App IOS *InfoCert Dike*
Manuale Utente

Indice

1 Introduzione

InfoCert, leader italiano per la firma digitale, è titolare del rivoluzionario servizio di "firma remota" che consente ad un utente la firma digitale di documenti elettronici senza l'ausilio di smartcard fisiche ma utilizzando, tramite la rete Internet, un certificato di firma digitale rilasciato dalla Certification Authority InfoCert su Hardware Secure Module. La rivoluzionaria tecnologia di firma remota è già largamente utilizzata dagli utenti delle principali piattaforme desktop tramite il noto software gratuito di firma denominato Dike. La presente App è la versione per iPhone ed iPad di Dike per desktop.

Grazie alla tecnologia di firma digitale remota messa a disposizione da InfoCert ed aderente alla normativa vigente in Italia, ora anche i possessori di iPhone e iPad possono firmare documenti elettronici in mobilità. Questa App consente infatti la firma dei documenti ricevuti via email nei formati CAdES (.P7M) e PAdES (.PDF) ed inoltre permette di marcare temporalmente i file nei formati CAdES-T (.P7M) e PAdES-T (.PDF) utilizzando il servizio di marcatura temporale messo a disposizione da InfoCert e conforme alle direttive presenti nella deliberazione CNIPA/45 del 2009 (RFC3161).

Grazie al protocollo OCSP ed all'integrazione dei certificati digitali di tutte le CA accreditate in Italia per la firma digitale, questa App è in grado di verificare la validità dei documenti firmati ricevuti via email fornendo una dettagliata analisi della firma, del certificato digitale del firmatario (via OCSP) e del certificato della Timestamping Autority che ha marcato il documento/firma.

1.1 Scopo del documento

Il seguente documento rappresenta una guida rapida per l'utilizzo dell'App per iOS denominata *InfoCert Dike.*

Nel corso del Capitolo verrà fornito l' elenco delle funzionalità dell'App descritte nel presente manuale. Nel Cap. 2 verranno descritte le principali schermate e la configurazione globale dell'App ed il meccanismo di importazione ed esportazione di documenti plain e di documenti firmati e marcati attraverso il meccanismo “Apri con...” del client di posta nativo di iOS e tramite iTunes. Il Cap. 3 fornirà una descrizione di parametri di configurazione dell'applicazione mentre i Cap. 4 e 5 illustreranno le procedure di firma e verifica per i file. Il documento termina con il Cap. 6 che fornisce una descrizione del processo di estrazione del documento plain dalle buste crittografiche.

1.2 Funzionalità dell'App

Le principali funzionalità dell'App sono riassunte nel seguente elenco:

- Firma/Verifica CAdES, CAdES-T
- Firma/Verifica PAdES, PAdES-T
- Controfirma firma CAdES o CAdES-T
- Aggiunta firma CAdES, CAdES-T a file firmato CAdES o CAdES-T
- Aggiunta firma PAdES o PAdES-T a file firmato PAdES o PAdES-T

- Marca sulla firma CAdES (CAdES-to-CAdES-T)
- Marca su file firmato (*.TSD - RFC5544)
- Verifica marche su firme, file TSD e file M7M (Dike MIME-embedded file format)
- Estrazione documento originale da file firmati CAdES o CAdES-T
- Estrazione documento firmato da file marcati TSD o M7M
- Visualizzazione certificati digitali X.509 (dettagli) e verifica online OCSP
- Invio/importazione documenti via Mail
- Richiesta OTP via SMS

2 Per cominciare...

Le principali schermate dell'App mostrano vari elenchi di file, suddivisi in due principali categorie, più una schermata per la configurazione dell'App e le informazioni sulla versione:

1. **Firma digitale**. Documenti importati nell'App o estratti da buste crittografiche
2. **Archivio**. Documenti lavorati dall'App (firmati e/o marcati) e report generati dalla verifica di file crittografici.
3. **Impostazioni**. Configurazione dei parametri per la firma e per la marca e lista dei certificati dei certificatori che rilasciano certificati per la firma digitale.

2.1 Schermate

Di seguito una panoramica delle principali schermate dell'applicazione.

