



ProxySign: Firma digitale remota

Manuale Utente

Versione

1.0

Data

25 Giugno 2016



Sommario

Sommario	2
1. Novità introdotte rispetto alla precedente emissione	3
2. LegalCare ProxySign.....	4
2.0. Portale di firma digitale su dispositivi remoti.....	4
2.1. Firma digitale.....	5
2.1.1. Lista Parametri:	5
2.1.2. Firma digitale Remota	7
2.1.3. Firma digitale Automatica.....	11
2.2. Verifica di firma	11
2.3. Marca Temporale.....	13

1. Novità introdotte rispetto alla precedente emissione

Versione/Release n°	1.0	Data Versione/Release	25/06/2016
Motivazioni	prima emissione		
Collaborazioni	Antonio Battistini, Gianluigi Sannito		

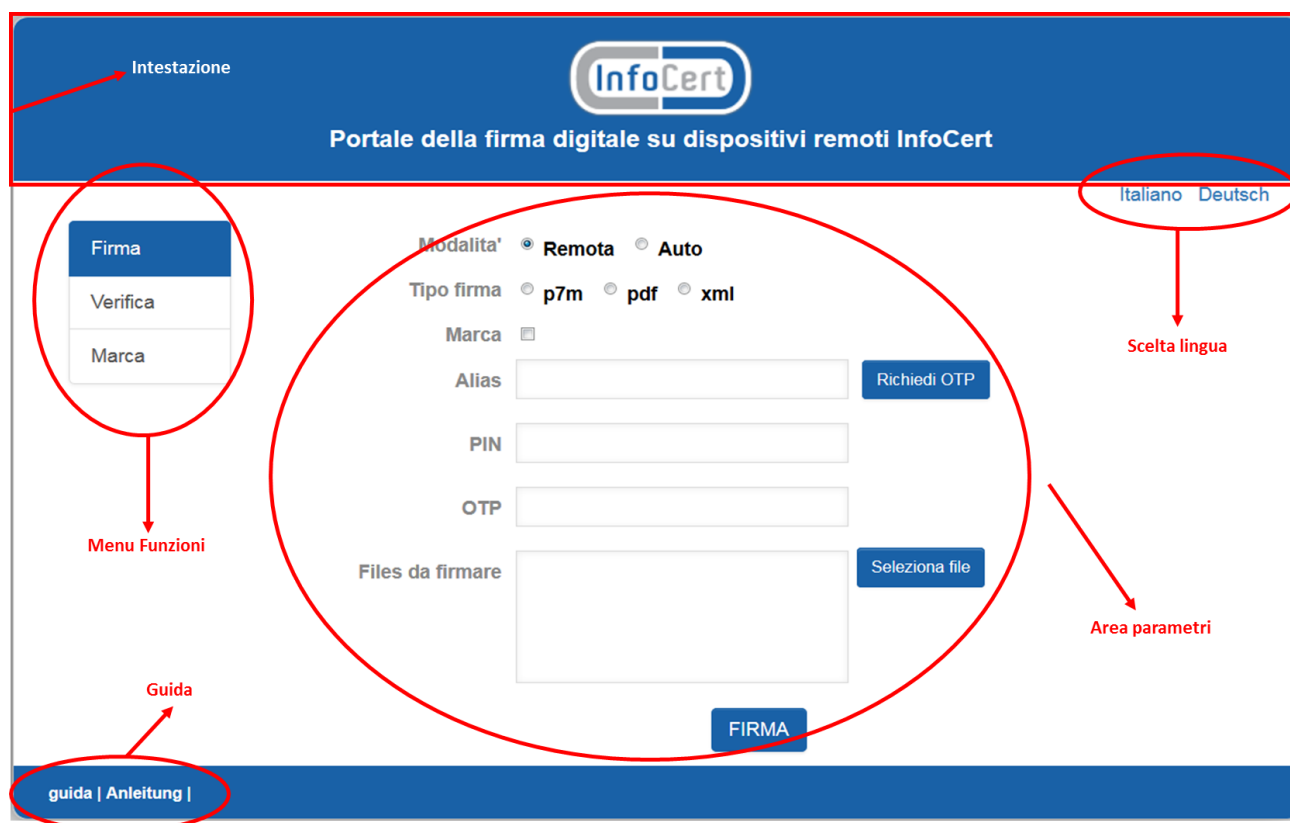
2. LegalCare ProxySign

Il presente documento descrive le modalità di utilizzo del Portale di firma digitale su dispositivi remoti InfoCert.

