COD	D16

DELIBERAZIONE

232	DGEN	28 DIC. 2017
NUM.	AREA	DATA

Istituto Nazionale di Statistica

IL DIRETTORE GENERALE

Visto il decreto legislativo 6 settembre 1989, n. 322, recante "Norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di Statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400 e s.m.i.";

Visto il D. lgs. 30 marzo 2001, n. 165 recante "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche" e successive modificazioni;

Visto il D. lgs. n. 82/2005 e successive modificazioni e integrazioni (Codice dell'amministrazione digitale), ed in particolare gli articoli 12 e seguenti, relativi agli obblighi delle pubbliche amministrazioni in materia di utilizzo delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa, nonché gli articoli 20 e seguenti in materia di documento informatico e firme elettroniche;

Visto il DPR 7 settembre 2010, n. 166, concernente il regolamento recante il riordino dell'Istituto nazionale di statistica e in particolare l'art. 5 relativo agli uffici dirigenziali e all'organizzazione interna;

Visto il Regolamento di organizzazione dell'Istituto approvato con DPCM del 28 aprile 2011, ed in particolare l'art. 10, che conferisce al Direttore Generale funzioni di coordinamento delle attività dell'Istituto, in ordine alle funzioni giuridiche e amministrative, nonché funzioni propositive in materia di assetto organizzativo, semplificazione dei procedimenti amministrativi e di adozione di carte dei servizi interni;

Visto l'Atto di Organizzazione Generale n. 1, concernente le "Linee fondamentali di organizzazione e funzionamento dell'Istituto nazionale di statistica", approvato dal Consiglio dell'Istituto con deliberazione n. CDXII del 9 febbraio 2016 e modificato con successive deliberazioni del 9 novembre 2016 e del 26 giugno 2017;

Viste la deliberazione n. 46/DGEN del 18 marzo 2016, con la quale sono stati costituiti, a decorrere dal 15 aprile 2016, i Servizi giuridici amministrativi nell'ambito delle Direzioni centrali afferenti alla Direzione Generale, e la deliberazione n. 97/DGEN del 28 luglio 2016, con la quale sono specificamente individuate, nell'ambito delle corrispondenti Direzioni centrali, le linee di attività dei Servizi giuridici amministrativi;

Visto il DPCM 13 novembre 2014, recante le Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni;

Visto il Piano Strategico Triennale (PST) 2017/2019 il quale assegna alla Direzione Generale il coordinamento del Programma "PG6. Piena digitalizzazione dei dati e dei processi", che include le iniziative finalizzate a potenziare e a integrare i sistemi gestionali che concorrono a rendere trasparente l'azione amministrativa e di produzione, con l'obiettivo di "aumentare la disponibilità e l'accesso ai dati, sfruttando pienamente le opportunità offerte dalla tecnologia";

Rilevato che, nell'ambito del progetto per il passaggio da un sistema documentale a base cartacea ad un sistema a base digitale, occorre adottare in modo sistematico la firma digitale, ferme restando le competenze funzionali spettanti ai titolari;

Ritenuto necessario disciplinare le modalità di gestione e utilizzo della firma digitale all'interno dell'Istituto, fornendo contestualmente le istruzioni operative per l'utilizzo del servizio di firma digitale;

DELIBERA

l'adozione della Versione 1.0 delle "Linee guida per l'attivazione e l'utilizzo della firma digitale d'Istituto" e del relativo Manuale operativo, allegati al presente provvedimento, di cui costituiscono parte integrante.

Sede, 28 DIC. 2017

IL DIRETTORE GENERALE
Tommaso Antonucci

Direzione Generale

Direzione centrale per le tecnologie informatiche della comunicazione

Linee guida per l'attivazione e l'utilizzo della firma digitale d'Istituto.

Versione 1.0

Versione	Aggiornamenti e variazioni	Data
1.0		28 Dicembre 2017

Sommario

Premessa

Il sistema di gestione documentale adottato dall'Istituto, in linea con la regolamentazione vigente in materia di Amministrazione Digitale, si basa sull'utilizzo e l'integrazione dei seguenti strumenti ICT:

- protocollo informatico e gestione dell'iter documentale
- posta elettronica certificata (PEC)
- firma digitale
- conservazione digitale.

Nell'ambito del progetto per il passaggio da un sistema documentale a base cartacea ad un sistema a base digitale, un importante traguardo è rappresentato dall'adozione della firma digitale, che consente di sottoscrivere documenti informatici con lo stesso valore giuridico dei documenti sottoscritti con firma autografa.

Le presenti Linee guida offrono una panoramica generale della normativa in materia, con riferimento sia al quadro giuridico sia alle normative interne vigenti nell'Istituto, e disciplinano le modalità di gestione e utilizzo della firma digitale nell'Istituto nazionale di statistica (da questo punto in avanti Istat), nel rispetto delle previsioni e degli obblighi di legge (parte 1).

Nella parte 2 sono descritte:

1. l'organizzazione interna del servizio di assegnazione, sospensione e revoca dei certificati da utilizzare per la sottoscrizione in forma elettronica dei documenti informatici;
2. le regole e l'ambito di applicabilità della sottoscrizione dei documenti informatici con firma digitale.

Le linee guida sono completate dal Manuale operativo (allegato 2) in cui sono riepilogate le istruzioni per l'utilizzo del servizio di firma digitale in ambito Istat.

Parte 1 – Concetti generali

1. I documenti informatici e la firma digitale: contesto normativo di riferimento

La gestione documentale di una pubblica amministrazione riguarda tutti i documenti prodotti o acquisiti nello svolgimento delle relative funzioni istituzionali e amministrative. Tali documenti, tra loro connessi da vincolo originario, necessario e determinato, vanno a costituire l'archivio dell'amministrazione.

Il documento rappresenta un'entità fisica in cui sono registrate delle informazioni, a prescindere dal supporto utilizzato per contenerle, purché il supporto stesso risulti tra quelli accettati ufficialmente dall'ente produttore di documenti ed archivi.

All'interno del complesso di requisiti funzionali archivistici, organizzativi e tecnologici necessari per la corretta gestione di archivi digitali, un aspetto centrale è svolto da strumenti e procedure di qualità, finalizzati ad assicurare affidabilità e accuratezza nelle diverse fasi di produzione e tenuta delle risorse documentarie, soprattutto nel caso di documenti informatici formati o acquisiti dalla pubblica amministrazione.

Il Codice dell'amministrazione digitale (da ora in poi CAD) definisce **documento informatico** il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti anche interni all'amministrazione pubblica, comunque utilizzati ai fini dell'attività amministrativa della stessa, espressi mediante un testo, un'immagine, un filmato, una riproduzione sonora.

Il documento informatico è, quindi, un *file*, cioè una sequenza determinata di valori binari indifferente al supporto fisico su cui è memorizzata, ed è leggibile solo mediante l'ausilio di strumenti tecnologici.

La rilevanza giuridica e la capacità probatoria del documento informatico derivano dalla sua **autenticità**, intesa come capacità di rappresentare in modo efficace il fatto o atto giuridico, e **integrità** , ovvero il non aver subito manomissioni o altre alterazioni.

Quanto sopra riportato implica una serie di conseguenze in termini di gestione dei controlli e presenza di informazioni necessarie a garantire, nei documenti informatici:

- certezza nell'imputabilità dei contenuti del documento all'autore (integrità, data certa, provenienza[1]);
- definizione della posizione logica che il documento occupa nell'archivio o nel sistema di tenuta e identificazione delle relazioni di contesto, documentarie e amministrative in particolare;
- stabilità dei contenuti e delle componenti del documento nel tempo e delle relazioni tra i documenti (condizioni adeguate di verifica, gestione persistente delle informazioni rilevanti).

Nella corretta gestione del documento informatico occorrerà, pertanto, prestare cura ed attenzione al mantenimento dei seguenti requisiti:

[1] Da non confondersi con l'indirizzo di provenienza o di trasmissione, ma come origine/indicazione, certa e verificabile, dell'autore del documento in quanto responsabile per il suo contenuto. La certezza della provenienza implica controlli sulla corretta formazione del documento stesso e una sottoscrizione (autografa o digitale), dalla quale derivano limiti al potere di creare documenti e privilegi di accesso agli stessi.

Affidabilità = capacità del documento di rappresentare i fatti cui si riferisce, che attengono al momento della sua creazione. Un documento informatico è affidabile in relazione alla capacità di fare fede dell'ente produttore, se la persona che lo produce è affidabile e identificabile nel suo ruolo.

Autenticità = caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.

Accessibilità = Usabilità costante. Il documento deve essere reperibile, leggibile, intelligibile a breve e lungo periodo.

Integrità = Certezza di conservazione non manipolata o contraffatta.

Tabella 1 –Il documento amministrativo informatico in sintesi

DOCUMENTO AMMINISTRATIVO INFORMATICO	Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
FORME	Documenti di testo, fogli di calcolo, schemi XML redatti tramite l'utilizzo di appositi strumenti software Documenti acquisiti per via telematica o su supporto informatico, e-mail, documenti acquisiti come copia per immagine di un documento analogico Registrazioni informatiche di transazioni o processi informatici, dati forniti dall'utente attraverso la compilazione di moduli o formulari elettronici Insieme di dati, provenienti da una o più basi dati, raggruppati secondo una struttura logica determinata (viste)
CARATTERISTICHE	Essere identificato in modo univoco e persistente Essere immodificabile, cioè formato in modo che forma e contenuto non siano alterabili e ne sia garantita la staticità nella fase di conservazione Essere prodotto in uno dei formati idonei alla conservazione essere memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi Avere associati almeno un set minimo di metadati

A differenza del documento analogico, che si caratterizza per la pluralità di forme – scrittura privata, atto pubblico, scrittura privata autenticata – che ne sostanziano il diverso valore giuridico-probatorio, il documento informatico si caratterizza per la pluralità di firme elettroniche, con diversi valori di sottoscrizione, firma, sigla o visto, che caratterizzano e diversificano l'efficacia giuridico-probatoria del documento stesso.

La firma elettronica non è, infatti, la rappresentazione informatica grafica della firma, ma un meccanismo di associazione di dati per l'imputazione di effetti giuridici in capo a un determinato soggetto che ne appare l'autore.
Ciò che contraddistingue il documento informatico è la sua forma elettronica, di rappresentazione informatica. Solo in questa forma il documento informatico può essere formato, acquisito, sottoscritto, trasmesso e conservato.

Il documento amministrativo informatico deve essere formato, come descritto nel par. 2, garantendo l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento. Prerogativa necessaria affinché il documento integri le caratteristiche di qualità e sicurezza, è la sua gestione all'interno di un sistema di gestione documentale conforme alla normativa vigente in materia di amministrazione digitale.

L'attributo "qualità", utilizzato nel capoverso precedente, è da intendersi anche come adeguatezza all'uso e capacità del documento di rendere fruibili le informazioni in esso contenute: il documento informatico deve garantire la leggibilità del suo contenuto; posto che quest'ultima dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato, la scelta dei formati risulta estremamente importante e, dal punto di vista della leggibilità dei documenti informatici, decisiva.

Infine, l'imputabilità di una determinata rappresentazione ad un soggetto, nella maggior parte dei documenti, è garantita dalla sottoscrizione: chi sottoscrive fa proprio il contenuto dell'atto sottoscritto. Per il documento informatico si è reso necessario ideare una sottoscrizione elettronica, in grado di assicurare il legame tra il firmatario e il documento informatico.
La sottoscrizione elettronica è un processo informatico basato su algoritmi crittografici che permettono di rappresentare un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

In particolare la **firma digitale** è il risultato di una procedura informatica, detta validazione, che garantisce: (i) al firmatario del documento informatico di renderne manifesta l'autenticità; (ii) al destinatario di verificare l'integrità dei documenti informatici ricevuti. Consente pertanto di scambiare in rete documenti con piena validità legale. Essa è associata stabilmente al documento elettronico sulla quale è apposta e non consente: (i) di modificare il documento su cui è apposta; (ii) di estrapolarne la firma ed allegarla ad un altro oggetto; (iii) all'autore di negarne l'attribuzione.

I requisiti legali ai sensi del CAD cui assolve la firma digitale sono, infatti:

- integrità, cioè la certezza che il documento non sia stato manomesso o modificato dopo la sottoscrizione;
- autenticità, garanzia dell'identità di chi firma;
- non ripudio, il documento informatico sottoscritto ha piena validità legale e non può essere ripudiato dal firmatario.

Possono dotarsi di firma digitale tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni.

La firma digitale viene rilasciata da un'Autorità di certificazione, cioè un soggetto pubblico o privato, accreditato ed autorizzato ai sensi dell'articolo 29 del CAD, che ha il compito di garantire la sicurezza della firma, ponendosi come "terza parte fidata", cioè soggetto terzo che si trova in posizione di neutralità rispetto agli utilizzatori [2].

La differenza tra firma autografa e firma digitale è che la prima è legata ad una caratteristica di tipo fisico-materiale della persona che appone la firma, vale a dire la grafia, mentre la seconda al possesso di uno strumento informatico e di un PIN di abilitazione, da parte del firmatario.

Ai sensi dell'art. 21 co. Del CAD *"Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, ha altresì*

[2] Tra i compiti di tali Enti: verifica ed attestazione, emettendo un apposito certificato digitale, dell'identità del titolare; stabilire il termine di scadenza dei certificati; pubblicare il certificato e la chiave pubblica; ricevere la segnalazione di eventuali smarrimenti, furti, cancellazioni, divulgazioni improprie di chiavi private e pubblicare, quindi, la lista dei certificati revocati o sospesi in conseguenza di tali fatti.

l'efficacia prevista dall'articolo 2702 del codice civile[3]*. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria."*

All'utilizzo della tecnologia avanzata è connesso pertanto il rischio di abusiva sottoscrizione da parte di un soggetto diverso dal titolare. Il "disconoscimento" di quanto sottoscritto con firma digitale[4] non potrà avere ad oggetto l'apposizione della firma, né la scrittura, ma solo l'utilizzo del dispositivo di firma. Il concetto di paternità del documento, in ambito elettronico, è sostituito da quello della responsabilità **del** e **sul** documento.

In altri termini, sarà possibile dar conto del "furto" di identità digitale documentando eventuali situazioni di sottrazione ad es. del codice identificativo, che potrebbero consentire ad un soggetto differente dal titolare di sottoscrivere il documento informatico con la firma digitale appartenente ad altri [5]. In questi casi l'eventuale raggiungimento della prova del "furto" di identità elettronica da un lato condurrà all'inefficacia delle statuizioni giuridiche di cui al documento, e dall'altro non escluderà conseguenze risarcitorie anche a carico dell'apparente sottoscrittore, ogniqualvolta costui non abbia adottato le cautele del caso nella custodia del dispositivo di firma.

2. Le procedure per la corretta produzione di documenti amministrativi informatici

I documenti dell'Istituto sono prodotti, gestiti e conservati, in conformità alla vigente normativa in materia di documentazione amministrativa, tramite il sistema di gestione documentale dell'Istituto e la scheda di protocollazione e di repertoriazione costituisce parte integrante del documento informatico prodotto.

Gli atti formati con strumenti informatici, nonché i dati e i documenti informatici detenuti dall'Istituto, costituiscono informazione primaria e originale da cui è possibile effettuare duplicazioni e copie per gli usi consentiti dalla legge.

Il **duplicato del documento informatico** è un documento prodotto mediante idoneo processo o strumento che assicuri che il documento informatico, ottenuto sullo stesso sistema di memorizzazione o su un sistema diverso, contenga la stessa sequenza binaria del documento informatico di origine da cui è tratto.

La **copia di documento informatico** è, invece, un documento informatico che può mutare il formato del documento originario o che muta il supporto del documento originario informatico (ad esempio, il salvataggio di un file in un formato differente: da .doc a .pdf, oppure da .doc a .ods).

La **copia su supporto analogico** di documento informatico, sottoscritto con firma digitale, per avere la stessa efficacia probatoria dell'originale da cui è tratta, deve essere certificata come conforme all'originale

---

[3] Art. 2702 c.c.: *"la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta".*

[4] Per indicazioni sul corretto utilizzo del dispositivo di firma, sulle precauzioni da adottare e sui doveri dei titolari si rinvia alla parte 2 delle presenti linee guida.