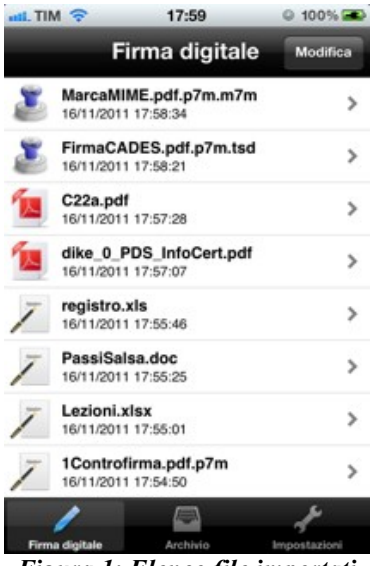

Figura 1: Elenco file importati

E' la prima schermata ad apparire al caricamento dell'App.

Mostra:

- Documenti crittografici o plain importati nell'App tramite la funzione “Apri con...” (vedi Par. 2.2)
- Documenti crittografici o plain risultanti dall'operazione di estrazione da documenti crittografici (vedi Cap. 4)

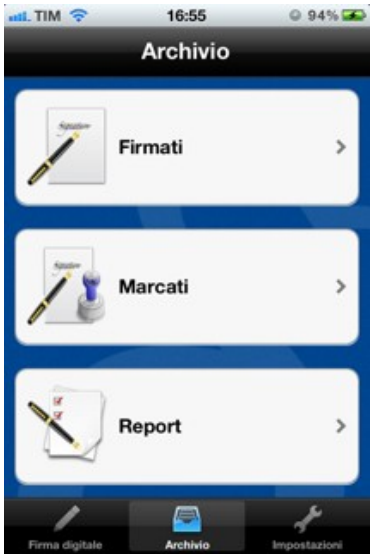

Figura 2: Archivio dei documenti lavorati dall'App

Con riferimento al tasto premuto si accede al rispettivo elenco dei file:

Firmati. File è cui è stata applicata una firma digitale secondo i formati CAdES, CAdES-T, PAdES e PAdES-T (*.P7M, *.PDF).

Marcati. File firmati CAdES o CAdES-T a cui è stata applicata una marca temporale secondo lo standard definito da *RFC5544* (*.TSD).

Report. File di Report generati dalla verifica di firme e marche sui file.

Figura 3: Accesso ai parametri di configurazione

Schermata di accesso a:

Certificati. Lista dei certificati dei certificatori che rilasciano certificati per la firma digitale

Firma PDF. Scelta tra la modalità di firma CAdES o PAdES per i file PDF.

Firma remota. Parametri di configurazione della firma remota e richiesta di OTP via SMS.

Marca temporale. Parametri di configurazione per il servizio di marca temporale e richiesta di disponibilità marche.

"i". Schermata di visualizzazione delle informazioni sulla versione dell'App.

2.2 Importare un documento nell' App

Alla versione attuale l'App permette di importare i seguenti formati di file plain e crittografici.

Plain

- PDF (*.PDF)
- Microsoft Word (*.doc, *.docx)
- Microsoft Excel (*.xls, *.xlsx)

- Microsoft Powerpoint (*.ppt, *.pptx)
- Rich Text Format (*.rtf)

Crittografici:

- Documento firmati digitalmente (*.P7M)
- Timestampeddata (RFC5544) – Marca temporale + documento firmato (*.TSD)
- Marca temporale + documento firmato in formato MIME (*.M7M)

Per importare un formato di file supportato è sufficiente utilizzare un'applicazione per iOS che supporti il meccanismo “Apri con...”. Il tipico esempio è costituito dal client di posta elettronica preinstallato in iPhone ed iPad.

Come mostrato in Figura è sufficiente toccare l'icona del file allegato al messaggio di posta per far apparire un menù contestuale che permette di aprire (importare) il file selezionato con l'App.

Figura 4: Esempio di importazione di un file da un messaggio email

Nota

È possibile importare un file nell'App tramite qualsiasi App per iOS che gestisca i file supportati di Infocert Dike. Ad esempio anche tramite il browser web Safari è possibile cliccare sul link di un file ed importarlo direttamente. Un altro tool molto noto è il servizio di condivisione *Dropbox* che permette l'apertura dei file condivisi con Infocert Dike.