2.0. Portale di firma digitale su dispositivi remoti

Per accedere al Portale il titolare del certificato dovrà collegarsi, tramite qualsiasi Internet Browser di ultima generazione, all'indirizzo <https://proxysig-XXX.linkverse.com/proxysign/> raggiungibile all'interno della intranet aziendale. Dove XXX è la signa dell'azienda di riferimento es: ASLTO3, ULSS9, ASLBZ ecc). E' possibile in accordo con l'azienda, definire un URL che sia coerente con le policy interne.

Dalla Home Page del Portale si potranno eseguire tutte le funzionalità descritte in dettaglio nei paragrafi successivi.



La Home Page è costituita dalle seguenti aree:

- **Intestazione:** Area che riporta il logo e la descrizione del portale. Quest'area è personalizzabile nel logo dell'azienda e nel colore di sfondo che può essere impostato in modo congruente con i colori riportati nel sito istituzionale.
- **Scelta lingua:** Alla data il Portale gestisce l'Italiano e il Tedesco. Sono possibili, a richiesta aggiunte di ulteriori lingue.
- **Menu funzioni:** Pulsanti per la scelta della funzione.

- **Area parametri:** In quest'area, in base alla funzione scelta vengono visualizzati i parametri da impostare per l'esecuzione della funzione.
- **Guida:** Menu per l'accesso a questa guida.

2.1. Firma digitale

La prima funzione del menu è quella che riguarda la Firma Digitale.

Cliccando sul pulsante, nella parte centrale della pagina, appaiono i parametri da impostare per eseguire la funzione.

The screenshot shows the 'Portale della firma digitale su dispositivi remoti InfoCert' interface. At the top, there is the InfoCert logo and the title. Below the title, there are language options for 'Italiano' and 'Deutsch'. On the left, there is a navigation menu with 'Firma' (selected), 'Verifica', and 'Marca'. The main content area contains the following fields and options:

- Modalita'**: Radio buttons for 'Remota' (selected) and 'Auto'.
- Tipo firma**: Radio buttons for 'p7m' (selected), 'pdf', and 'xml'.
- Marca**: A checkbox that is currently unchecked.
- Alias**: A text input field with a 'Richiedi OTP' button to its right.
- PIN**: A text input field.
- OTP**: A text input field.
- Files da firmare**: A large empty text area with a 'Seleziona file' button to its right.
- FIRMA**: A large blue button at the bottom center.

At the bottom left of the page, there is a footer with the text 'guida | Anleitung |'.

2.1.1. Lista Parametri:

Modalità: Questo parametro indica il tipo di firma che deve essere applicata. Le opzioni possibili sono Firma Remota e Firma Automatica. Va selezionata l'opzione compatibile con il certificato che è stato rilasciato. Il parametro è obbligatorio.

Tipo firma: ProxySign gestisce tre formati di firme:

1. firma digitale in formato p7m (CAAdES);
2. firma digitale in formato PDF (PAdES);
3. firma digitale in formato XML (XAdES).