[5] E' possibile distinguere tra falsificazione di un documento apparentemente sottoscritto da un determinato soggetto e falsificazione della richiesta di firma digitale apparentemente presentata da quel soggetto. Mentre nel primo caso viene in considerazione un'ipotesi di falsità in scrittura privata (perseguibile a querela di parte), nel secondo si tratta della ben più grave ipotesi di falsità ideologica commessa da privato in atto pubblico (Cass. Pen, Sez.V, 10200/11).

in tutte le sue componenti da un pubblico ufficiale autorizzato a eseguire tale attestazione nell'esercizio delle sue funzioni (copia "autentica") salvo che la conformità allo stesso non sia espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

Si evidenzia che mentre le copie di documenti informatici si limitano a mantenere il contenuto dei documenti originari (ma non il loro formato), i **duplicati informatici** non necessitano di attestazione di conformità all'originale da parte di un notaio o di un pubblico ufficiale, stante la loro perfetta corrispondenza nel numero e nella sequenza dei valori binari e hanno il medesimo valore giuridico del documento informatico da cui sono tratti qualora prodotti mediante processi e strumenti che assicurino la predetta sequenza.

La produzione di documenti originali informatici favorisce anche le attività necessarie a rispondere agli obblighi di trasparenza ed implica che gli atti e i documenti Istat siano, progressivamente, prodotti, trattati e conservati come originali informatici.

Il documento amministrativo informatico e le istanze, le dichiarazioni e le comunicazioni previste dalla legge sono soggetti, ove necessario, a registrazione di protocollo, segnatura, classificazione e fascicolazione.

Il documento amministrativo informatico assume le caratteristiche di immodificabilità e di integrità oltre che nei modi di cui al presente paragrafo anche con la registrazione nel registro di protocollo unico e nei registri particolari contenuti nel sistema di gestione documentale d'Istituto.

Il documento informatico è formato mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software. In tal caso il documento informatico assume le caratteristiche di **immodificabilità e di integrità** con la sottoscrizione con firma digitale/firma elettronica qualificata, oppure con l'apposizione di una validazione temporale o con il trasferimento a soggetti terzi tramite PEC, con ricevuta completa o con la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza o con il versamento ad un sistema di conservazione;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico. In tali casi, le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione documentale che garantisca l'inalterabilità del documento o in un sistema di conservazione;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente. In tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica: in tal caso le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della medesima

operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Per la formazione, gestione e conservazione dei documenti informatici, Istat usa tipologie di formato coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico e tali da garantire i principi di interoperabilità tra i sistemi di conservazione, in base alla normativa vigente.

La scelta dei formati è stata effettuata considerando che essi, come da previsione normativa, devono garantire la leggibilità e la reperibilità del documento informatico nell'intero ciclo di vita dello stesso; pertanto nella scelta si sono valutate le caratteristiche di apertura, sicurezza, portabilità, funzionalità e il supporto allo sviluppo e la diffusione dei formati. I formati standard adottati dall'Istituto nella gestione documentale dell'Istituto sono riepilogati nella Tavola 1.

Tavola 1. Formati standard validi

Testo	**PDF** (Portable document format), basato su un linguaggio di descrizione di pagina sviluppato per la prima volta da Adobe Systems nel 1993 per rappresentare documenti in modo indipendente dall'hardware e dal software utilizzati per generarli o per visualizzarli; **PDF/A** standard ISO basato sulla versione 1.4 del formato PDF di Adobe Systems e implementato in Adobe Acrobat versione 5 e successive; **TXT** quale formato generico di testo con codifica MS-DOS. **ODT**, ODS, **ODP** e **ODG** per i documenti nel formato Open Document (ODF) **DOCX** e **PPTX** quali documenti prodotti da pacchetto Office 2007 e successivi; **CSV**
Calcolo	**XLSX** (estensione di Excel introdotta con la versione 2007 di Microsoft Office. Si tratta di un file XML compresso con metodo ZIP)
Immagini	**TIFF** (Tagged Image File Format), formato immagine di tipo raster sviluppato da Aldus (assorbita da Adobe) di tipo G4; **TIF** **JPG** **JPEG**
Suoni	**Mp3 compressi in formato Zip**
Video	**Avi compressi in formato Zip**
XML	Extensible Markup Language (XML) è un formato di testo flessibile derivato da SGML (ISO 8879). Su XML si basano numerosi linguaggi standard utilizzati nei più diversi ambiti applicativi.
Archiviazione e compressione	**Zip**
Formati e-mail	**EML**, per i messaggi di posta elettronica, in particolare utilizzato per contenere i messaggi ricevuti/tramessi via PEC
Formati firme	**P7M**, quale standard dei messaggi crittografici utilizzato per i documenti firmati digitalmente **m7m** **tsd** **tsr**

Per effettuare correttamente le operazioni di produzione di un documento amministrativo informatico occorre seguire la seguente procedura:

- redazione del documento con software di videoscrittura o altro (quali ad esempio produzione da applicativi specifici che permettano la produzione di documenti);
- salvataggio del documento (cfr. tavola 1 per la scelta del formato);
- messa a disposizione del documento al firmatario in formato;
- firma digitale del documento;
- acquisizione del documento informatico firmato nel sistema documentale dell'Istituto;
- protocollazione o registrazione particolare.

Completata la redazione, indipendentemente dall'applicazione e dal formato utilizzati, il documento deve essere salvato in formato .PDF .

Il sistema documentale converte automaticamente in formato .PDF i documenti formato word predisposti attraverso gli iter di firma digitalizzati. Tutti gli altri documenti dovranno essere viceversa salvati in formato .PDF prima dell'inserimento nel sistema e la successiva firma digitale.

Il salvataggio in PDF offre le migliori garanzie di corretta visualizzazione al momento dell'apertura, anche tramite software liberamente disponibili, inoltre assicura:

- maggiore stabilità al documento informatico
- migliori garanzie per la sua conservazione e per la validità della firma digitale apposta, in quanto normalmente è privo di macroistruzioni o codici eseguibili (di cui è, comunque, facilmente verificabile la presenza
- migliore leggibilità anche in caso di invio a soggetti terzi.

Si richiede il salvataggio in questo formato anche quando, in casi quali disegni tecnici o riproduzione in immagine di documenti, non sia necessaria l'elaborazione tramite applicativi specialistici.

Inoltre, nel caso siano presenti degli allegati, è bene convertire anch'essi in formato pdf, a meno che non si tratti di modelli o file che il destinatario debba compilare, completare o su cui debba intervenire in qualche modo. In questo caso, debbono essere spediti i file corrispondenti, nel loro formato originale.

Si sottolinea che solo nei casi in cui vengano rispettate le suddette procedure e formati (individuati dal conservatore certificato), il documento originale è documento informatico, acquisito nel sistema documentale tramite la registrazione di protocollo o tramite altra registrazione particolare, e che, come tale, sarà conservato in futuro nel fascicolo e nell'archivio Istat, tramite il trasferimento al sistema di conservazione dei documenti informatici.

3. L'apposizione di firme e la gestione delle informazioni sui documenti firmati

La firma digitale si basa sul metodo della crittografia a chiave asimmetrica:

- privata, da parte del mittente che utilizza la funzione di cifratura per generare una informazione che associata al messaggio ne garantisce la provenienza;
- pubblica, da parte dei destinatari che possono verificarne la provenienza.

La firma digitale viene realizzata tramite tecniche crittografiche a chiave pubblica insieme all'utilizzo di particolari funzioni matematiche, chiamate funzioni hash unidirezionali.

Il processo di firma digitale e quello di verifica della validità di un documento informatico sottoscritto con firma digitale è articolata in tre fasi:

1. **Generazione dell'impronta digitale** ossia calcolare il valore dell'impronta del messaggio (detto hash) applicando un algoritmo di cifratura sull'intero contenuto. L'impronta ha una lunghezza fissa (20 caratteri), indipendentemente dalle dimensioni dell'originale e due proprietà fondamentali:
   a. unidirezionalità, ossia dato x è facile calcolare f(x), ma data f(x) è computazionalmente difficile risalire a x.
   b. assenza di collisioni (collision-free), ossia a due testi diversi deve essere computazionalmente impossibile che corrisponda la medesima impronta.

L'impronta è unica, nel senso che modificando anche un solo carattere del testo si otterrà un'impronta diversa.

2. **Generazione della firma**, consiste nella cifratura con la chiave privata dell'impronta digitale generata in precedenza. In questo modo la firma risulta legata, da un lato (attraverso la chiave privata usata per la generazione) al soggetto sottoscrittore, e dall'altro (per il tramite dell'impronta) al testo sottoscritto. Mediante un software specifico, nel nostro caso quello di InfoCert, al sistema crittografico adottato, si genera una coppia di chiavi da utilizzare: una, che verrà mantenuta segreta, per l'apposizione della firma; l'altra, destinata alla verifica, che verrà resa pubblica.

3. **Apposizione della firma,** consiste nell'aggiunta al documento originale della firma digitale – generata precedentemente – in una posizione predefinita, normalmente alla fine del testo del documento e nella creazione della busta crittografica con l'aggiunta del certificato qualificato del sottoscrittore.

Al destinatario vengono spediti: il documento con la "firma digitale" in calce e il certificato rilasciato dalla competente autorità di certificazione a garanzia della titolarità della chiave pubblica necessaria per decriptare la firma digitale.

Il successivo **processo di verifica** è articolato in quattro fasi:

1. Separare dal messaggio ricevuto la firma digitale. Il destinatario procederà all'apertura e/o verifica dello stesso mediante il proprio software per l'attività di firma. Il programma acquisirà dal certificato annesso al documento firmato, la chiave pubblica del mittente.
2. Decifrare la firma digitale con la chiave pubblica del mittente ottenendo così il valore di hash ricevuto ossia l'impronta del documento
3. Applicare al documento originario lo stesso algoritmo di cifratura utilizzato per il calcolo dell'impronta sull'intero contenuto del messaggio ricevuto ottenendo così il valore di hash calcolato;
4. Confrontare il valore di hash ricevuto con quello calcolato: se coincide con quella decrittata del mittente allora sarà sicuro dell' integrità e provenienza del documento. Se sono identici, la verifica ha avuto esito positivo, altrimenti l'esito è da considerare negativo ed il documento deve essere

rifiutato. Con l'ultimo passo, oltre al mittente, il destinatario verifica anche l'integrità del messaggio.

Il processo di verifica della firma è preceduto da quello di **controllo di validità del certificato** del sottoscrittore.

Un certificato qualificato si può ritenere valido se sono eseguiti e superati i seguenti controlli:

- La validità della firma digitale del certificatore che ha emesso il certificato;
- La data di scadenza ,presente all'interno del certificato, della validità del certificato stesso;
- La non presenza del certificato nella lista dei certificati revocati/scaduti (CRL/CSL), emessa ed aggiornata dal certificatore.

Il superamento di tali controlli è prerequisito perché siano eseguiti i successivi controlli di autenticità e di integrità del messaggio precedentemente descritti.

4. La gestione delle informazioni aggiuntive sui documenti firmati digitalmente

Un documento sottoscritto con firma digitale, come precedentemente illustrato, ha nel nostro ordinamento piena efficacia giuridica, a condizione che non sia modificato dopo l'apposizione della firma. Ci sono però dei casi in cui è necessario apporre più firme su uno stesso documento oppure aggiungere dei dati dopo la sottoscrizione, ad esempio, allo scopo di riportare gli estremi della segnatura di protocollo di un documento spedito o ricevuto dall'Istituto.

Gli standard europei[6] prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi CadES, PadES e XadES, modalità di sottoscrizione adottate anche in Italia. Nella Tavola 2 sono riepilogate le principali caratteristiche dei tre standard.

Tavola 2. Formati standard di firma digitale

Formato	Principali caratteristiche
CadES	La "busta crittografica" assume un'estensione ".p7m", il cui contenuto è visualizzabile solo attraverso idonei software in grado di "sbustare" il documento sottoscritto digitalmente. Tale formato permette di sottoscrivere qualsiasi tipo di file, ma presenta lo svantaggio di non consentire di visualizzarlo in modo agevole. Infatti, è necessario utilizzare un'applicazione specifica che deve essere fornita od indicata dai certificatori che rilasciano certificati qualificati. Nell'ipotesi in cui si intenda riportare sul documento delle annotazioni successive alla sottoscrizione (ad esempio i dati della segnatura di protocollo), sarà necessario esportare il documento nel formato originario, ossia non firmato, per apportarvi le annotazioni. In caso contrario, tali modifiche, infatti, sarebbero apportate nell'unica versione del documento presente all'interno della busta CadES, operazione questa che renderebbe le firme invalide. E' evidente il limite di questa tipologia di firma. Nell'esempio fatto, si avrebbero due documenti: uno con la firma digitale del sottoscrittore del documento ma incompleto, l'altro con la segnatura di protocollo ma privo della firma digitale del sottoscrittore.
XadES	E' utilizzato per consentire la sottoscrizione di documenti generati in XML (eXtended Markup Language). Diffuso in seguito alla direttiva n. 1999/93/CE, rappresenta una specializzazione della XML-Signature in quanto standard per la sottoscrizione elettronica dei documenti in formato XML. La caratteristica di questa tipologia di firma è che, seguendo la struttura del linguaggio utilizzato, è possibile firmare anche solo una parte del documento invece che l'intero file (a differenza del CadES) in tal modo consentendo di aggiungere nuovi campi o file lasciando inalterati i marcatori del documento precedentemente firmati.

[6] Decisione della Commissione europea 2011/130/EU.

PadES	E' basato sullo standard ISO/IEC 32000 e conforme alle specifiche ETSI TS 102 778. La firma digitale è un file con estensione .pdf, leggibile con i comuni "reader" disponibili per questo formato. Nota come "firma PDF", prevede diverse modalità per l'apposizione della firma, a seconda che il documento sia stato predisposto o meno ad accogliere le firme previste ed eventuali ulteriori informazioni, e rende il documento più facilmente accessibile, consentendo di firmare solo documenti di tipo PDF. Il formato PadES presenta alcuni particolari vantaggi, quali la possibilità di visualizzare "graficamente" il punto del documento in cui la firma è inserita, e gestire diverse versioni del documento senza invalidare le sottoscrizioni precedentemente apposte. Ulteriore peculiare caratteristica è che il documento sottoscritto coincide con il documento originario, nel senso che sono un unico file. Tale caratteristica rende questo formato particolarmente idoneo anche nel caso in cui si renda necessario apportare delle modifiche al documento dopo averlo sottoscritto, ad esempio per riportarvi delle annotazioni, come i dati degli estremi di protocollo che sono disponibili solo successivamente alla sottoscrizione del documento stesso.

Il formato adottato dall'Istat per la sottoscrizione dei documenti informatici il PadES.

5. La firma digitale adottata in Istat

L'Istat ha adottato la firma digitale remota, un sistema innovativo di firma digitale che consente di firmare qualsiasi documento informatico senza l'utilizzo di Token USB o Smart Card da collegare al PC, pur garantendone lo stesso grado di sicurezza e gli stessi effetti di legge.

La "**firma digitale remota**" è infatti una tipologia di firma digitale, fruibile via rete (Internet), nel quale la chiave privata del firmatario viene conservata assieme al certificato di firma, all'interno di un server remoto sicuro (basato su un HSM – *Hardware Security Module*) da parte di un certificatore accreditato. Con questa soluzione l'utente non possiede fisicamente il dispositivo di firma, ma utilizza un dispositivo remoto (l'HSM), su cui sono utilizzate le chiavi crittografiche necessarie per la generazione della firma digitale.

L'accesso al dispositivo è sempre protetto da adeguate credenziali di sicurezza.

Il principio di conoscenza è garantito dalla necessità di conoscere un PIN (anche una userid e password), e quello di associare anche un terzo fattore di "conferma temporale", quale un OTP password (*One Time Password*) che possa certificare l'effettiva "data di firma". , I generatori di password "usa e getta" (OTP) sono dunque la soluzione per assicurare l'effettivo "istante di firma", soprattutto se associato al proprio telefono cellulare (talvolta associati alla SIM telefonica).