2.3 Visualizzazione ed azioni sui file

Ogni qualvolta viene selezionato un file in uno degli elenchi descritto nel Par. 2.1 l'App esegue una operazione predefinita che dipende dal tipo di file. I tipi di operazione predefinita possono essere riassunti sostanzialmente in due categorie:

- **Visualizzazione**. Operazione predefinita per i file plain. Il file viene visualizzato utilizzando la componente browser del SO.
- **Verifica**. Operazione predefinita per i file crittografici. Viene avviato il meccanismo di verifica del file crittografico e viene mostrato l'esito della verifica.

Sia che sia stata eseguita una visualizzazione che una verifica, nell'angolo in alto a destra della schermata risultante viene mostrato il tasto “Azioni” che permette di mostrare l'elenco delle operazioni possibili su quel determinato file. Le Figure seguenti mostrano l'elenco delle operazioni possibili per un documento PDF, un file firmato (P7M) ed un file marcato (TSD).

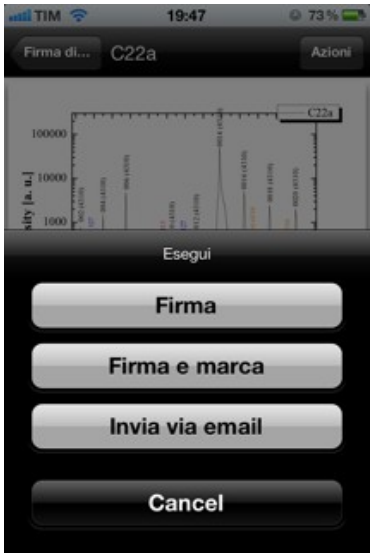

Figura 5: Elenco delle azioni possibili su un file PDF

Figura 6: Elenco delle azioni possibili su un file firmato (P7M)

Figura 7: Elenco delle azioni possibili su un file marcato (TSD o M7M)

Come si può notare, l'elenco delle operazioni possibili dipende dal tipo di file. Si rimanda ai Cap. 4 e 5 per una descrizione dettagliata delle varie azioni possibili su file plain e non.

Nota

Per ogni file è sempre presente l'azione “Invia via email” che permette di comporre un messaggio di posta elettronica allegando il file in questione.

2.4 Operazioni di base su file ed elenchi di file

Ordinamento

Gli elenchi di file accessibili tramite le schermate “Firma digitale” e “Archivio” hanno la caratteristica comune di ordinare di default i file rispetto alla **data** di ultima modifica (dal più recente al meno recente). È comunque possibile ordinare i file in ordine **alfabetico** rispetto al nome (a-z) premendo sul bottone “Modifica” in alto a destra e successivamente premendo sul bottone “Ordina”.

Cancellazione

Agendo sul tasto “Modifica” è possibile abilitare il meccanismo tipico delle applicazioni per iOS per la cancellazione dei file.

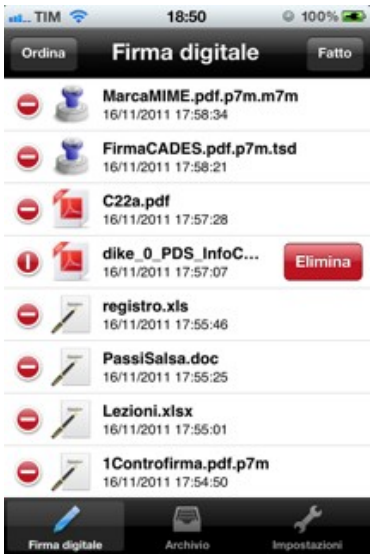

Figura 8: Esempio di cancellazione di un file

Rinominare i file

Applicando una pressione prolungata sul nome di un file viene mostrato un menù contestuale che permette di rinominare un file come mostrato nelle seguenti Figure.

Figura 9: Accesso alla funzione per rinominare un file

Figura 10: schermata per la digitazione del nuovo nome per il file

Note

- Per la schermata che mostra l'elenco dei certificati digitali delle CA non è permesso cambiare l'ordinamento o eliminare/rinominare alcun certificato.
- Non è consentito lo spostamento dei file.

3 Configurazione

Nel corso del presente Capitolo verranno illustrati i parametri di configurazione dell'App. Per accedere alla configurazione dell'App è sufficiente selezionare il tasto “Impostazioni” presente nella barra sottostante.

Per il rilascio dei certificati di firma e quindi per l'abilitazione al servizio di Firma Remota, la normativa italiana impone il riconoscimento "de visu" dell'utente al quale il certificato viene rilasciato, impone inoltre che l'utente sottoscriva un contratto cartaceo col certificatore ed in presenza di una persona incaricata dal certificatore. Questo impedisce, di fatto, la possibilità di acquisire il servizio via web.