1. **La firma CADES** è una firma digitale che può essere apposta su qualsiasi tipo di file, con la CADES si possono firmare file di testo comunque generati (Microsoft Word, OpenOffice Writer, file di testo, etc.), fogli di calcolo (Microsoft Excel, OpenOffice Calc), file immagine (JPEG, GIF, PNG, etc.), ovviamente è possibile firmare anche dei PDF. L'apposizione di una firma CADES su un qualsiasi file genera una busta crittografica contenente il file originale che si presenta come un file la cui estensione è P7M dopo l'estensione del tipo di file (ad esempio 'fattura.pdf' diventerà 'fattura.pdf.p7m'). **“Attenzione a non confondere la firma di un file pdf in formato pkcs#7 con la firma pdf** – specifica un documento ufficiale del Governo in tema di **firma digitale** – *Quest'ultima non modificherà l'estensione del nome del file che rimarrà sempre 'pdf'”*.
2. La firma **PAdES** è una firma che può essere apposta su un solo tipo di file, il PDF che è lo standard di riferimento per quanto riguarda i documenti in formato digitale. L'apposizione di una firma PAdES su un file .pdf genera un nuovo file la cui estensione è ancora PDF (ad esempio 'fattura.pdf' resterà 'fattura.pdf'). In questo caso l'evidenza della firma è incapsulata all'interno del documento stesso e può essere visualizzata utilizzando un reader di Acrobat o grazie ai software gratuiti messi a disposizione dalle CA.
3. **La firma XAdES** rappresenta un nuovo standard di firma digitale basato su file XML. Come per la firma PAdES, questo formato non necessita di operazioni di imbustamento/sbustamento per poter essere interpretato. La firma XAdES permette anche di firmare singole parti di un documento.

Marca: Questo parametro serve ad indicare la volontà di applicare una Marca Temporale oltre alla firma.

Alias: Rappresenta l'identificativo che permette di recuperare il certificato da utilizzare per la firma. L'alias viene indicato al momento della registrazione per la richiesta del certificato. Tipicamente potrebbe essere il codice fiscale del firmatario.

PIN: Il PIN è il codice segreto consegnato all'atto del rilascio del certificato che associato all'Alias garantiscono l'autenticazione del firmatario.

OTP: One Time Password. E' un ulteriore chiave di sicurezza che viene richiesta solo in caso di firma remota. Per la firma automatica non viene richiesto. L'OTP è un codice numerico che viene inviato al cellulare del firmatario, o ad altro dispositivo sicuro, dopo aver premuto il pulsante “Richiedi OTP”. Il codice ricevuto va inserito nel campo OTP.

FILES da firmare: in questo campo si indicano il o i files da firmare. La scelta viene fatta premendo il pulsante “Seleziona file”.

N.B: *la selezione multipla si può effettuare tenendo premuto il tasto CTRL e cliccando sui nomi dei file visualizzati nella lista.*

2.1.2. Firma digitale Remota

Firma p7m

Per applicare questa firma è necessario essere in possesso di un Certificato di Firma Remota rilasciato da una Certification Authority. Nella figura successiva viene visualizzato un esempio di firma remota in formato p7m.

Nel campo Alias si deve inserire l'alias dichiarato in sede di registrazione e il PIN.



The screenshot shows the 'Portale della firma digitale su dispositivi remoti InfoCert' interface. It features a navigation menu on the left with 'Firma', 'Verifica', and 'Marca'. The main area contains a form for remote signing with the following fields and options:

- Modalita'**: Radio buttons for 'Remota' (selected) and 'Auto'.
- Tipo firma**: Radio buttons for 'p7m' (selected), 'pdf', and 'xml'.
- Marca**: A checkbox that is currently unchecked.
- Alias**: A text input field containing 'snnglg53h09g224h' and a 'Richiedi OTP' button.
- PIN**: A text input field with seven dots representing a masked PIN.
- OTP**: A text input field containing '12345678'.
- Files da firmare**: A list box containing three files: 'Prova firma.pdf', 'Prova firma_f.pdf', and 'Prova firma1_f.pdf', with a 'Seleziona file' button.
- FIRMA**: A large blue button at the bottom of the form.