L'uso del telefono cellulare arricchisce la sicurezza per due ragioni. Eventuali tentativi di attacchi dovrebbero essere portati a termine contemporaneamente sulla rete internet e sulla rete di telefonia mobile; l'esperienza insegna che può trascorrere molto tempo prima che un utente si accorga di non possedere più la smartcard o il token di firma, mentre dopo pochi minuti si accorge di aver smarrito il proprio cellulare.

Il meccanismo di utilizzo della OTP password può avvenire sia via SMS che generando una password randomatica mediante una "App" installata sul proprio smartphone.

La firma digitale remota ha l'ulteriore valore aggiunto di essere sotto il controllo del certificatore che custodisce il dispositivo HSM. Il certificatore quindi sa quando un determinato soggetto genera una firma digitale (la segretezza dell'oggetto della firma è comunque garantito). Ciò consente di poter comunicare

all'utente lo storico dei suoi documenti firmati, su base giornaliera. Tale servizio, di particolare interesse, consente di avere un avviso ogni volta che una firma digitale remota è generata (su base giornaliera).

Il servizio di Firma Digitale Remota adottato dall'Istat, ed erogato dal certificatore accreditato Infocert S.p.A, è completamente integrato con il sistema documentale adottato dall'Istituto, mediante l'utilizzo di apposite "librerie software".

I titolari della Firma Digitale Remota, potranno firmare documenti digitali Istat anche al di fuori del sistema documentale, utilizzando il software di firma Dike6, fornito dal Certificatore Infocert .

Sarà possibile utilizzare tale software su svariati sistemi client (Personal Computer): Windows based, Mac OS, Linux Ubuntu e alcuni sistemi mobili di tipo Android (SmartPhone e tablet) e Osx (iPhone e iPad).

In fase di firma sono richiesti all'utente:

1. **Username** = assegnato in fase di attivazione della firma remota e non è modificabile dall'utente.
2. **Password** = rilasciata e consegnata in fase di attivazione della firma remota e deve essere modificata al primo accesso. In genere i software di firma permettono di memorizzare username e password in modo tale che non vengano richieste ogni volta.
3. **PIN** = codice numerico di 8 cifre rilasciato in fase di attivazione e deve essere modificato al primo accesso. In caso di smarrimento o dimenticanza dovrà essere annullato il certificato di firma e rilasciato un nuovo certificato.
4. **OTP** (One Time Password) = codice numerico inviato tramite SMS o generato tramite APP, valido per un solo processo di firma.

Le modalità di funzionamento della firma remota con riferimento ai documenti dell'Istituto sono illustrate **nell'allegato 2**.

Oltre al sistema di firma digitale del singolo documento, ai sensi del CAD, sono stati previsti altri due sistemi di firma digitale: firma multipla e firma automatica.

La firma multipla, già integrata nel sistema documentale, consente di firmare contestualmente una pluralità di documenti specificatamente selezionati dal titolare del certificato di firma.

La firma digitale automatica consente di firmare in maniera massiva tutti i documenti di un unico flusso ed aventi il medesimo contenuto, es. fatture, mandati di pagamento, informative ai rispondenti.

Parte 2 – Modalità organizzative

6. Ambiti di applicazione

Nell'ambito delle attività di produzione e diffusione dell'informazione statistica, di erogazione dei servizi tecnici e gestione delle funzioni amministrative dell'Istituto, i documenti da inviare all'esterno o all'interno, le delibere e gli altri atti amministrativi di rilevanza interna ed esterna dell'Istituto devono essere firmati digitalmente.

I documenti firmati digitalmente sono inviati tramite PEC. Nel caso in cui il destinatario sia sprovvisto di domicilio digitale, ai sensi del co. 4bis dell'art. 3bis del CAD, l'Istat può, per posta ordinaria o raccomandata A.R., copia analogica dei documenti sottoscritti con firma autografa, sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39.

Il documento informatico ricevuto da un ente o soggetto esterno o spedito dall'Istat ad un ente o soggetto esterno deve essere protocollato mediante il sistema del protocollo informatico ed includere la segnatura di protocollo che può contenere tutte le informazioni di registrazione del documento. Inoltre, se l'invio è verso un'altra amministrazione pubblica, il documento informatico deve essere obbligatoriamente sottoscritto con firma digitale.

7. Soggetti coinvolti

Agiscono nel processo di assegnazione e gestione dei dispositivi di firma digitale:

a. **l'Istat**, in qualità di "terzo interessato", richiede il rilascio del certificato a favore del titolare, fornisce informazioni e certificazioni per ciò che attiene alle deleghe, al ruolo e alle funzioni istituzionali dei dipendenti eventualmente da riportare sul certificato ed ha la facoltà, ai sensi dell'art. 36, comma 1, lettera c) del Codice, di richiedere la sospensione o la revoca del certificato;
b. **L'autorità di certificazione**, nella duplice funzione di responsabile del rilascio, della pubblicazione e della tenuta del certificato, nonché di responsabile della identificazione della persona che fa richiesta della certificazione. Il certificatore individuato dall'Istat è **InfoCert S.p.a.**;
c. **Il titolare**, inteso come il dirigente dell'Istat o il soggetto al quale, per disposizione del Direttore Generale, adottata anche in ragione del ruolo istituzionale e della funzione di cui egli è investito, sia assegnato il certificato per la firma digitale;
d. l'**Ufficio di Registrazione** (RAO) ISTAT, collocato nella Direzione centrale per le tecnologie informatiche della comunicazione i cui compiti sono regolati da una specifica convenzione stipulata con l'Ente Certificatore;
e. **Gli incaricati dell'Ufficio di Registrazione**, d'ora in avanti denominati "incaricati di firma", sono individuati e nominati dal Direttore DCIT e responsabili, su delega del Certificatore, dell'identificazione dei richiedenti, dell'attivazione delle procedure di emissione, revoca o sospensione dei certificati e della consegna di dispositivi e codici per l'utilizzo del servizio di firma digitale.

7.1 Compiti e responsabilità del Certificatore

Le responsabilità dell'Autorità di certificazione (Certificatore) sono sancite dall'art. 30, comma 1 del CAD.
Nel rispetto del disposto dell'art. 32, comma 3 del CAD, ai fini delle presenti Linee Guida, il Certificatore, così come previsto nel contratto di fornitura, ha i seguenti obblighi:

a. identificazione della persona a cui rilasciare il certificato, restando il Certificatore responsabile di detta identificazione anche quando effettuata materialmente da terzi, su delega del Certificatore medesimo;
b. attivazione della procedura per il rilascio del certificato
c. attivazione della procedura per la revoca o la sospensione del certificato;
d. rilascio, pubblicazione e tenuta del certificato nel rispetto delle regole tecniche di cui all'art. 71 del Codice e nel rispetto della normativa in materia di tutela della privacy;
e. conformità delle informazioni contenute nel certificato a quelle previste nell'art. 28 comma 1 del Codice, ad esclusione dell'uso dello pseudonimo;
f. impostazione dell'informazione relativa al nome dell'organizzazione di cui fa parte il titolare con la denominazione "Istituto Nazionale di Statistica";
g. accettazione delle comunicazioni riguardanti il modificarsi o il venir meno delle informazioni inserite nel certificato, ai sensi del citato art. 28 del Codice, richieste esclusivamente dall'Istat;
h. tempestiva pubblicazione della revoca e della sospensione del certificato, con riferimento ai casi di cui al successivo par. 15;
i. tenuta della registrazione di tutte le informazioni relative al certificato dal momento della sua emissione per un periodo di almeno venti anni.

7.2 Obblighi dei titolari del certificato di firma digitale

Il titolare del certificato di firma digitale è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e ad assicurare la custodia del dispositivo di firma, che egli utilizzerà solo personalmente e per ragioni istituzionali.

Il titolare è tenuto ad informare immediatamente gli incaricati di firma di ogni circostanza che, ai sensi del successivo art. 14 renda necessaria o comunque opportuna la revoca o la sospensione del certificato e del dispositivo di firma a lui assegnati; deve altresì informare tempestivamente gli incaricati di firma di eventuali richieste di revoca o di sospensione che egli, per necessità o urgenza, abbia inoltrato direttamente al Certificatore.

7.3 Compiti e responsabilità degli incaricati di firma

Gli incaricati di firma provvedono a:

a. gestire e aggiornare gli elenchi dei titolari di certificato,
b. svolgere l'attività istruttoria interna necessaria affinché il Certificatore soddisfi le richieste di assegnazione, di revoca o di sospensione dei certificati, comprensiva degli adempimenti, per conto dell'Istat, per la tutela dei dati personali dei titolari dei certificati, ai sensi del d.lgs. 196/2003;
c. fornire istruzioni ai titolari sul corretto utilizzo del servizio di firma digitale.

Gli incaricati di firma sono inoltre formalmente delegati dal Certificatore a svolgere i seguenti adempimenti:

1. identificare le persone fisiche all'atto della registrazione, in ottemperanza a quanto disposto dalla normativa vigente in materia di tutela dei dati personali;
2. consegnare a ciascun titolare il dispositivo sicuro di firma ed i codici riservati.

I compiti degli incaricati di firma sono descritti analiticamente nella Convenzione che l'Istat, a seguito di stipula di contratto di fornitura di certificati, ha sottoscritto con il Certificatore, in linea con il manuale di gestione del servizio dovuto dal Certificatore medesimo.
In detto manuale d'uso interno sono descritte nel dettaglio le modalità operative di erogazione e di fruizione del servizio di firma digitale, coerentemente con l'elenco delle principali fasi procedimentali riportato nell'allegato 1, che è parte integrante delle presenti linee guida.
I contratti di fornitura di certificati devono prevedere espressamente la delega dal Certificatore agli Incaricati di firma.

8. Rilascio, revoca e sospensione del dispositivo di firma

In fase di prima applicazione delle presenti Linee Guida, i certificati da utilizzare per la sottoscrizione in forma elettronica dei documenti informatici sono assegnati ai responsabili delle strutture organizzative di I livello (Presidenza, Direzione Generale, Dipartimenti, Direzioni Centrali), e II livello (Servizi) e le strutture dotate di specifica autonomia con autonomia (Responsabile della prevenzione della corruzione e della trasparenza, Responsabile dei Procedimenti Disciplinari, ecc.).

A regime i certificati saranno rilasciati a tutti i dipendenti a cui è conferito, in virtù di uno specifico incarico, un potere di firma (es. RUP, Economo, Cassiere, Consegnatario dei beni).

La revoca di un certificato determina la cessazione anticipata della sua validità e può intervenire su iniziativa del titolare oppure dell'Istat tramite l'ufficio di registrazione interno (RAO).

8.1 Richieste di revoca dal parte di Istat

La revoca viene richiesta dall'Istat, quale terzo interessato, tramite l'ufficio di registrazione interno al Certificatore tutte le volte che ricorra almeno una delle seguenti cause:

8.1 cessazione del rapporto di lavoro del dipendente per qualunque causa;

8.2 venir meno, per qualunque causa[7], dei requisiti di ruolo, qualifica o funzioni istituzionali che ne motivavano l'assegnazione;

8.3 sospetta falsificazione o abusi.

8.2 Richieste di sospensione da parte del titolare

La sospensione deve essere richiesta dal titolare, al certificatore previa informativa all'Istat tutte le volte che ricorra almeno una delle seguenti cause:

a) possibile, anche se non certa, compromissione della chiave privata;
b) sospetta perdita di segretezza del codice di sblocco del dispositivo sicuro di firma;
c) blocco o smarrimento del telefono cellulare.

Ai sensi e per gli effetti dell'art. 36, comma 3, del Codice, la revoca o la sospensione del certificato, qualunque ne sia la causa, hanno effetto dal momento della pubblicazione della lista, rispettivamente, dei certificati revocati o sospesi che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

[7] Compresa l'assenza temporanea per comando o distacco.

9. Limitazioni d'uso del dispositivo di firma

La firma digitale remota adottata dall'Istat è caratterizzata dalla limitazione all'uso ESCLUSIVAMENTE per la sottoscrizione di atti e documenti connessi al ruolo all'interno dell'Istituto ed alle competenze formalmente assegnate. I titolari dovranno pertanto usano il certificato nell'esercizio delle funzioni istituzionali derivanti dal ruolo interno all'Istat. E' vietato l'utilizzo al di fuori dell'ambito istituzionale o per fini personali.

Non è previsto, invece una limitazione in valore e pertanto il certificato di firma potrà essere utilizzato per firmare accordi, contratti o atti giuridici a prescindere dal valore economico del singolo atto.

10. Delega di firma

In assenza di chiarimenti di AgID sul punto, è opportuno far riferimento alle regole in materia di delega amministrativa, previste dalla legge.

La delega di funzioni è un atto amministrativo in cui il delegato agisce in nome proprio e assume la responsabilità degli atti (ordinarie e/o straordinari) che produce. Il delegante non si spoglia della funzione ma solo del suo esercizio. Il delegato, dunque, riceve apposita investitura con atto formale (atto amministrativo informatico) firmato digitalmente dal delegante, e deve dotarsi anch'egli di firma digitale.

Diversamente dalla delega di funzioni, con la delega di firma il provvedimento resta nella sfera di competenza del delegante sotto il profilo dell'imputazione e il relativo regime giuridico è quello proprio degli atti del delegante.

La delega di firma, secondo i giudici amministrativi, a differenza della delega di funzioni, non altera l'ordine delle competenze ma attribuisce al soggetto titolare dell'ufficio delegato (e non all'ufficio oggettivamente considerato) il potere di sottoscrivere atti, i quali continuano ad essere sostanzialmente atti dell'autorità delegante e non di quella delegata"[8].

L'atto di delega deve essere redatto per iscritto[9] e portato alla piena conoscenza degli interessati.
Fuori da apposito atto formale di delega, dunque, valgono le regole generali che prevedono, a seconda dei casi, il c.d. potere di avocazione o il potere di sostituzione.

In caso di assenza/impedimento non prevedibili [10] del titolare del potere di firma ed in mancanza di delega specifica, sono applicate le regole organizzative riepilogate nella Tavola 3.

---

[8] Consiglio di Giustizia Amministrativa per la Sicilia, sentenza n. 182 del 30/5/1995 e, in un obiter dictum, T.A.R. Piemonte, sentenza n. 309 del 17/3/2000. Sul tema la Cassazione ha precisato che "nell'ordinamento amministrativo possono essere individuate una delega di firma ed una di funzioni. Nella prima ipotesi il delegante mantenendo la piena titolarità dell'esercizio di un determinato potere, delega ad altro organo o funzione non titolare dell'organo, il compito di firmare gli atti di esercizio di esso, onde l'atto firmato dal delegato resta imputato all'organo delegante" .

[9] Cons. Stato, sez. V, 30 giugno 1984, n. 540; T.A.R. Campania, sez.1, 10 gennaio 1986, n. 7; Cass. civ., sez. I, 26 aprile 1991, n. 4618.

[10] Il dirigente è considerato assente dal servizio quando non è presente per motivi personali da giustificare (ferie, malattie, congedi di varia natura, ecc.). Sono equiparate alla presenza in servizio le prestazioni fuori sede, comprese le missioni per ragioni di servizio.

Tavola 3. Regole per la firma degli atti in assenza del titolare e mancanza di delega formale

Titolare della firma	Supplente
Presidenza	
Presidente	Membro del Consiglio più anziano
Dirigente tecnico Ufficio di Presidenza	Direttore Generale
Direzione Generale	
Direttore Generale	Dirigente amministrativo di I fascia (Direttore DCRU e in caso di assenza Direttore DCAA)
Dirigente amministrativo di I fascia	Direttore Generale
Dirigente amministrativo di II fascia	Dirigente amministrativo di I fascia
Dipartimenti e direzioni tecniche	
Capo Dipartimento	Presidente e in caso di assenza altro Capo Dipartimento
Direttore centrale	Capo Dipartimento
Direttore centrale (*non inserito in un dipartimento*)	Capo Dipartimento DIPS e in caso di assenza il Capo Dipartimento DIRM o il Direttore Generale
Dirigente tecnico	Direttore centrale
Dirigente ufficio territoriale	Capo Dipartimento DIRM

11. Sistemi di sicurezza

La firma digitale remota adottata dall'Istat è fruibile via rete (Internet) e prevede che la conservazione della chiave privata del firmatario, assieme al certificato di firma, all'interno di un server remoto sicuro (basato su un HSM - *Hardware Security Module*) da parte di un certificatore accreditato.