3.1 Formato firma per documento PDF

Figura 11: Selezione della modalità di firma CAdES o PAdES per i file PDF

Impostando il selettore a **"I"** l'App viene configurata in modo da firmare i documenti PDF sempre in formato PAdES.

Impostando il selettore a **"O"** il file PDF vengono firmati in modalità CAdES come tutti gli altri tipi di file (ossia tramite la generazione di una busta crittografica PKCS#7 - *.P7M).

3.2 Parametri per la firma remota

Figura 12: Configurazione delle credenziali per la firma

La schermata di configurazione della firma remota permette di salvare la username associata al servizio di firma remota di InfoCert (in modo da non dovera ridigitare al momento della firma). Inoltre consente di:

Visualizzare i dettagli del certificato digitale associato alla username inserita.

Richiedere l'invio di un OTP (per la firma) sulla numerazione mobile selezionata dall'utente in fase di sottoscrizione al servizio di firma remota.

Nota

Username e password di firma sono differenti da username e password di marca.

3.3 Parametri per la marca

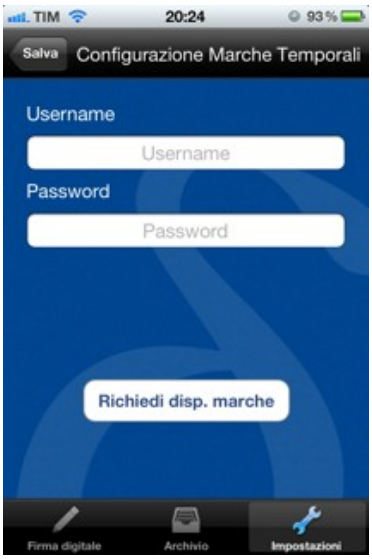

Figura 13: Configurazione delle credenziali per il servizio di marca temporale

La schermata relativa alla configurazione delle marche temporali permette di inserire e salvare le credenziali per il servizio di marca temporale messo a disposizione da InfoCert. Inoltre permette di controllare la disponibilità residua di marche temporali associare all'account.

Nota

Username e password di firma sono differenti da username e password di marca.

4 Firmare e marcare un documento

L'App applica firme digitali conforme alle direttive della Legge Italiana a documenti elettronici.

Il processo di firma coinvolge complessivamente l'uso di 4 parametri: username+password, un PIN di Firma ed un OTP.

- username+password sono necessari per ricevere l'OTP via SMS su una numerazione scelta dall'utente
- username+PIN+OTP abilitano il processo di Firma

Opzionalmente è possibile applicare una marca temporale (timestamp) alla firma o ad un documento firmato (P7M). Per utilizzare la timestamp authority di InfoCERT sono necessari una username ed una password per la marca che differiscono da quelli per la firma e devono essere acquistati a parte.

Nota

È possibile ottenere l'OTP anche in una seconda forma ossia tramite l'acquisto di una licenza per l'App denominata Vasco Digipass già disponibile gratis nello store di iTunes.

La seguente tabella mostra le tipologie possibili di operazioni firma digitale e marca applicabili ai documenti gestiti dall'App. Per ogni tipologia di firma viene data una descrizione, l'elenco dei formati di file su cui è possibile eseguire l'operazione, il formato di output, le credenziali necessarie.

Operazione	Descrizione	File input	File output	Credenziali necessarie F=Firma M=Marca
Firma CAdES	Applica la firma digitale ad un file generico producendo un PKCS#7 in formato CAdES	*	P7M	F
Firma CAdES-T	Come la Firma CAdES con l' utilizzo della TSA di InfoCert per applicare una marca temporale alla firma generata	*	P7M	F,M
Firma PAdES	Firma un documento PDF in formato PAdES ossia un nuovo PDF copia dell'originale con la firma digitale all'interno **Nota**: Viene firmato l'intero documento PDF incluse le eventuali firme PadES/PAdES-T già presenti all'interno del file	PDF	PDF	F
Firma PAdES-T	Come la Firma PAdES con l' utilizzo della TSA di InfoCert per applicare una marca temporale alla firma generata	PDF	PDF	F,M
Aggiunta firma CAdES	Dato un documento già firmato in modalità CAdES aggiunge una ulteriore firma CAdES al documento **Nota**: Non è una operazione di firma sulle firme già presenti ma viene aggiunta una nuova firma sul dato	P7M	P7M	F
Aggiunta firma CAdES-T	Come “Aggiunta firma CAdES” con l' utilizzo della TSA di InfoCert per applicare una marca temporale alla firma	P7M	P7M	F,M
Controfirma	Applica una controfirma su una specifica firma CAdDES o CAdES-T già presente	P7M	P7M	F

