanto segue.

In generale, le applicazioni trattano la rappresentazione delle immagini in maniera molto differente e questa dipende anche dalle informazioni che l'immagine stessa mette a disposizione; inoltre, una stessa applicazione può comportarsi in modo differente a seconda della periferica di output.

Al riguardo, esemplari sono i browser, i quali in genere ignorano le informazioni sulla densità dell'immagine e la rappresentano secondo una densità fissa (72 PPI, la tipica densità degli schermi) oppure dipendente dalle esigenze di contenimento della pagina web.

Spesso si comportano in maniera differente al momento della stampa su carta, anche se quest'ultimo aspetto, diventa in genere trascurabile se la pagina web è realizzata in maniera tale da essere facilmente stampabile sul tipico foglio A4.

I prodotti pensati per generare documenti PDF, invece, procedono secondo canoni diversi.

Il documento PDF è per sua natura pensato per essere stampato coerentemente, quindi la rappresentazione a video è sempre rappresentativa del risultato su carta se:

- ☞ il documento è stato realizzato riportando le corrette dimensioni per i vari elementi
- ☞ la procedura di stampa impone il rispetto delle misure così come sono (devono essere quindi disabilitate funzioni del tipo "adatta alla pagina");

bisogna tuttavia osservare che il modo di impostare la dimensione di un'immagine nel file PDF varia a seconda del software utilizzato per lo sviluppo.

L'applicazione ideale è un'applicazione che, ricevuto il timbro digitale con le relative informazioni sulla densità di stampa nel file stesso, produce o mostra un documento secondo tali informazioni.



Per quanto visto, la maggior parte delle applicazioni non utilizzano le informazioni sulla densità di stampa delle immagini; in ogni caso, l'appliance inserisce questa informazioni nei formati che la supportano, ovvero il JPEG e il TIFF.

Si vuole anche osservare che le densità di stampa da preferirsi sono:

- ☞ 300 ppi, per stampanti laser
- ☞ 150 ppi, per stampanti a getto d'inchiostro o quando non si conosce la natura delle periferiche di stampa

In genere, il programmatore procederà secondo i seguenti passaggi:

1. determinare la dimensione del timbro sulla base delle proprie esigenze grafiche

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 23 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

2. richiedere all'appliance un timbro digitale che occupa al massimo o esattamente lo spazio desiderato
3. manipolare la rappresentazione dell'immagine per i propri scopi

Per quanto riguarda il punto (2), si suggerisce di utilizzare sempre una configurazione che restituisce un'immagine esattamente della dimensione desiderata; in tal modo si potrà utilizzarla in uno spazio predisposto sempre allo stesso modo, senza dover prima verificarne l'effettiva lunghezza e larghezza.

Se l'immagine viene inserita in una pagina HTML, bisogna tenere presente una serie di fatti:

- ♦ i browser suppongono che la giusta rappresentazione di un'immagine, per la quale non è nota la densità di stampa, sia di 72 PPI. Se anche l'informazione c'è, essa viene in genere ignorata
- ♦ dal punto di vista delle dimensioni, quello che i browser mostrano a video ha spesso poco a che fare con la stampa della medesima pagina; molti browser tendono a rappresentare la pagina sul video in modo da farla entrare nello spazio a disposizione e a fare aggiustamenti di tipo diverso in fase di stampa
- ♦ il modo migliore per controllare l'aspetto delle pagine sul video e in stampa è quello di utilizzare i fogli di stile; bisogna però fare attenzione alle diverse esigenze del monitor e della stampante e dell'incompatibilità nella gestione dei CSS tra diversi browser

Un modo per ottenere la giusta resa con i browser più comuni è quello di utilizzare l'attributo "width" del tag "src".

Se la larghezza di un timbro è di L pixel, volendo rappresentarlo a 300 ppi (e noto che il browser assume una risoluzione della periferica di 72 ppi), si ottenga il valore:

$$R = L * 72 / 300$$



e lo si utilizzi in questo modo:

```

```

Ovvero, si è costretto il browser a "restringere" l'immagine di un fattore 300/72.

§

 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 24 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

7 PIATTAFORMA DI TEST ED ESEMPI D'USO

Secure Edge mette a disposizione una piattaforma di test, costituita da un appliance α PeS™, disponibile via Internet.

L'accesso alla piattaforma deve anticipatamente, essere concordato con Secure Edge.