L'accesso al dispositivo è sempre protetto da adeguate credenziali di sicurezza che prevedono l'integrazione del PIN (anche una userid e password), con un terzo fattore di "conferma temporale", quale un OTP password (One Time Password) associato alla SIM telefonica) del titolare di firma .

Oltre a ciò, il "Dominio di firma" ISTAT è altresì integrato con il servizio di autenticazione forte Safenet/Gemalto, attualmente utilizzato in Istituto per altri servizi, il sistema di OTP integrato è utilizzabile su SmartPhone, di tipo Android, iOS, BlackBerry e Windows Phone e su sistemi operativi client tipo Windows Desktop Client e MAC OS Client.

Per quanto qui non specificamente indicato si rinvia al "DOCUMENTO ANNUALE SULLA SICUREZZA DEI DATI" disponibile sulla intranet dell'Istituto.

12. Trattamento dei dati personali

In base all'art. 4, commi 4 e 5 dell'atto organizzativo generale n. 1 (AOG 1) il Direttore generale, i Direttori di dipartimento e i Direttori centrali, ciascuno per gli ambiti di rispettiva competenza, sono responsabili del trattamento dei dati personali ai sensi del d.lgs. 30 giugno 2003, n. 196. I Direttori di dipartimento e i Direttori centrali, ciascuno per gli ambiti di rispettiva competenza, sono responsabili dei trattamenti di dati connessi alla realizzazione dei processi dei rispettivi uffici; a tal fine, predispongono le misure e curano gli adempimenti necessari affinché i suddetti trattamenti di dati si svolgano secondo i principi e le modalità

stabiliti dalla normativa europea e nazionale, nonché dagli atti di indirizzo tecnico, con particolare riguardo alla tutela del segreto statistico.

Il titolare della firma digitale ed eventuale delegato devono attenersi alle regole e alle prescrizioni indicate nel CAD nell'uso della firma, nonché al rispetto delle disposizioni e delle misure di sicurezza indicate nel Codice in materia di trattamento dei dati personali di cui al d.lgs. n. 196/2003 sopra citato.

Per quanto qui non specificamente indicato si rinvia al "documento annuale sulla sicurezza dei dati" disponibile sulla intranet dell'Istituto.

13. Entrata in vigore

Le presenti linee guida entrano in vigore il **1 gennaio 2018** e potranno essere oggetto di integrazioni e modifiche mediante specifico aggiornamento.

Allegato 1. Definizioni

ALGORITMO DI HASHING	Una firma digitale viene creata facendo passare un documento attraverso un particolare algoritmo, detto di hashing (spezzettamento): il codice prodotto dall'algoritmo, una sorta di "impronta" del documento, viene poi criptato usando la chiave privata di chi spedisce il messaggio. Si tratta di un algoritmo che partendo da un documento di qualsiasi dimensione lo elabora e produce un codice di dimensione fissa. Il metodo di elaborazione è tale che, se il documento venisse cambiato in qualunque sua parte, questo codice cambierebbe. Per esemplificare immaginiamo un algoritmo che calcola il numero di lettere, il numero di parole, la frequenza di ogni lettera ecc.., se cambia una qualsiasi lettera o parola anche il risultato cambia. Dall'impronta non è possibile risalire al documento, però se il documento cambia, anche solo in minima parte, allora cambia anche l'impronta.
AUTORITÀ DI CERTIFICAZIONE/CERTIFICATION AUTHORITY (CA)	Ente che gestisce il rilascio e la revoca delle chiavi per la firma digitale e i certificati digitali contenenti informazioni sul depositario della firma. Una CA può offrire ulteriori servizi, quali ad esempio certificati che attestano la data di un evento o un'avvenuta transazione o elenchi dei nominativi e delle chiavi pubbliche di tutti i suoi iscritti. Struttura/Ente abilitato a rilasciare un certificato digitale tramite procedura di certificazione. La validità dei certificati a chiave pubblica risiede sostanzialmente nella fiducia che la comunità ripone nell'ente che emette i certificati stessi. Le CA sono organizzazioni che, verificata l'identità del richiedente emettono il certificato seguendo standard internazionali e conforme alla normativa europea e nazionale in materia. Il sistema in oggetto utilizza la crittografia a doppia chiave, o asimmetrica, in cui una delle due chiavi viene resa pubblica all'interno del certificato (chiave pubblica), mentre la seconda, univocamente correlata con la prima, rimane segreta e associata al titolare (chiave privata). Una coppia di chiavi può essere attribuita ad un solo titolare.. Viene così autenticata l'associazione utente-chiave pubblica. La CA si preoccupa inoltre di mantenere un archivio delle chiavi pubbliche che sia sicuro, disponibile a tutti e soprattutto protetto da attacchi in scrittura e lettura. Per provare che il certificato è stato emesso proprio da quella determinata CA essa incorpora la sua firma sul certificato stesso (analogamente al timbro del Comune sulla Carta di identità). Tale firma è calcolata criptando il digest del certificato con la chiave privata della CA. I compiti della CA sono: - Identificare con certezza la persona che fa richiesta della certificazione della chiave pubblica; - Rilasciare e rendere pubblico il certificato (firmato con la propria chiave privata); - Mantenere il registro delle chiavi pubbliche; - Procedere alla revoca o alla sospensione dei certificati in caso di richiesta dell'interessato o in caso di abusi, falsificazioni, etc - mantenere aggiornata la lista (pubblica) dei certificati sospesi o revocati; - rispondere (per via telematica) alle richieste di invio dei certificati.

CERTIFICATO	Insieme di informazioni utilizzato per distribuire in modo sicuro le chiavi pubbliche degli utenti. Un certificato definisce con certezza la CA che lo ha emesso nonché il periodo di tempo in cui deve essere utilizzato.
CERTIFICAZIONE	Il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare, si identifica quest'ultimo, si attesta il periodo di validità della predetta chiave e il termine di scadenza del relativo certificato.
CHIAVI ASIMMETRICHE	Coppia di chiavi crittografiche, una pubblica e una privata, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione. Chiave privata Elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.
CHIAVE PRIVATA	Elemento della coppia di chiavi asimmetriche, destinato a essere conosciuto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.
CHIAVE PUBBLICA	Elemento della coppia di chiavi asimmetriche destinato a essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi.
CERTIFICATE REVOCATION LIST (CRL)	Lista conseguente alle operazioni con cui la CA annulla la validità di un certificato da un dato momento, non retroattivo, in poi. Tale elenco è firmato digitalmente dalla CA, periodicamente aggiornato e pubblicato nella Directory.
CONSERVATORE ACCREDITATO	Realtà pubblica o privata la cui attività è quella di conservazione documentale a cui l'Agenzia per l'Italia digitale abbia riconosciuto il possesso dei requisiti di qualità e sicurezza.
CRITTOGRAFIA	Insieme di tecniche e procedure per rendere segreto il testo di un documento e viceversa per rendere leggibile un testo cifrato. La crittografia, o cifratura, è la tecnica fondamentale per la generazione della firma digitale, e viene utilizzata per assicurare la riservatezza, l'autenticazione e il non ripudio delle informazioni archiviate o inviate attraverso reti di computer. Con la crittografia, un messaggio o, più in generale, un qualunque file di dati (testo, immagini, musica, ecc.) è trasformato in un insieme di segni e simboli assolutamente privi di significato per chi non conosca la "chiave" giusta per decifrarli. Il problema cruciale della crittografia è sempre stato la gestione della chiave. Anche il sistema di cifratura più sofisticato non serve a nulla se non si riesce a garantire la segretezza della chiave. Da questo punto di vista, si parla di due approcci principali alla crittografia: a chiave unica, detto anche a chiave privata o simmetrica; a doppia chiave, detto anche a chiave pubblica o asimmetrica.
CRL Certificate Revocation List – LISTA DEI CERTIFICATI REVOCATI O SOSPESI	E' una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea. Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla lista CRL, che viene

	quindi pubblicata nel registro dei certificati.
DISPOSITIVO DI FIRMA	È uno dei possibili supporti di memorizzazione della chiave privata del titolare del certificato (protezione software/hardware con password stabilita dall'utente). Tali dispositivi sono, ad esempio, una smart card o un dispositivo hardware (protezione hardware con password digitata solo sulla tastiera del dispositivo).
DOCUMENTO	In archivistica il documento è analizzato e interpretato nella sua funzione e capacità di rappresentare un atto o fatto e di testimoniarne l'esistenza, con efficacia e continuità nel tempo, all'interno di un sistema di sedimentazione documentaria e, quindi, di relazione tra documenti anche al fine di supportare l'esercizio delle funzioni del soggetto produttore (Istat, nel nostro caso). Secondo una definizione classica archivistico-diplomatistica documento è una testimonianza scritta di un fatto di natura giuridica, compilata con l'osservanza di determinate forme, le quali sono destinate a procurarle fede e a darle forza di prova. Il contenuto del documento deve necessariamente rappresentare un atto che crea un diritto; il documento deve essere stilato con forme regolamentate in modo certo, che forniscono credibilità assoluta al documento. L'assenza di uno degli elementi formali mette in dubbio la veridicità e l'autenticità del documento. Il concetto di documento ha subito poi, negli ultimi decenni, una sorprendente evoluzione, parallela a quella dei mezzi di comunicazione. Il concetto di documento, rispetto alla definizione tradizionale, si è dilatato oltre il rapporto con la natura giuridica del suo contenuto, mantenendo però una relazione con la natura funzionale del documento in rapporto al sistema documentario del soggetto produttore, rimanendo pur sempre "strumento e residuo" della sua attività pratica.
DOCUMENTO INFORMATICO	Rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti.
DOCUMENTO AMMINISTRATIVO	Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.
DOCUMENTO AMMINISTRATIVO INFORMATICO	Atto formato dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, che costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge. Si evidenzia che, oltre alla naturale associazione determinata dal termine documento, risultano da includere nei documenti amministrativi informatici anche: - Le registrazione informatica delle informazioni risultanti da transazioni o processi informatici. - I dati derivanti da moduli o formulari presentati tramite strumenti telematici. - Le comunicazioni, istanze e dichiarazioni che pervengono o sono inviate dalla casella di posta elettronica certificata dell'Amministrazione pubblicata sull'Indice della Pubblica Amministrazione - I dati e le informazioni scambiate tra Pubbliche Amministrazioni in

	modalità cooperazione applicativa.
FIRMA DIGITALE	Un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare, tramite la chiave privata, e al destinatario, tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. Solo chi è in possesso della chiave privata avrà accesso ai contenuti di quanto spedito. La firma digitale è una informazione che viene aggiunta ad un documento informatico al fine di garantirne integrità e provenienza. Sebbene l'uso per la sottoscrizione dei documenti formati su supporti informatici sia quello più naturale, essa può essere utilizzata per autenticare una qualunque sequenza di simboli binari, indipendentemente dal loro significato. La principale differenza tra firma autografa e firma digitale sta nel fatto che la prima è direttamente riconducibile all'identità di colui che la appone, poiché la calligrafia è un elemento identificativo della persona, mentre la seconda non possiede questa proprietà. Per ovviare a questa deficienza si ricorre all'autorità di certificazione, il cui compito è quello di stabilire, garantire e pubblicare l'associazione tra firma digitale e soggetto sottoscrittore.
FIRMA DIGITALE REMOTA	La firma remota ottimizza le funzionalità del servizio di firma digitale, rendendo l'utilizzatore completamente libero da qualsiasi vincolo legato all'installazione di hardware. Il certificato utente per la firma digitale risiede su un server remoto sicuro nel quale viene conservata la chiave privata insieme al certificato di firma. La firma avviene mediante accesso al server remoto con username, password e codice OTP.
FORMAZIONE DEI DOCUMENTI INFORMATICI	Processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione di protocollo o ad altre forme di registrazione previste dalla vigente normativa (repertori, registri, etc.).
HASH VALUE	Stringa di caratteri calcolata casualmente a partire da un documento, attraverso un algoritmo segreto. Una volta generata diventa praticamente impossibile ripetere il calcolo per riprodurla. Correlata a un documento, consente di renderlo univocamente identificabile, inalterabile e non replicabile
IMMODIFICABILITÀ	Una delle caratteristiche del documento informatico a norma di legge: esso deve essere non alterabile, nella forma e nel contenuto. Il contenuto del documento informatico non deve essere alterabile nella forma e nel contenuto durante l'intero ciclo di gestione; allo scopo occorre garantire la staticità nella conservazione del documento stesso.
IMPRONTA	Sequenza di bit generata attraverso una funzione di hash.
INTEGRITÀ	Insieme delle caratteristiche di un documento informatico che lo identificano come completo e inalterato.
LDAP - Lightweight Directory Access Protocol	Protocollo utilizzato per accedere alla directory contenente i certificati ed effettuare tutte le operazioni di prelievo certificato, CRL, etc.

MARCA TEMPORALE	Evidenza informatica che consente la validazione temporale. Struttura di dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo (data e ora). In generale, il servizio di marcatura temporale fornito dagli Enti Certificatori, consente di stabilire l'esistenza di un documento informatico prima di un certo istante temporale associando all'evidenza informatica una data e ora certe validandola temporalmente.
NON RIPUDIO	Capacità di un sistema di encryption di rendere impossibile all'autore di un messaggio, o più in generale di un documento elettronico, di disconoscerne la paternità.
OTP - One Time Password	Codice alfanumerico, che viene generato da un algoritmo che crea una serie casuale di numeri, inviati al titolare del rapporto su sms e email (la differenza di canale usato dipende dal tipo di servizio di cui si sta usufruendo). L'acronimo OTP sta a indicare una password "usa e getta" che, a differenza dei codici usati dalle tessere ricaricabili, vengono generati 'al bisogno' dall'apposito software a disposizione.
PKI - Infrastruttura di Chiave Pubblica - Public Key Infrastructure	Insieme di tecnologie, politiche, processi e persone utilizzate per gestire (generare, distribuire, archiviare, utilizzare, revocare) chiavi di crittografia e certificati digitali in sistemi di crittografia a chiave pubblica.
PKCS (Public Key Cryptography Standards)	PKCS è un insieme di standard per la crittografia a chiave pubblica sviluppati dai Laboratori RSA: definiscono la sintassi del certificato digitale e dei messaggi crittografati. In particolare il PKCS#10 definisce la struttura della richiesta per la certificazione della chiave pubblica di una coppia di chiavi asimmetriche; il PKCS#12 descrive una sintassi per il trasferimento di informazioni d'identità personale, tra cui chiavi private e certificati digitali a chiave pubblica, garantendo riservatezza e integrità dei dati trasmessi.
PUK - Personal Unblock Key	Si riferisce ad un numero utile allo sblocco di un dispositivo (ad esempio una smart card o un token USB) nel caso si sia digitato per più volte in modo erroneo il PIN.
REGISTRATION AUTHORITY (RA)	Entità responsabile dell'identificazione e dell'autenticazione dei soggetti della certificazione, ma che non è una CA e, pertanto, non firma né emette certificati. La RA procede al riconoscimento delle persone che si recano fisicamente ai propri sportelli e ne raccoglie dati anagrafici, tipo di servizio, etc., comunicandoli in modalità protetta alla CA.
REGISTRO DEI CERTIFICATI (directory)	Il Registro dei Certificati è un archivio che contiene tutti i certificati validi emessi dal Certificatore per i quali sia stata richiesta dal titolare la pubblicazione e la lista dei certificati revocati o sospesi (CRL).
REVOCA DEL CERTIFICATO	Operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi. Vedi CRL - Lista dei Certificati Revocati o sospesi.
RIFERIMENTO TEMPORALE	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
SISTEMA DI VALIDAZIONE	Sistema informatico e crittografico in grado di generare e apporre la firma digitale o di verificarne la validità.
SOSPENSIONE DI UN CERTIFICATO	E' l'operazione con cui il Certificatore sospende la validità del certificato per un determinato periodo di tempo. Vedi Lista dei Certificati Revocati o Sospesi - CRL.