Marca su firma	Applica una marca temporale ad una specifica firma CAdES già presente. In altre parole, trasforma una firma CAdES già applicata in formato CAdES-T	P7M	P7M	M
Marca su file firmato	Applica una marca temporale su un generico file firmato CAdES o CAdES-T	P7M	TSD	M

Tabella 1: Riassunto delle principali operazioni crittografiche previste dall'App. Nome, descrizione, tipo di file in input ed output e credenziali necessarie

4.1 Credenziali

L'App utilizza una sola schermata per l'inserimento delle credenziali necessarie all'operazione crittografica (Vedi Par. 4.2, 4.3, 4.4 e 4.5). La schermata è auto esplicativa e visualizza:

- Operazione crittografica che si sta per eseguire
- Il nome del file in input
- Il nome del file in output
- Campi per l'inserimento delle credenziali di firma e di marca

Inoltre sono presenti anche il campo “password” necessario per la richiesta dell' OTP ed il bottone per la visualizzazione delle marche disponibili.

Nota

L'attuale versione dell'App produce esclusivamente firme e marche in formato *attached.*

Le operazioni di firma e/o marca che cambiano formatto al file aggiungono l'estensione necessaria al nome di file originario.

Indipendentemente dalla cartella di origine del file (“Firma digitale” o sottocartelle di “Archivio”) i file lavorato dall'App vengono salvati nella relativa sottocartella di “Archivio”.

L'App non sovrascrive mai alcun file, se il nome di file destinazione esiste già, allora automaticamente viene apposto al nome del file un prefisso numerico progressivo.

4.2 Esempio 1: Firma CAdES

Figura 14: Inserimento delle credenziali necessarie alla operazione crittografica selezionata

Figura 15: Esito dell'operazione

Note

- Al file viene aggiunta l'estensione P7M
- Il campi per l'inserimento delle credenziali per la marca sono disabilitati

4.3 Esempio 2: Firma PAdES-T

Figura 16: Esempio di inserimento di credenziali per una firma PAdES-T

Figura 17: Esito dell'operazione

Note

- Per le firme PAdES, l'App aggiunge il prefisso *PDS_* al nome del file
- E' opportuno verificare la correttezza delle credenziali per la marca utilizzando il tasto per la verifica della disponibilità delle marche. Se il processo di firma con marca fallisce nell'applicazione della marca l'OTP per la firma viene comunque consumato.

4.4 Esempio 3: Controfirma

Figura 18: Esempio di selezione dell'operazione di controfirma su una firma esistente

Figura 19: Credenziali necessarie alla controfirma

Note

- La controfirma si applica su una firma specifica dopo il processo di validazione della firma e per sua natura non necessita delle credenziali di marca
- Il file di output è già presente in Archivio e l'App quindi seleziona automaticamente un nuovo nome di file

4.5 Esempio 4: Marca su file

Figura 20: Esempio di inserimento credenziali per la marca su file

Figura 21: Risultato dell'operazione di marca su file

Note

- Sono necessarie solo le credenziali per la marca
- Viene apposta l'estensione TSD al nome del file

5 Verificare firma e marca su un documento

L'operazione di verifica di un file e avviata automaticamente una volta selezionato un file crittografico. **L'operazione richiede necessariamente la connessione del device a Internet in quanto com parte integrante della verifica delle firme è inclusa la verifica OCSP del certificato dell'utente firmatario**.

Data la mole di dettagli relativi ad una firma digitale e gli ulteriori dettagli relativi al certificato digitale del firmatario e delle CA, la visualizzazione di una firma e/o marca verificata con successo avviene mostrando prima una anteprima dei dettagli della firma ed eventualmente si può accedere ad ulteriori dettagli ed alla visualizzazione completa del certificato digitale.