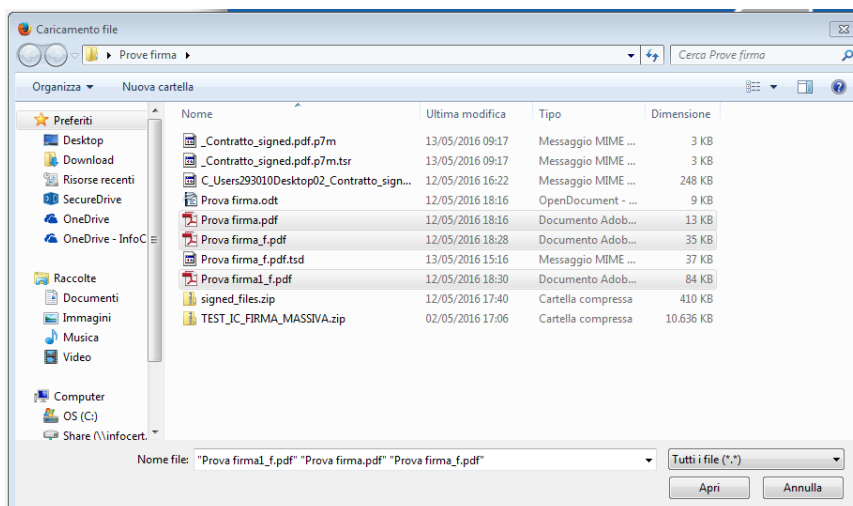
At the top right, there are language options for 'Italiano' and 'Deutsch'. At the bottom left, there is a link for 'guida | Anleitung |'.

Per richiedere l'OTP (secondo codice di sicurezza) basta premere il pulsante dopo aver inserito nel campo Alias la propria credenziale.

Dopo qualche secondo riceverete sul vostro cellulare o altro dispositivo fisico un codice numerico che dovete inserire nel campo OTP.

La selezione del o dei file da firmare avviene premendo il pulsante "Seleziona file" e tenendo premuto il tasto CTRL si clicca sui file da firmare.

ProxySign Manuale Utente – Versione 1.0

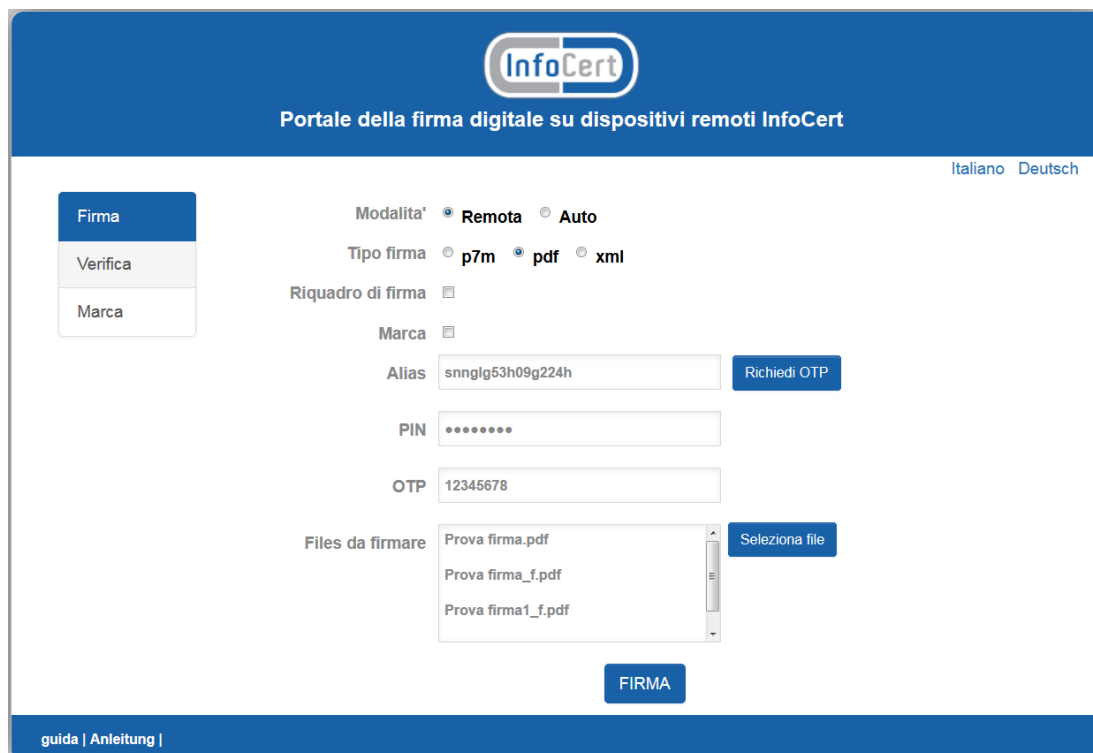


L’elenco dei file viene riportato sulla pagina e a questo punto è possibile avviare le operazioni di firma premendo il tasto firma.