TERZA PARTE FIDATA (TTP)	Ente o società che fornisce determinate garanzie (di solito tramite un marchio o un certificato digitale) sulle caratteristiche di un interlocutore di una transazione virtuale (individuo o sito Web).
TITOLARE	La persona fisica identificata nel certificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso; al titolare è attribuita la firma digitale generata con la chiave privata della coppia. La titolarità è stata certificata da un soggetto terzo (Autorità di certificazione/Certification Authority).
UID - Identificatore Univoco del Dispositivo di firma	È il codice associato univocamente al dispositivo di firma al momento della sua personalizzazione
VALIDITÀ DEL CERTIFICATO	Efficacia e opponibilità al titolare della chiave pubblica, dei dati contenuti nel certificato stesso.
VALIDAZIONE TEMPORALE - Time stamping	Il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, un riferimento temporale opponibili ai terzi.

Direzione centrale per le tecnologie informatiche della comunicazione

Allegato 2
Manuale operativo per la gestione della firma digitale d'Istituto.

Versione 1.0

1. Attivazione del dispositivo di firma

La procedura di rilascio si attiva, qualora **l'Istituto** identifichi la necessità del rilascio di un nuovo certificato di firma, sia nel caso di un rilascio ex-novo per un dipendente autorizzato al possesso e all'utilizzo della firma, sia nel caso della sostituzione di una firma digitale in scadenza.

Al fine della registrazione del Certificato di Firma Digitale Remota, il **Richiedente** deve inviare all'indirizzo di posta elettronica dell'**Ufficio di registrazione (**firmadigitale@istat.it) i seguenti dati:

- la scansione di un documento di riconoscimento in corso di validità (a scelta tra Carta D'Identità, Patente di guida, o Passaporto);
- la scansione del Codice Fiscale o della Tessera Sanitaria;
- il proprio numero di cellulare;
- il "Modulo per autocertificazione della residenza" (precedentemente ricevuto via mail dall'Ufficio di Rgistrazione) debitamente compilato e firmato.

Per conto di InfoCert, gli **incaricati dell'ufficio di Registrazione**

12. identificano il Richiedente;
13. validano la richiesta di **registrazione** del certificato;
14. inviano la "busta virtuale", una mail contenente le credenziali necessarie nella procedura di attivazione del certificato del Richiedente/Titolare;

Dopo la registrazione, il Richiedente/Titolare dovrà restituire all'**Ufficio di Registrazione** l'originale della richiesta di registrazione e certificazione firmato, conservandone la copia.

Il **Richiedente/Titolare** riceverà dagli indirizzi **elaborazione.certificati@infocert.it** e **codici.firmadigitale@infocert.it** due mail con le istruzioni per l'attivazione del Certificato di Firma Digitale e con il link per aprire la busta cifrata contenente il PIN di Firma, il codice PUK ed il numero di busta relativo alla sua Firma Digitale. La password per aprire la busta virtuale cifrata è costituita dal codice fiscale del Titolare in lettere MAIUSCOLE.

Seguendo il link https://mysign.infocert.it/ncfr/#/login , presente nella mail, il Titolare potrà accedere con le credenziali indicate nelle mail stessa, alla procedura di attivazione.

Le credenziali sono un UserID (NGIFR + tre cifre numeriche, come indicato nella mail) e una Password (ncfr0101 – valida solo per il primo accesso)

La procedura di attivazione prevede, in prima istanza, la personalizzazione della password (che contenga caratteri maiuscoli e minuscoli, cifre numeriche e caratteri speciali) e, in seconda istanza, la personalizzazione del PIN, ossia un codice esclusivamente numerico e composto da un numero di 8 cifre che associato a un Certificato di Firma permette di verificare se la persona che lo utilizza sia effettivamente autorizzata a compiere quella operazione. Il PIN viene generato la prima volta in fase di registrazione del certificato e deve essere necessariamente modificato e ricordato con attenzione.

Se questo PIN viene smarrito o dimenticato, non sarà possibile recuperarlo e sarà necessaria la revoca del Certificato di Firma Digitale e conseguentemente una nuova attivazione.

Terminata la procedura di attivazione, il Titolare potrà firmare digitalmente i documenti all'interno del sistema di gestione documentale oppure mediante il software Dike6, utilizzando PIN e Password impostati precedentemente e il codice OTP generato di volta in volta.

Credenziali	Formato	Uso
USER ID	NGIFR + "TRE CIFRE NUMERICHE" (Assegnato da InfoCert e presente sulla ricevuta di Richiesta di Registrazione del Certificato Di Firma Remota).	15. Accesso al portale: https://mysign.infocert.it/ncfr/#/login 16. Acquisizione del Certificato di Firma nel SW Dike6
NOME UTENTE (ALIAS)	Utenza di Dominio Istat. (Usata per l'accesso al proprio PC)	17. Apposizione di Firma tramite il Sistema Documentale Archiflow
PASSWORD	Obbligatoriamente da personalizzare sul portale "mysign", con una stringa contenente maiuscole e minuscole, uno o più numeri e almeno un carattere speciale (&%!"()?^+[].<>,_). Non deve contenere più di due caratteri identici consecutivi. Lunghezza: almeno 8 caratteri.	18. Accesso al portale: https://mysign.infocert.it/ncfr/#/login Password per il primo accesso: ncfr0101 19. Acquisizione del Certificato di Firma nel SW Dike6
PIN	Codice numerico ad otto cifre da conservare con attenzione. Se smarrito, non è possibile reimpostarlo.	20. Apposizione di Firma tramite il Sistema Documentale Archiflow o tramite il SW Dike6
OTP/SMS	Codice numerico ad otto cifre con valenza temporanea. (Trasmesso tramite SMS o tramite l'APP MobilePASS).	21. Acquisizione del Certificato di Firma nel SW Dike6 22. Apposizione di Firma tramite il Sistema Documentale Archiflow o tramite il SW Dike6
PIN dell'applicazione MobilePass Safenet	Codice numerico di 4 cifre, definito dall'utente durante l'installazione dell'applicazione sul proprio smartphone	23. Generazione del codice OTP nella procedura di apposizione di firma, tramite l'APP MobilePASS

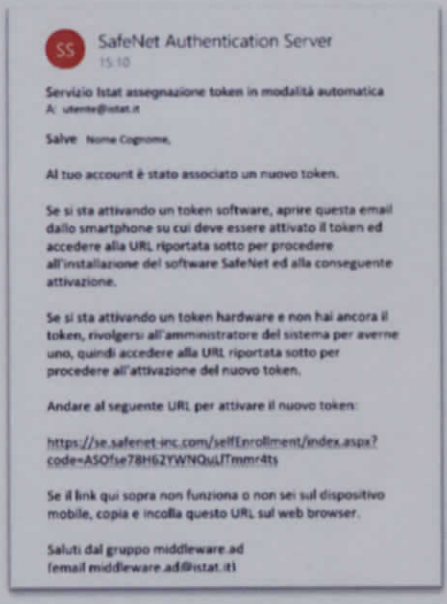
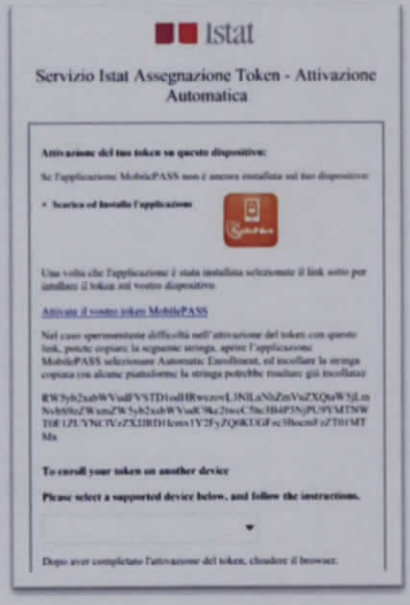
2. Attivazione del servizio OTP di Istat

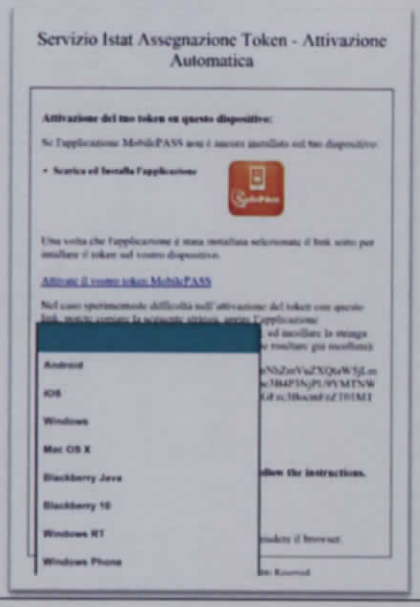
L'One-Time Password – OTP è un codice numerico e rappresenta una password che può essere utilizzata per una singola sessione di accesso o una transazione.
In Istat l'OTP è utilizzato per consentire al personale fuori sede il collegamento alla rete interna tramite un canale di comunicazione cifrato che garantisce la riservatezza delle trasmissioni.
La sicurezza è ulteriormente rafforzata dalla limitazione di accesso alla rete interna alle risorse necessarie per lo svolgimento delle attività di competenza, mentre l'utilizzo delle applicazioni viene realizzato tramite virtualizzazione del client su server dedicati.
Con riferimento alla firma digitale, l'utilizzo dell'OTP certifica la data dell'apposizione della firma sui documenti e garantisce l'autenticità della stessa dato il collegamento al telefono cellulare personale.

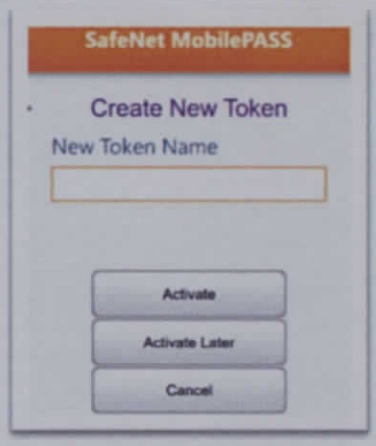
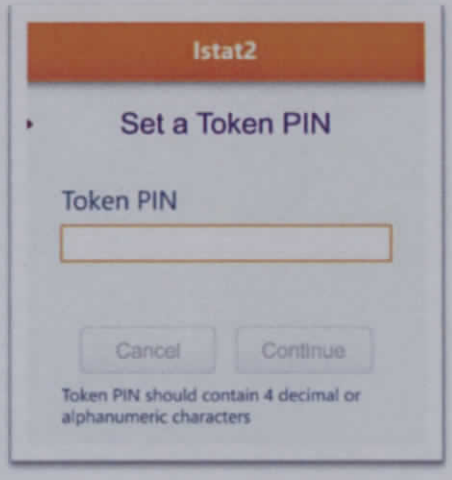
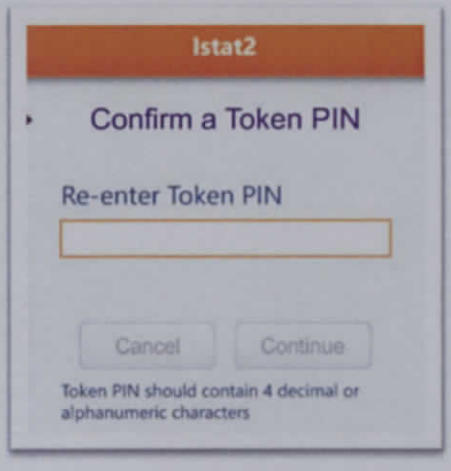
2.1 Scelta del tipo di token per l'accesso alla VDI da rete esterna

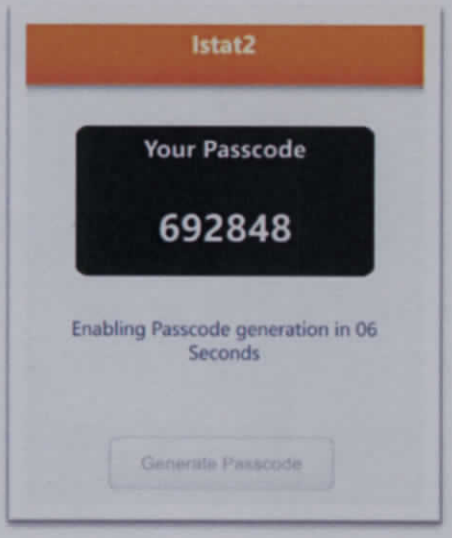
Se si è in possesso di uno smartphone e si vuole attivare un token software aprire l'email inviata dall'indirizzo "SafeNet Authentication Server" <noreply@safenet-inc.com> dal proprio smartphone e seguire la procedura indicata di seguito

2.2 Come scaricare/installare/attivare MobilePASS di Safenet per Smartphone

1. Aprire l'email inviata dall'indirizzo "SafeNet Authentication Server" noreply@safenet-inc.com	
2. Cliccare sul link presente nell'email	

3. Se sullo smartphone non è presente l'applicazione **MobilePass Safenet**, scaricarla selezionando il tipo di sistema operativo come indicato in figura e seguire le indicazioni per l'installazione	
4. Dopo aver installato l'applicazione sullo smartphone, tornare al punto **2.** e cliccare sul link "Attivate il vostro token MobilePASS"	

5. Se viene richiesto assegnare un nome al Token e cliccare su Activate	
6. Definire un PIN di 4 cifre che sarà utilizzato per accedere alla generazione delle OTP (One Time Password) e cliccare su Continue	
7. Ripetere il pin e cliccare su Continue	

8. Quando appare il passcode per accedere alla VDI come in figura il token è attivato	

3. Firma digitale nel sistema documentale

3.1 Firma singola digitale nel sistema documentale dalla rete interna

Il sistema documentale è un sistema non esposto su rete esterna all'istituto, è raggiungibile tramite un browser all'interno della rete istat oppure tramite l'applicativo client installato sulla singola postazione.

I possessori della Firma Digitale Remota ISTAT possono firmare documenti digitali dell'Istituto nel sistema documentale Archiflow secondo le modalità operative riportare di seguito; le modalità saranno illustrate per entrambe le interfacce disponibili per il prodotto.

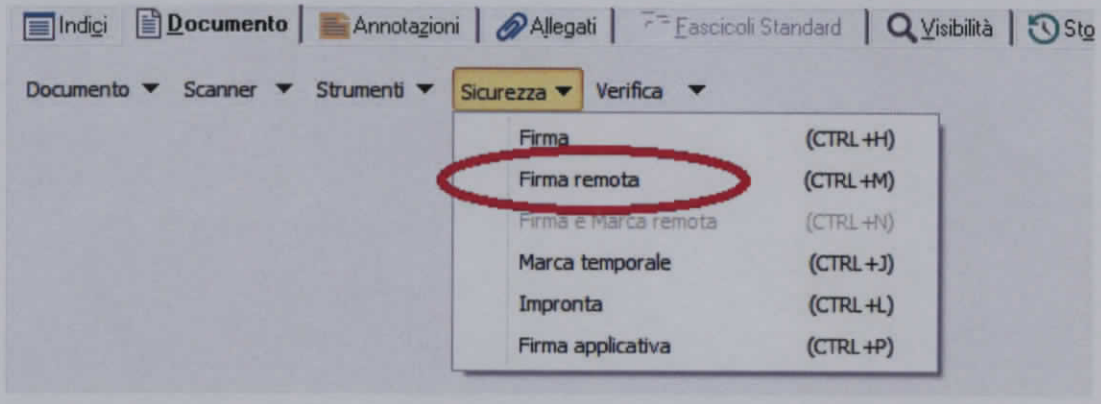
Ogni documento può essere firmato da due percorsi distinti:

a. nella scheda documentale per la quale il documento è stato inserito come principale;
b. dall'elenco rintracciati risultato di una ricerca, in questo caso è possibile firmare contemporaneamente anche più di un documento.

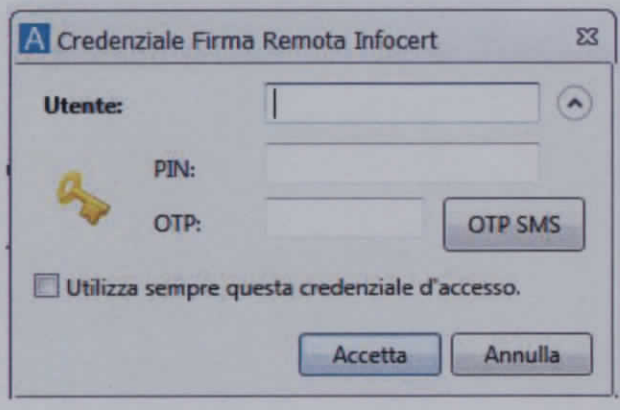
Nel primo caso si accede alla scheda documentale ricevuta via posta interna di Archiflow per l'interfaccia Client o via area Workspace per l'interfaccia Web; dalla scheda documentale è necessario visualizzare l'area relativa al Documento.