Dopo ogni esecuzione di verifica, l'App crea automaticamente un **report in formato PDF** che è possibile visualizzare ed esportare dalla schermata di “Archivio”

5.1 Verifica firme CAdES e CAdES-T

Figura 22: Anteprima dei dettagli di una firma CAdES con una controfirma

Figura 23: Anteprima dei dettagli di una firma CAdES-T

Note

- Le due Figure mostrano la verifica di un file PDF con due firme apposte (una CAdES ed una CAdES-T)
- La firma CAdES ha una controfirma e riporta che la data e l'ora della firma provengono dal device che ha firmato (PC)
- La firma CAdES-T invece riporta che la data e l'ora della firma sono state apposte da una TSA di cui nell'anteprima viene riportato il *common name* del certificato

Agendo sul bottone “Più dettagli” è possibile visualizzare i dettagli aggiuntivi su firma, controfirme e marche ed accedere ai dettagli sui certificati

Figura 24: Sezione di dettagli di una firma CAdES-T

Figura 25: Sezione dei dettagli di una marca su firma CAdES

Figura 26: Sezione dei dettagli sulla controfirma di una firma esistente

Note

- Le tre immagini mostrano una sezione dei dettagli della firma CAdES-T e della relativa marca ed i dettagli del controfirmatario della firma CAdES
- Agendo sul bottone "Certificato" è possibile accedere a due schermate relative ai dettagli sul certificato

Figura 27: Anteprima dei dettagli di una certificato digitale

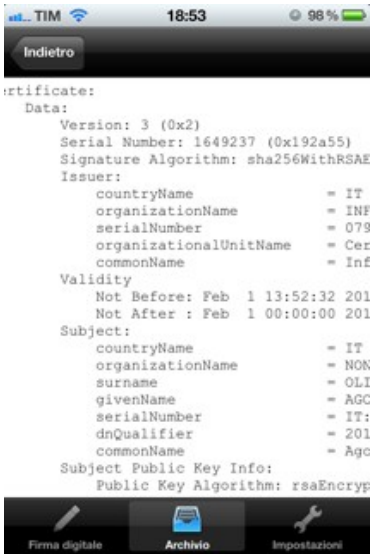

Figura 28: Visualizzazione di tutti i dettagli di un certificato

Note

- La prima visualizzazione mostra un elenco dei principali dettagli di un certificato digitale
- La seconda immagine mostra tutti i dettagli in stile OpenSSL

5.2 Verifica firme PAdES e PAdES-T

Ogni qualvolta l'App visualizza un documento PDF, in automatico viene verificato se sono presenti firme PAdES all'interno del file. Se viene riconosciuta la presenza di una firma, l'App mostra nell'angolo in alto a destra una icona a forma di penna. Agendo sull'icona è possibile procedere alla visualizzazione dell'elenco delle firme presenti ed alla verifica.

Figura 29: Segnalazione di una firma PAdES presente nel documento PDF con l'icona di una penna

Figura 30: Visualizzazione dell'elenco delle fime PAdES o PAdES-T presenti nel documento

Figura 31: Visualizzazione anteprima e dettagli di una firma PAdES-T

Note

- La prima figura mostra il PDF con l'immagine della penna
- Agendo sulla penna vengono visualizzate le firme presenti
- Selezionando la firma si procede alla verifica ed alla visualizzazione dei dettagli

5.3 Verifica PDF con firme PAdES e CAdES

È possibile che un file PDF firmato PAdES sia poi successivamente firmato CAdES. Il processo di verifica automaticamente segnala all'utente che all'interno della busta crittografica

P7M o TSD è presente un file firmato PAdES. Il processo di verifica mostra il risultato per la busta esterna, per procedere alla verifica delle firme PAdES è necessario procedere con l'estrazione del documento dalla busta (vedi Cap. 6).

6 Estrarre il documento originale dalla busta crittografica

L'App è in grado di estrarre il documento originario da una busta crittografica P7M oppure da una file marcato TSD. È possibile selezionare l'azione “Estrai documento” ogni qualvolta viene selezionato un file crittografico o in “Firma digitale” o in “Archivio”.

Il documento estratto viene salvato in “Firma digitale” secondo le seguenti modalità.

- Se il file è un **P7M** viene salvato il dato firmato eliminando dal nome del file l'estensione P7M
- Se il file è un **TSD** o un **M7M** in “Firma digitale” l'App salva sia la busta crittografica P7M che il dato firmato originale