N.B: E’ possibile firmare anche l’intero contenuto di una cartella selezionando il nome della directory. In questo caso su tutti i file contenuti verrà applicata una firma.

Firma PDF

La firma PDF si effettua selezionando il tipo firma PDF. L’unica variante rispetto alla firma p7m è che qui appare un parametro in più. Il “Riquadro firma” permette di aprire una finestra dove inserire ulteriori parametri caratteristici della firma PDF.



Nella figura seguente sono riportati i parametri per la firma PDF:

Pagina riquadro di firma: Qui si indica su quale pagina del documento si vuole apporre la firma. Il default è Pagina 1.

Formato di pagina: E' possibile indicare il formato della pagina del documento da firmare. I formati possibili sono A3 e A4 sia in Portrait che in Landscape.

Larghezza/Altezza riquadro firma: La firma viene apposta su riquadro del quale si possono indicare le dimensioni in altezza e larghezza. Le coordinate di posizionamento vanno impostate spostando il riquadro blu situato all'interno della preview del riquadro di firma


Reason: E' possibile indicare il motivo della firma che verrà visualizzato nel riquadro.

Immagine signature: Se si dispone di una immagine scannerizzata della propria firma è possibile indicare il nome del file su cui risiede. L'immagine verrà visualizzata nel riquadro di firma.

Riquadro di firma

Pagina riquadro di firma	<input type="text" value="1"/>
Formato di pagina	<input type="text" value="A4 Portrait"/>
Larghezza riquadro firma	<input type="text" value="40"/> mm
Altezza riquadro firma	<input type="text" value="25"/> mm
Reason	<input type="text" value="firma documento di prova"/>
Immagine signature	<input type="text" value="20100310154525572_0001.tif"/>

Preview riquadro di firma



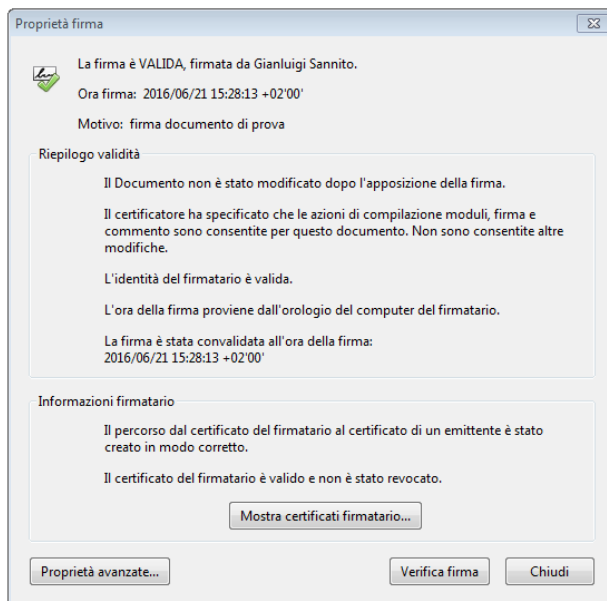
X vertice in basso a sinistra: 20
Y vertice in basso a sinistra: 17
X vertice in alto a destra: 134
Y vertice in alto a destra: 88

Una volta firmato il documento se lo si apre con Acrobat reader vedremo che laddove lo abbiamo impostato, troveremo il nostro riquadro di firma che avrà il seguente aspetto.