Per utilizzare la firma remota il percorso si differenzia a seconda dell'interfaccia:

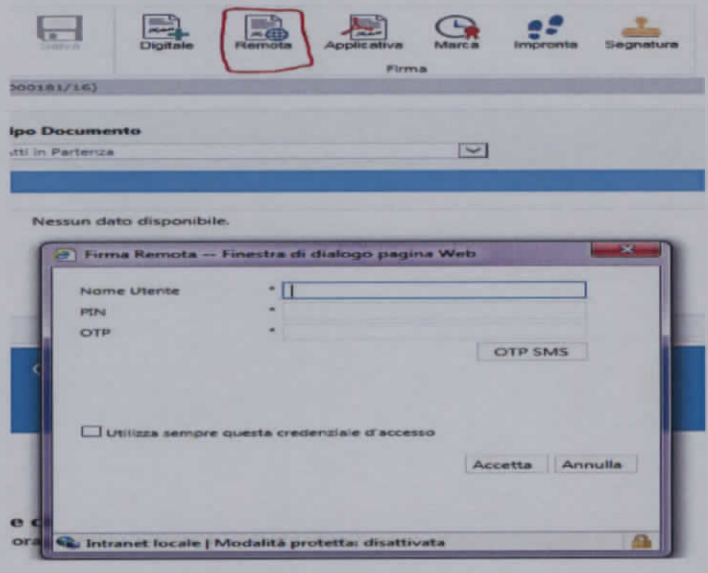
a. **per l'interfaccia client, dal menù Sicurezza fare click su Firma Remota.**



Il sistema richiederà conferma di lettura del documento e presenterà la maschera dove è possibile inserire l'utenza ed il pin della firma remota e l'OTP, se si utilizza l'App, invece se si utilizza il servizio via sms fare click sul tasto "OTP SMS" per ricevere via sms la password temporanea per firmare.

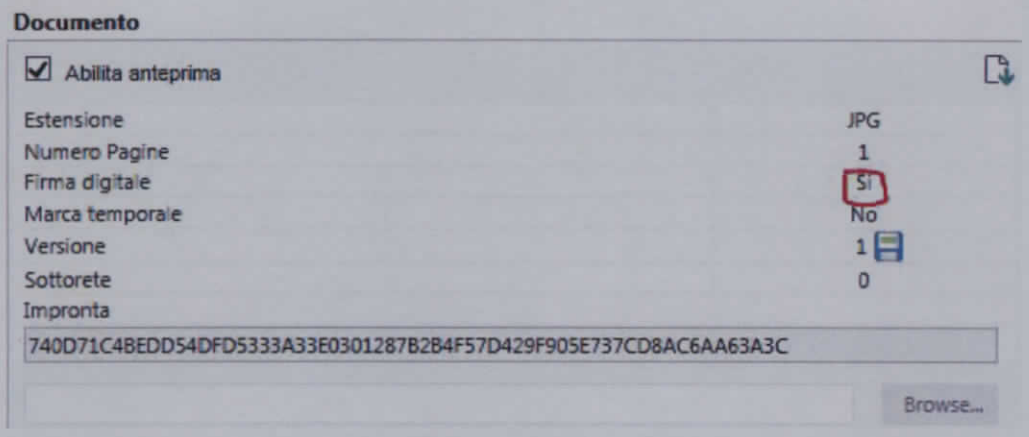


b. **per l'interfaccia web**, dalla barra Operazioni, fare click sull'icona "Remota", il sistema richiederà conferma di lettura del documento e presenterà la maschera dove è possibile inserire l'utenza ed il pin della firma remota e l'OTN, analogamente all'interfaccia Client, se si utilizza il servizio di OTP via SMS, fare click sul pulsante "OTP SMS" e sarà inviato via sms il codice numerico per la password temporanea per la firma.



Per visualizzare la presenza della firma, dall'interfaccia Client l'icona del documento posta in alto a destra riporterà una penna stilizzata

invece dall'interfaccia Web nella tabella riassuntiva delle proprietà del documento l'attributo Firma è positivo.



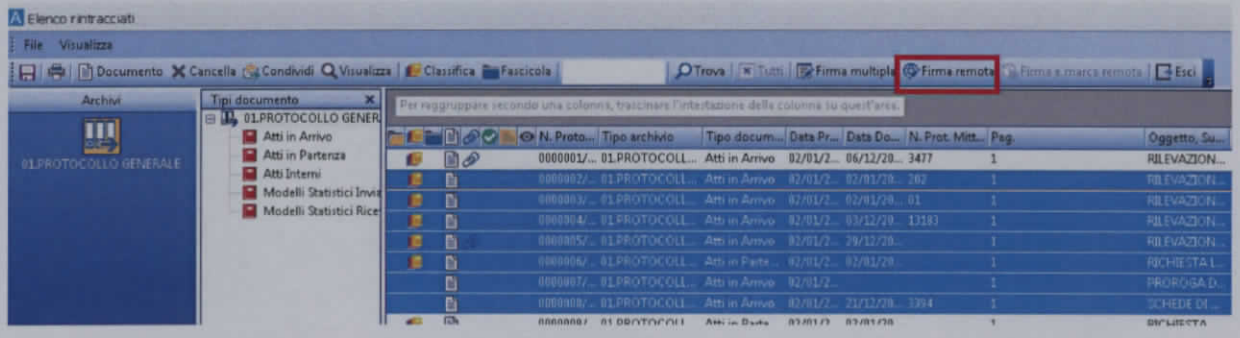
Per firmare il documento dall'elenco dei rintracciati, è necessario selezionare la scheda documentali il cui documento principale deve essere firmato e fare click, sia per l'interfaccia Client sia per l'interfaccia web, sulla voce di Menù Firma Remota. Il sistema ripresenterà lo stesso processo finora descritto.

Se il documento necessità di diverse firme, le successive alla prima saranno registrate seguendo le medesime modalità ed il sistema, prima di permettere la seconda firma, notifica l'utente della presenza di altre firme.

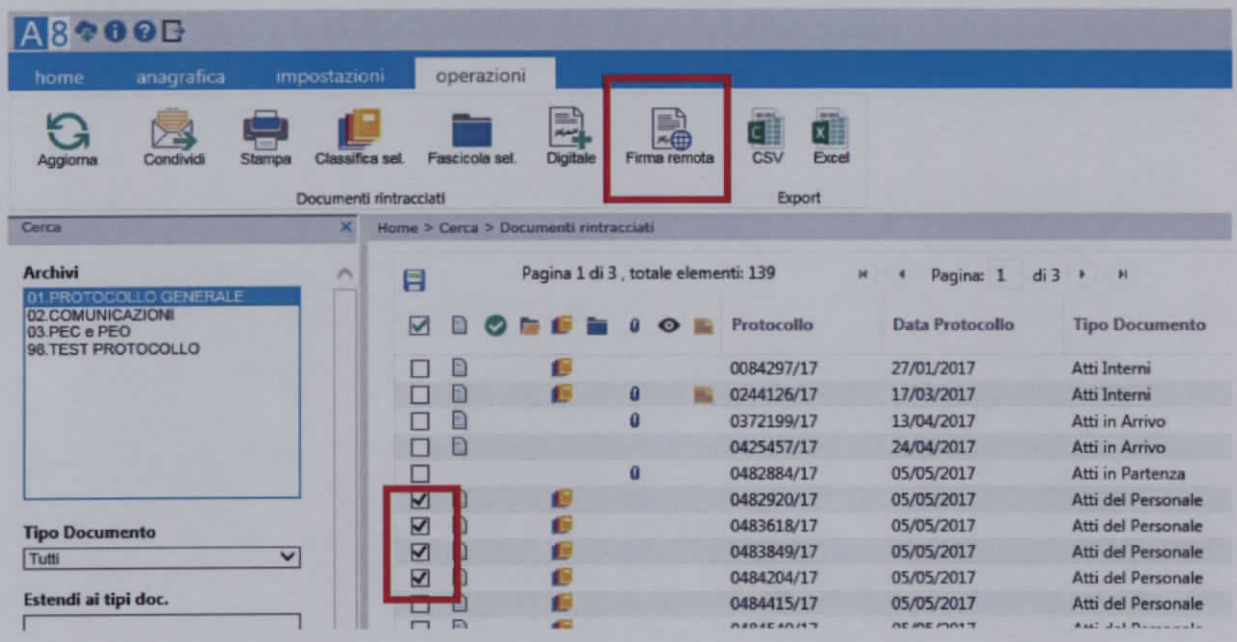
3.2 Firma multipla digitale nel sistema documentale dalla rete interna

E' possibile firmare contemporaneamente diversi documenti utilizzando il sistema documentale, ciò è fattibile dall'elenco dei rintracciati selezionando i documenti che devono essere firmati ed utilizzando il tasto "Firma Remota" posto nella barra funzionale.

Dall'interfaccia client i diversi documenti sono da selezionare utilizzando il tasto Ctrl e la selezione cosi come in figura



Dall'interfaccia web i diversi documenti sono da selezionare il controllo ad hoc cosi come in figura



Il sistema richiede conferma di lettura dei documenti e propone l'identificazione del firmatario come descritto nel paragrafo precedente.

Se per uno dei documenti è riscontrato un errore qualsiasi, è mostrato il messaggio di errore e saranno firmati soltanto i documenti per i quali non si riscontra nessun errore.

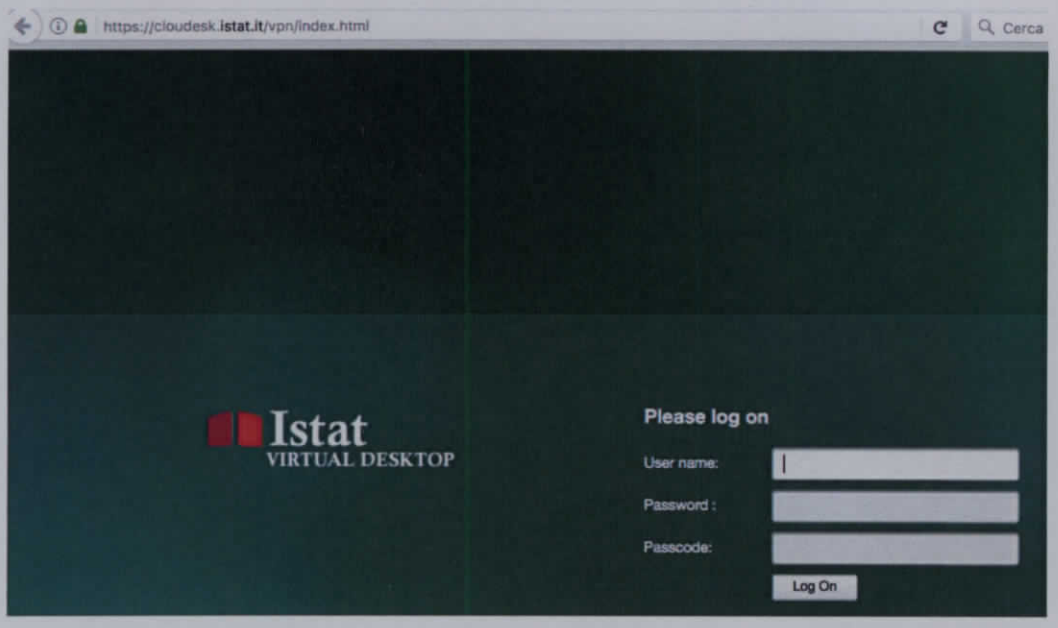
3.3 Firma digitale nel sistema documentale dalla rete esterna

Per accedere al sistema documentale dalla rete esterna, gli utenti già abilitati all'ambiente di "SmartWorking" (VDI - Infrastruttura di Desktop Virtuale) potranno accedere in modalità semplice e sicura alle risorse informatiche dell'Istituto, quindi anche al sistema documentale; nessuna attivazione necessaria per questo tipo di utenti, per loro sarà sufficiente usare l'applicazione Archiflow presente all'interno della medesima postazione virtuale.

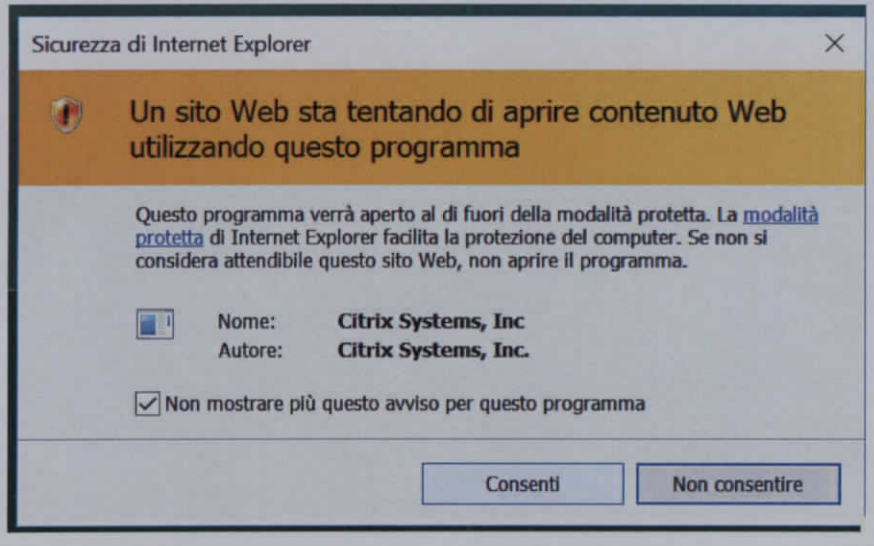
Gli utenti non ancora in possesso di una postazione virtuale ne dovranno richiedere l'utilizzo.

Un requisito necessario per l'accesso dall'esterno all'Istituto è scaricare, installare ed attivare (una tantum) una app sul proprio smartphone che possa generare sequenze di numeri casuali. Il software di riferimento è MobilePASS di Safenet, medesimo software per la firma in caso di scelta OTP e la cui installazione è illustrata nel paragrago 2.

Quindi potranno accedere alla rete interna istat dall'esterno, aprendo un browser dalla propria postazione esterna ed *digitando* l'indirizzo https://cloudesk.istat.it, utilizzando l'utenza e password di dominio e il passcode ottenuto dall'app installata sullo smartphone.



Soltanto la prima volta che si accede, sarà richiesto, dopo aver inserito le credenziali, di consentire l'installazione di un plugin, CitrixReceiver, cosi come mostrato in figura.



Per l'installazione del plugin i passi in sintesi dovranno essere Install->Esegui->Consenti->Finish->Consenti.

Infine per utilizzare l'applicazione del sistema documentale, si dovrà fare clik sul segno + alla sinistra della finestra, scegliere "All Application" ed aggiungere l'app "Archiflow ClientWeb", sul desktop virtuale sarà disponibile l'applicazione cosi come all'interno della rete istat; per chiudere l'applicazione si dovrà utilizzare la sequenza di tasti Alt+F4.

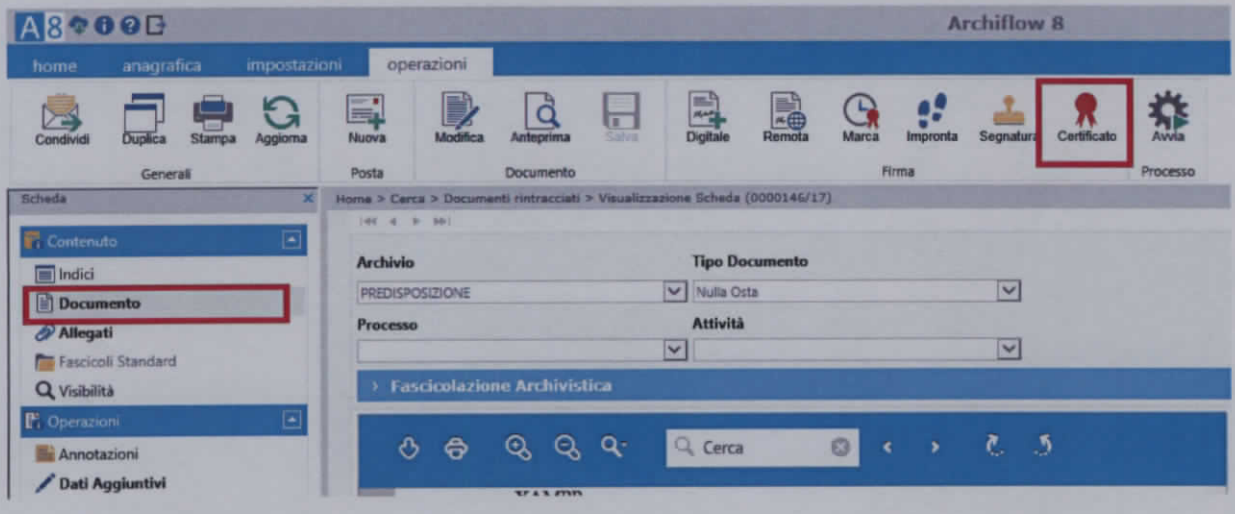
Si ricorda che non sarà possibile movimentare file tra il proprio dispositivo e l'applicazione del documentale.