L'appliance di test (risponde all'indirizzo "pes.secure-edge.com"),

Come già indicato nel capitolo del protocollo applicativo (4.2), è possibile richiedere all'appliance la creazione di un timbro digitale con i seguenti parametri

cfg configurazione da utilizzare
data stringa di dati, realizzata effettuando **prima una codifica in Base64 e poi una codifica URLEncoding.**

Sono state definite 5 configurazioni di test:

- **cfg.demo2** dati in forma XML (con verifica integrità XSL referenziato)
- **cfg.txt2** dati in forma di testo
- **cfg.xmlxsl2** dati in forma XML (con verifica integrità XSL referenziato)
- **cfg.rtf2** dati in forma rtf
- **cfg.p7d2** dati binari; restituisce un file p7m

NOTA: i nomi sono case-sensitive.

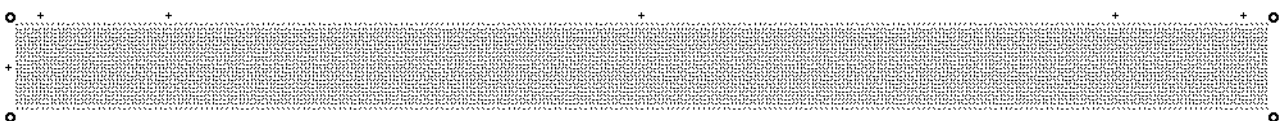
Ad esempio, la configurazione "cfg.demo2" ha definito al suo interno una serie di caratteristiche dell'immagine che viene restituita: un'immagine TIFF (MIME type image/tiff) con densità di 300 PPI, larghezza 85mm e altezza variabile (in base alla quantità di dati da codificare): l'immagine rappresenta il timbro 2DPlus™; tutte queste caratteristiche sono presenti nella configurazione **cfg.txt2**.



Come già indicato nel capitolo dei parametri opzionali (5.2), è possibile fornire nella chiamata valori diversi di alcuni parametri; questi nuovi valori saranno presi in considerazione dal swCore dell'appliance solo per l'invocazione corrente.

In caso di errore, viene restituito un testo (MIME type text/txt) contenente un codice d'errore numerico.

Quindi un esempio di URI correttamente funzionante è:

[http://pes.secure-edge.com/cgi-bin/gateway?
cfg=cfg.txt2&PeS_image_format=8&data=UGlwcG8gcGlwcGVybwo=](http://pes.secure-edge.com/cgi-bin/gateway?cfg=cfg.txt2&PeS_image_format=8&data=UGlwcG8gcGlwcGVybwo=)
che restituisce questa immagine jpg (PeS_image_format=8) da 150PPI e 169mmx15mm:

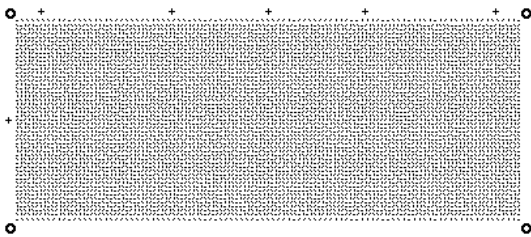


 SECURE EDGE <small>your safety .net</small>	Descrizione commessa	pag. 25 di 25	 SECURE EDGE <small>your safety .net</small>
	Realizzazione Appliance α PeS™		
	Nome del file di riferimento		
	[SE_T-07-0049] T I DST Usage from applications [3.5].doc		

Un'altra possibilità, usando gli stessi dati è:

http://pes.secure-edge.com/cgi-bin/gateway?cfg=cfg.txt2&PeS_IMG_MAXHmm=30&PeS_IMG_MAXWmm=69&data=UGlwcG8gcGlwcGVybwo=

che restituisce questa immagine gif (default della configurazione cfg.txt) di larghezza ed altezza minimi, a 150dpi.



NOTA: un file gif non ha memoria della risoluzione adottata; se si utilizza un file gif, bisogna sapere come è stato creato, cioè a quale risoluzione, in modo da gestirlo in modo corretto.

Il passaggio dei parametri può avvenire indifferentemente con metodo POST o GET.

§

8 FORMATO DATI DA INVIARE ALL'APPLIANCE

L'appliance tratta i dati in modo (quasi) completamente trasparente; all'opposto è invece il comportamento del software Decoder 2D-Plus, il quale, capace di interpretare il tipo di dato inserito nel codice 2D-Plus, permette di sfruttare appieno i formati standard;

La trattazione dei formati dati è per questa ragione piuttosto estesa, ed è presente nel documento:

[SE_T-07-0054] DST useful data structures [1.0].doc