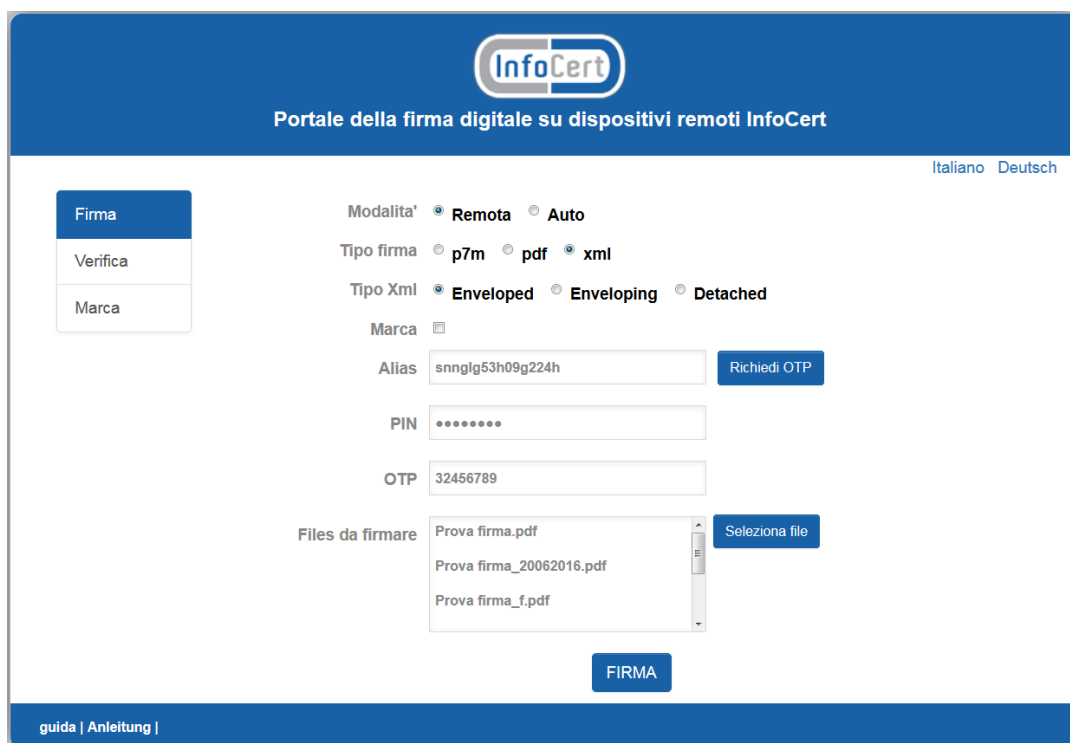
Digitally signed by:
Gianni Sannito
Date: 2016.06.21
13:29:08 +0100
Reason: firma
documento di prova

Cliccando sul riquadro verrà visualizzata una finestra contenente il rapporto di verifica.

ProxySign Manuale Utente – Versione 1.0

**Firma XML**

La firma XML è un particolare formato di firma che si applica ai files fomato XML.



Le opzioni di firma sono le stesse dei formati precedenti ad esclusione del tipo di XML che può essere scelto. Selezionando l'opzione XML appariranno tre nuove scelte.

- Enveloping: Documento da firmare incluso nella firma
- Detached: Documento da firmare esterno al documento che include la firma
- Enveloped: Elemento Firma incluso nel documento da firmare

Firma e Marca

Se si vuole applicare anche una marca temporale basta selezionare la casella “Marca” ed impostare i campi USER e PASSWORD di accesso al servizio di marcatura.

Marca

Username	YYI0105
Password

2.1.3. Firma digitale Automatica

La firma Automatico è esattamente uguale alla firma remota con la sola differenza che non appare il campo OTP e il relativo pulsante.

2.2. Verifica di firma

E' possibile in qualsiasi momento effettuare la verifica di un file firmato digitalmente. Premendo il pulsante “Verifica” appare la schermata

InfoCert
Portale della firma digitale su dispositivi remoti InfoCert

Italiano Deutsch

Firma
Verifica
Marca

File da verificare: Prova firma_20062016.pdf


Seleziona file

Verifica

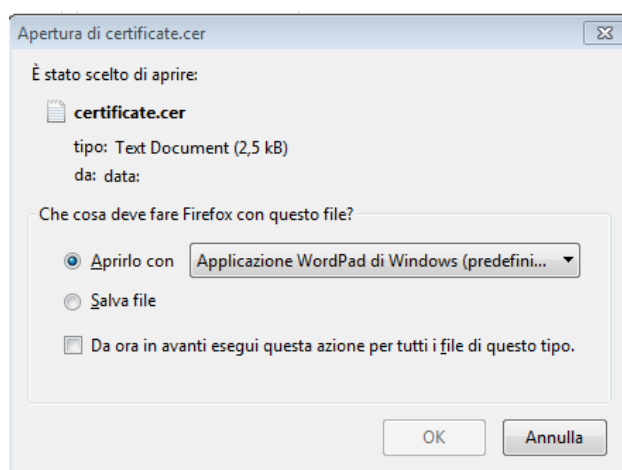
guida | Anleitung |

L'unico parametro da inserire è il nome del file da verificare. Una volta premuto il pulsante Verifica apparirà la risposta dal sistema:

ProxySign Manuale Utente – Versione 1.0

File verificato	Prova firma_20062016.pdf
Firmatario 1	
 Firma valida	
Firmatario	SANNITO GIANLUIGI
Data di verifica	21 06 2016 15:23:08
Ente Certificatore	InfoCert Firma Qualificata 2
Codice Fiscale	IT:SNNGLG53H09G224H
Nome comune	Gianluigi Sannito
Stato	IT
Organizzazione	NON PRESENTE
Limite D'Uso	Il presente certificato Ãˆ valido solo per le firme apposte con procedura automatica. This certificate may only be used for unattended/automated digital signatures.
Codice Identificativo	201660000268
Validit� del certificato	Dal 11 05 2016 09:00:05 al 11 05 2019 00:00:00
Data e ora della firma	21 06 2016 13:28:13
 Scarica il certificato	

L'esito riporta l'indicazione della validit  della firma e i dati qualificanti il certificato utilizzato. Dal rapporto   anche possibile scaricare il certificato premendo sulla voce "Scarica il certificato"



2.3. Marca Temporale

La terza funzionalità disponibile è la marca temporale che abbiamo già trattato in precedenza.

La differenza consiste nel fatto che questa funzione permette di applicare marche temporali in maniera disgiunta dalla firma. E', quindi, possibile marcare un file senza firmarlo.

La funzionalità precedente era una marcatura contestuale alla firma.

La figura seguente illustra i parametri necessari al completamento della funzione di marca.

The screenshot shows the 'Portale della firma digitale su dispositivi remoti InfoCert' interface. On the left, there is a navigation menu with 'Firma', 'Verifica', and 'Marca' (highlighted). The main area contains a form for applying a timestamp. At the top right, there are language options 'Italiano' and 'Deutsch'. The form includes: 'Tipologia di marca' with radio buttons for 'TSD' (selected), 'M7M', and 'TSR'; 'Username' with the value 'YYI0105'; 'Password' with masked characters; 'File da marcare' with the value 'Prova firma_20062016.pdf' and a 'Seleziona file' button; and a 'Marca' button at the bottom. A footer bar contains the text 'guida | Anleitung |'.

La novità consiste nella tipologia di Marca Temporale che è possibile applicare:

- **Formato TSR:** Contiene di fatto solo l'impronta del file, NON tutto il file, e l'evidenza informatica di quella che è l'apposizione della marca temporale, per fare la verifica di un file con questo formato è indispensabile possedere anche il file originale che si è marcato, altrimenti saremo solo in grado di controllare che la marca temporale sia stata realizzata in modo corretto ma non siamo in grado di verificare se il file TSR corrisponde al file originale. La dimensione di un file con formato ed estensione TSR è sicuramente di inferiore al file originale.
- **Formato M7M:** Contiene sia l'evidenza della marca temporale (il file con formato TSR) che il file stesso sottoposto a marcatura, quindi sottoponendo a verifica un file con formato M7M non abbiamo bisogno di altro in quanto nel file stesso è contenuto tutto sia l'originale che l'evidenza informatica della marca temporale.
- **Formato TSD:** Contiene sia l'evidenza della marca temporale (il file con formato tsr) che il file stesso sottoposto a marcatura, quindi sottoponendo a verifica un file con formato TSD non abbiamo bisogno di altro in quanto nel file stesso è contenuto tutto sia l'originale che l'evidenza informatica della marca temporale. Diversamente dal formato M7M il formato TSD rispetta una sintassi di composizione che rispetta standard ampiamente riconosciuti dalla comunità informatica ed è per questo che è da preferire al formato M7M.

ProxySign Manuale Utente – Versione 1.0

Una volta impostato il tipo di marca temporale da applicare inseriamo le credenziali e selezioniamo il file da marcare e premiamo il tasto marca.