3.4 Verifica firma digitale nel sistema documentale

Dall'interfaccia web del sistema documentale è possibile verificare le firme di tipo CAdES, ovvero le firme su file diversi dalla tipologia pdf, in quanto per questi ultimi la verifica della firma è possibile tramite il software di lettura del file, ovvero Acrobat Reader.

La differenza della tipologia di firma di un documento, ovvero CAdES o PAdES, è visualizzata dall'elenco dei rintracciati dall'interfaccia web del sistema documentale dal diverso colore della penna stilizzata, è utilizzata l'immagine rossa per la firma di tipo PAdES , l'immagine blu per la firma di tipo CAdES .

Quindi per verificare un file firmato secondo il formato CAdES, è sufficiente accedere alla scheda documentale contenente il file firmato, attivare l'area Documento e fare click sulla voce di menù Certificato, posizionata nella barra relativa alla "Firma", come evidenziato nella figura successiva.



4. Gestione della firma extra sistema documentale

I possessori della Firma Digitale Remota ISTAT possono firmare documenti digitali dell'Istituto anche al di fuori del sistema documentale, utilizzando il software di firma Dike6, fornito dal Certificatore Infocert.

Il software di firma Dike6, fornito dal Certificatore Infocert, può essere utilizzato su svariati sistemi client (Personal Computer): Windows based, Mac OS, Linux Ubuntu e alcuni sistemi mobili di tipo Android (SmartPhone e tablet) e OSx (iPhone e iPad).

Terminata la fase di attivazione della Firma Digitale Remota ed installato correttamente il software dike6 (scaricabile al link https://www.firma.infocert.it/installazione/software.php), come da manuale, si potrà iniziare ad usare la propria firma digitale remota (vedi breve video https://www.youtube.com/watch?v=kXf70YVvgAQ#action=share), secondo le modalità operative di seguito descritte.

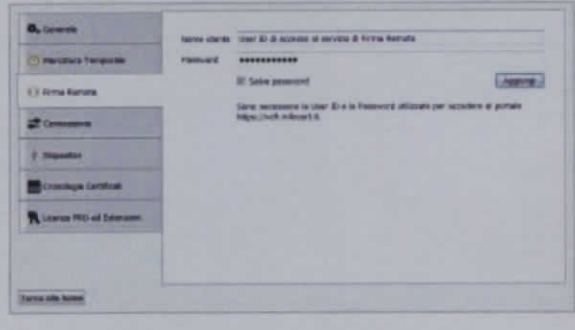
Il programma Dike 6 è avviato con un doppio click sull'icona disponibile sul desktop dopo l'installazione.

Il programma si apre sulla HOME page che consente di gestire la configurazione e firmare o verificare la firma apposta su un documento.

4.1 Associazione del certificato di firma remota

La prima operazione da effettuare riguarda l'associazione del certificato di firma remota.

Occorre selezionare la funzione *Configurazione* contrassegnata dall'icona a forma di ingranaggio, e selezionare la pagina dedicata alla **Firma Remota**.



All'interno di questa area è possibile inserire:

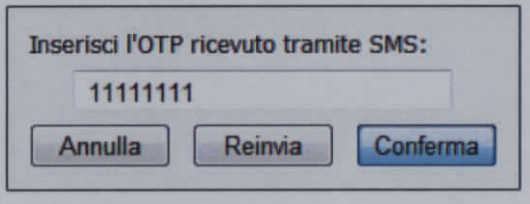
- la **User ID** di accesso al servizio (quella che mi è stata assegnata da InfoCert al momento della registrazione, la trovo sulla copia della Richiesta di Registrazione consegnatami in quell'occasione);

- la **Password** (quella che utilizzo per accedere al portale dedicato ai titolari di un certificato remoto, My.Sign, e che ho personalizzato al momento dell'attivazione del mio certificato).

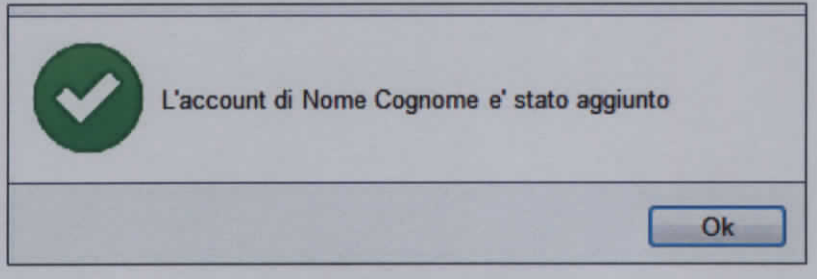
Selezionando l'opzione *Salva password*, inoltre, è possibile evitare che al momento della firma Dike 6 chieda nuovamente di inserirla.

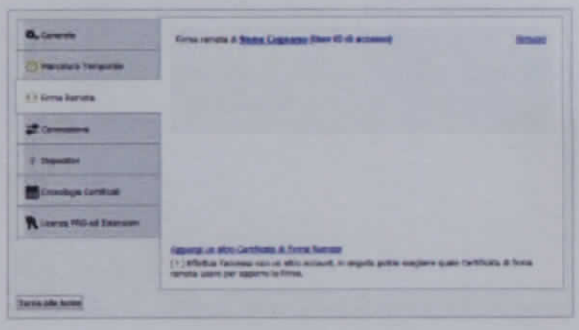
Se al momento della registrazione è stato indicato il numero personale di cellulare come sistema per ricevere i codici OTP, il clic sul pulsante *Aggiungi* provvede a richiederne uno automaticamente.

In alternativa, è possibile ottenere il codice numerico utilizzando la chiavetta OTP consegnata al momento del rilascio. Qualunque sia il sistema di recupero del codice OTP, Dike 6 chiede di digitare il codice.



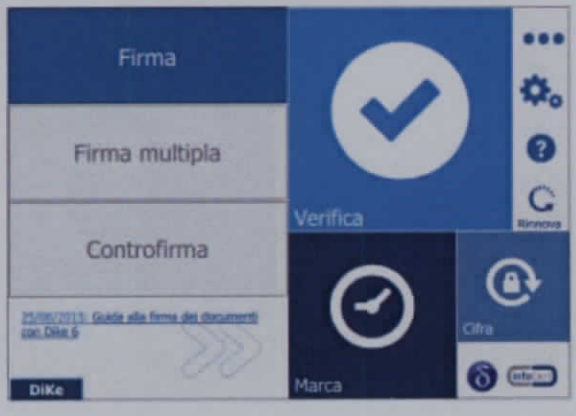
Dike 6 conferma successivamente l'avvenuta attivazione del certificato di firma remota.





4.2 Firma di un documento

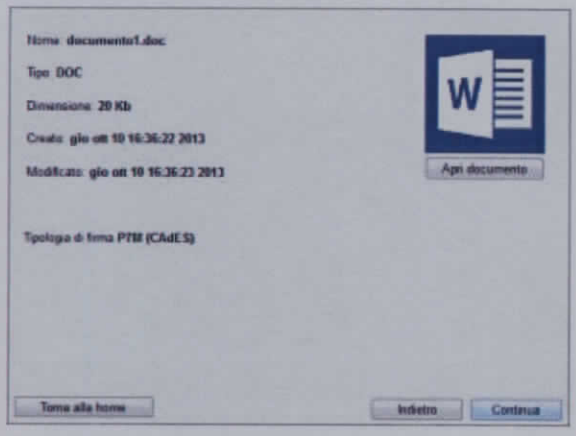
Passando il mouse sul riquadro *Firma* si accede all'elenco delle funzioni di firma.



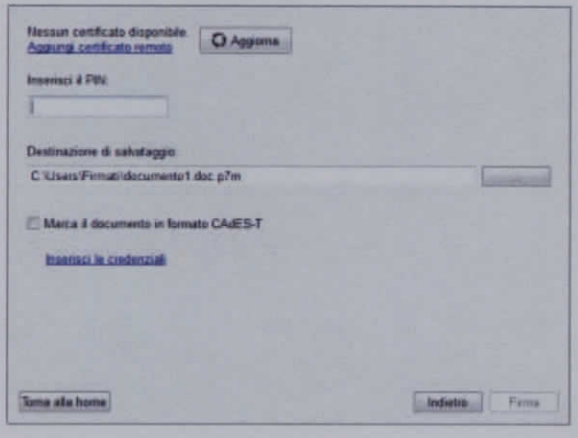
L'opzione *Firma* permette di selezionare il documento da firmare e di richiamarlo all'interno del software. Le opzioni *Firma multipla* e *Controfirma*, di colore grigio, sono disponibili nella versione PRO che l'Istat non utilizza al momento.

Dike 6 presenta:

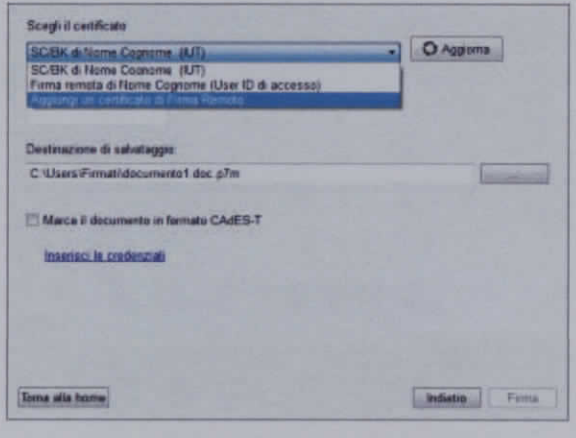
- gli estremi del documento (tipo, dimensione, ecc.)
- mette a disposizione il pulsante *Apri documento* per visualizzarlo.
- evidenzia che sto per eseguire una firma che produrrà un documento con estensione **.p7m**, cioè a standard CAdES e mi fa procedere con un clic sul pulsante *Continua*.



Prima di iniziare il processo di firma vero e proprio, il programma Dike 6 verifica che l'utente abbia a disposizione un certificato di sottoscrizione con il quale firmare.



Un clic sul pulsante *Aggiorna* propone le possibili alternative:



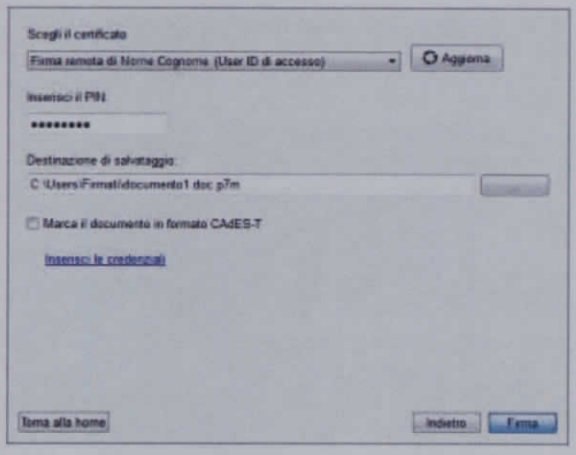
a. un dispositivo fisico, se è stato già collegato alla postazione di lavoro;

b. un certificato di firma remoto se è stato aggiunto ai possibili strumenti di firma a disposizione di Dike 6.

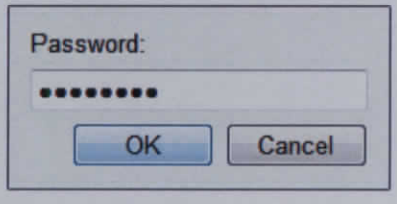
E' in ogni caso necessario che sia selezionato il tipo di firma che sarà utilizzato per sottoscrivere il documento.

4.2.1 Firma P7M con un certificato remoto

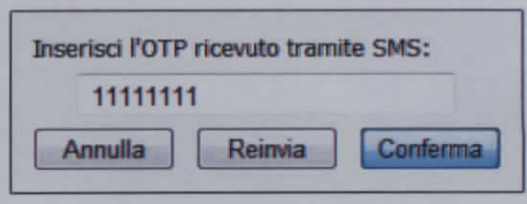
Dopo aver selezionato l'opzione *certificato di firma remota* è possibile procedere con la firma del documento.



E' necessario digitare il PIN di protezione del certificato personale nel campo *Inserisci il PIN* proseguendo poi con l'indicazione della cartella all'interno della quale memorizzare il documento firmato. Dike 6 propone un possibile percorso nel campo *Destinazione di salvataggio*. E' possibile il suggerimento o apportare una modifica utilizzando il pulsante posto a fianco del campo.
Un clic sul pulsante *Firma* fa avanzare il processo di sottoscrizione del documento: Dike 6, infatti, chiederà di inserire la **Password**, quella utilizzata per accedere al portale dedicato ai titolari di un certificato remoto, My.Sign, e che è stato personalizzato al momento dell'attivazione del mio certificato,



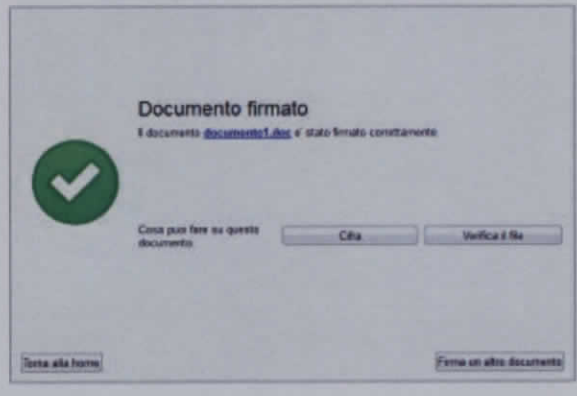
e l'**OTP**, il codice numerico che si può ottenere utilizzando l'App OTP, consegnata al momento del rilascio, ovvero tramite un SMS e/o email che arriverà sul telefono cellulare personale.



Se è stata ricevuto un codice mediante App OTP, sarà sufficiente attivarla e riportare, nel campo dedicato, le cifre che compongono il codice, facendo attenzione a digitarle correttamente.

Nel caso di codice OTP inviato via SMS, si ha la possibilità di richiederlo con un clic sul pulsante *Reinvia*. Il mittente del messaggio SMS è InfoCert; il testo del messaggio indica la data della richiesta, l'ora di generazione del Codice OTP e il codice stesso, di 8 cifre, che occorre riportare nel campo disponibile, facendo attenzione a digitarle correttamente.

Al termine del processo di firma, che richiede qualche secondo, Dike 6 conferma che l'attività si è conclusa con successo.



4.2.2 Firma PDF di un documento

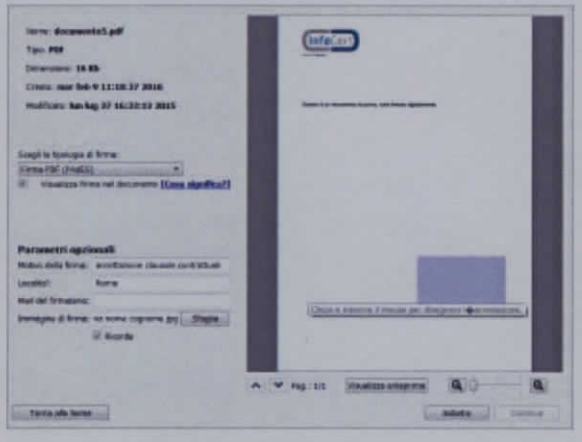
Passando il mouse sul riquadro *Firma* e facendolo ruotare si accede all'elenco delle funzioni di firma.

Dike 6 presenta l'opzione *Firma* che permette di selezionare il documento da firmare e di richiamarlo all'interno del software.

Le opzioni *Firma multipla* e *Controfirma*, di colore grigio, sono disponibili nella versione PRO (ISTAT non utilizza tale opzione).

Dike 6 presenta gli estremi del documento (tipo, dimensione, ecc.) nonché un riquadro di visualizzazione che lo contiene e che permette di scorrerlo, di ingrandirlo o di produrne un anteprima.
Dike 6 informa inoltre che il documento firmato manterrà l'estensione .pdf, cioè la firma sarà a standard PAdES.
E' possibile comunque firmare il documento in modalità CAdES ricorrendo all'opzione presente nel menu *Scegli la tipologia di firma*.

L'opzione *Visualizza firma nel documento* selezionata, segnala che la firma standard PAdES sarà arricchita con un'annotazione grafica visibile, contenente gli estremi della firma stessa.
Qualora si decidesse di eliminare l'annotazione grafica, il documento avrebbe comunque estensione .pdf e sarebbe firmato secondo lo standard PAdES, ma senza informazioni attinenti alla firma visibili sul documento.



I *Parametri opzionali*, infine, consentono di arricchire il processo di firma con informazioni riguardanti:

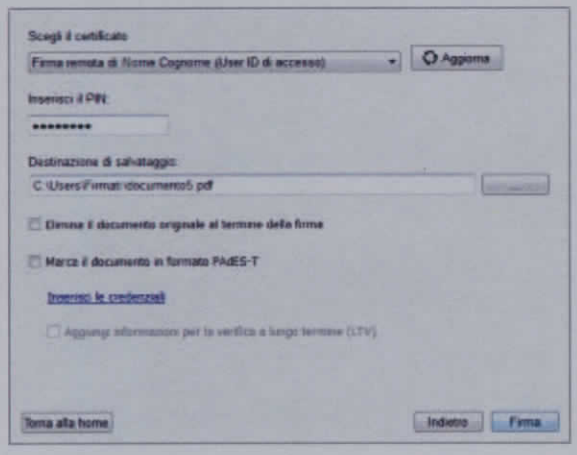
- il motivo per il quale è sottoscritto digitalmente il documento, ad esempio: accettazione delle clausole contrattuali, accettazione delle clausole vessatorie del contratto, espressione del consenso al trattamento dei dati personali ai sensi della L. 196/2003, ecc.;
- il luogo di apposizione della firma;
- un eventuale recapito e-mail;
- l'immagine della firma grafica, sempreché sia stata scansionata e salvata come immagine nel computer. Il formato ammesso è il .jpg. E' molto importante tenere a mente che questo segno grafico **non ha alcun valore legale** e **non è** in alcun modo **la mia firma digitale**.

Trascinando il puntatore che appare sullo schermo, è possibile delimitare un'area di colore viola all'interno del documento. La scelta del suo posizionamento è lasciata all'iniziativa del firmatario: va da sé che se si ha la necessità di firmare digitalmente un contratto, occorre posizionare l'area nella zona del documento in cui è prevista l'apposizione della firma del contraente.

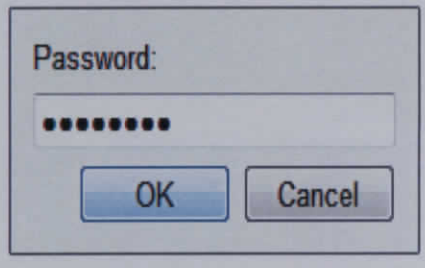
Per procedere occorre effettuare un clic sul pulsante *Continua*.

4.2.3 Firma PDF con un certificato remoto

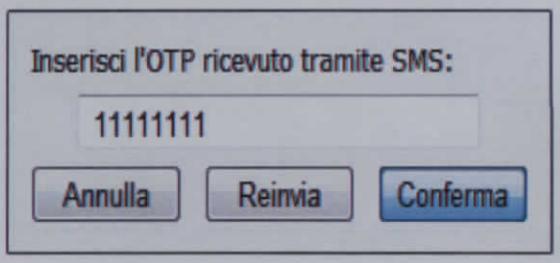
Dopo aver selezionato l'opzione *certificato di firma remota* potrò procedere con la firma del documento.



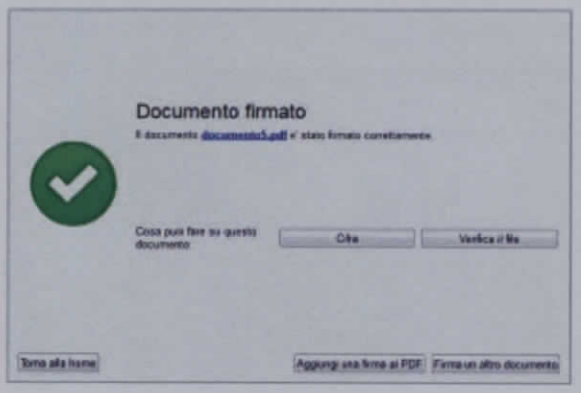
Inizierò a digitare il PIN di protezione del mio certificato nel campo *Inserisci il PIN* proseguendo poi con l'indicazione della cartella all'interno della quale memorizzare il documento firmato. Dike 6 propone un possibile percorso nel campo *Destinazione di salvataggio*. Posso accettare quanto suggerito o apportare una modifica utilizzando il pulsante posto a fianco del campo. Un clic sul pulsante *Firma* fa avanzare il processo di sottoscrizione del documento: Dike 6, infatti, mi chiederà di inserire la **Password**, quella che utilizzo per accedere al portale dedicato ai titolari di un certificato remoto, My.Sign, e che ho personalizzato al momento dell'attivazione del mio certificato,



e l'**OTP**, il codice numerico che posso ottenere utilizzando l'App (o chiavetta) OTP, consegnata al momento del rilascio, ovvero tramite un SMS e/o email che arriverà sul mio telefono cellulare.



Se ho ricevuto una App (o chiavetta) OTP, sarà sufficiente attivarla e riportare, nel campo dedicato, le cifre che compongono il codice, facendo attenzione a digitarle correttamente.
Nel caso di codice OTP inviato via SMS, ho sempre la possibilità di richiederlo con un clic sul pulsante *Reinvia*.
Il mittente del messaggio SMS è InfoCert; il testo del messaggio indica la data della richiesta, l'ora di generazione del Codice OTP e il codice stesso, che potrò riportare nel campo disponibile, facendo attenzione a digitarle correttamente.
Al termine del processo di firma, che richiede qualche secondo, Dike 6 mi confermerà che l'attività si è conclusa con successo.

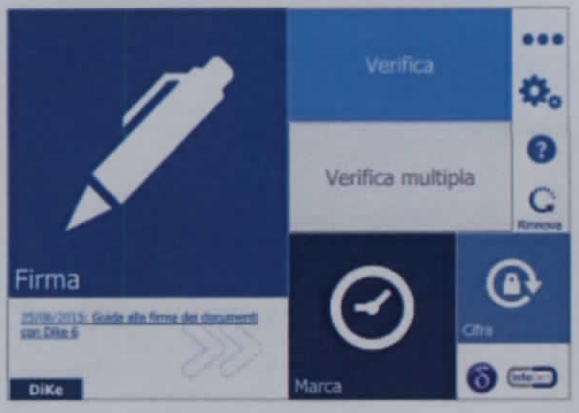


Un clic sul pulsante *Aggiungi una firma al PDF* mi permette di proseguire il processo di firma del documento, facendolo sottoscrivere da uno o più firmatari.

4.3 Verifica della validità di un documento

La verifica di un documento firmato digitalmente e/o marcato è importante tanto quanto lo è l'attività di firma e di marcatura temporale.

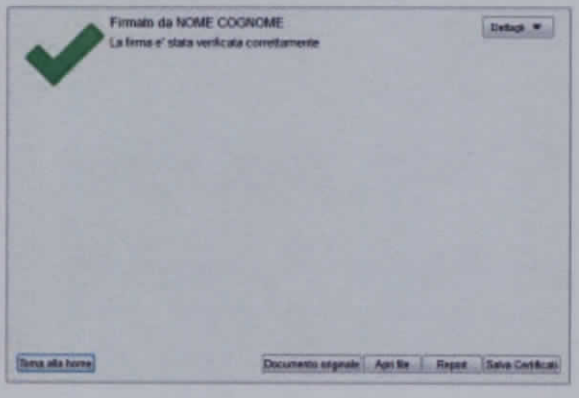
Passando il mouse sul riquadro *Verifica* occorre ruotare per accedere all'elenco delle funzioni di verifica.



Dike 6 mette a disposizione l'opzione *Verifica* che permette di selezionare il documento da verificare e di richiamarlo all'interno del software.

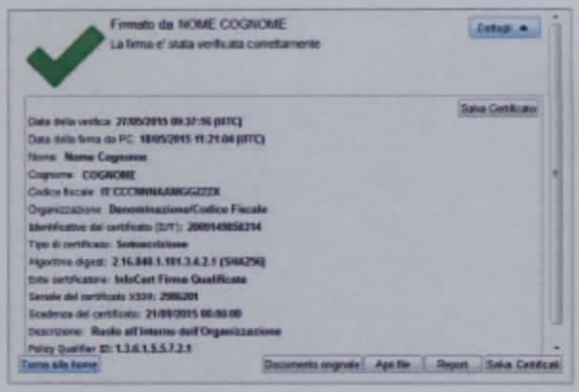
L'opzione *Verifica multipla*, di colore grigio, è disponibile nella versione PRO (ISTAT non utilizza tale opzione).

La risposta di Dike 6 è diretta e consiste in una sintesi dell'esito di verifica.

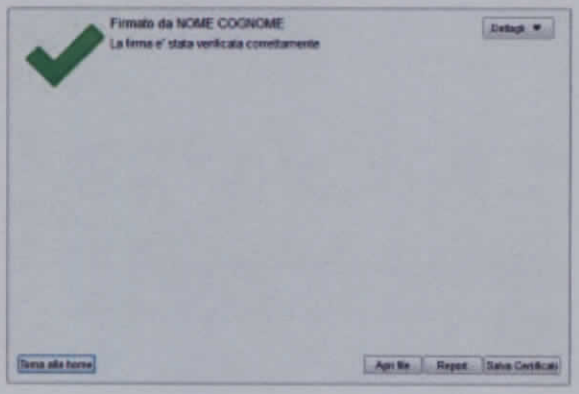


Un clic sul pulsante *Dettagli* permette di ottenere maggiori informazioni sulla firma (standard CAdES), sul firmatario e sul certificato utilizzato per firmare.

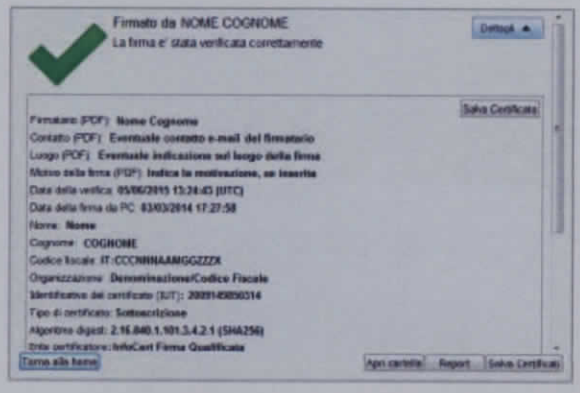
Tra le informazioni di dettaglio è presente anche la data di aggiornamento della *lista CRL*, ovvero la lista che fornisce informazioni sui certificati revocati, sospesi o scaduti.



Se è stato selezionato un documento firmato in modalità PDF (standard PAdES), l'esito della verifica produrrà una sintesi identica alla precedente.



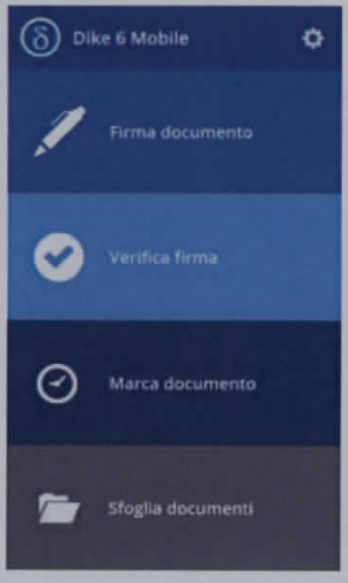
Un clic sul pulsante *Dettagli* permette di ottenere maggiori informazioni sulla firma, sul firmatario e sul certificato utilizzato per firmare nonché sui particolari della firma PDF: motivo, luogo della firma, eventuale contatto del firmatario.



4.4 Avvio attività da un dispositivo mobile

La selezione dell'icona avvia **Dike 6 Mobile**

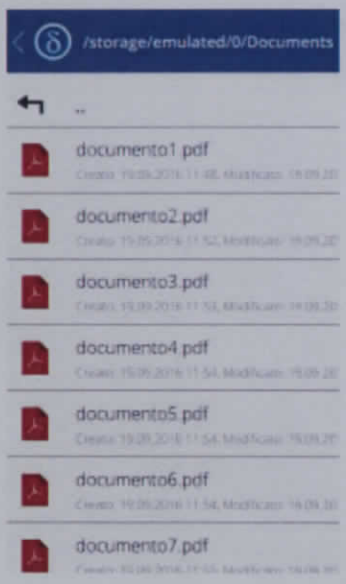
e permette di avere a disposizione la pagina iniziale dell'app dalla quale selezionare l'attività ricercata: firmare un documento, marcarlo temporalmente o verificarne la validità.



In alternativa, è possibile consultare l'archivio dei documenti già utilizzati o visionati con Dike 6 Mobile con la funzione *Sfoglia documenti*.

4.4.1 Selezione dei documenti da firmare con Android

Se lo smartphone o il tablet, sono supportati dal sistema operativo **Android**, è possibile scegliere i documenti che occorrono all'interno delle cartelle di sistema, dopo aver selezionato la funzione di interesse: *Firma*, *Verifica* o *Marca del documento*.



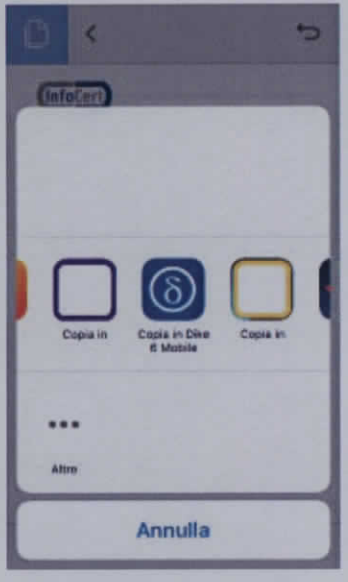
Una volta individuato il percorso per arrivare alla cartella in cui sono stati salvati i documenti, compare un elenco con i documenti trovati ed occorre selezionare quello di interesse per procedere.

4.4.2 Selezione dei documenti da firmare con iOS

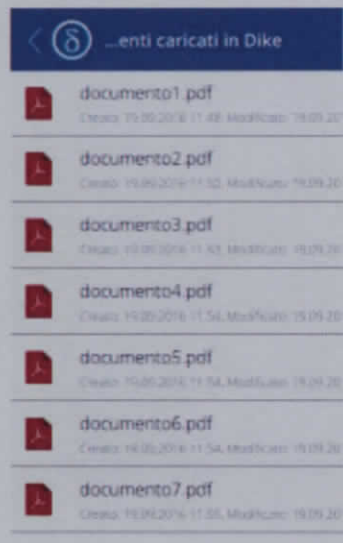
Se lo smartphone o il tablet sono supportati dal sistema operativo **iOS**, occorre preventivamente importare i documenti che occorrono all'interno di Dike 6 Mobile selezionandoli tra quelli salvati in locale.

Dopo aver aperto il documento ricercato con l'applicazione originale (nel caso di documenti .pdf, ad esempio, all'interno del visualizzatore Adobe Acrobat), è possibile procedere selezionando la funzione *Apri in....*

Tra le diverse APP con le quali eseguire la condivisione, selezionare l'icona di Dike 6 Mobile.



Al termine dell'operazione si riceve una conferma dell'avvenuta esecuzione del comando. I documenti condivisi con Dike 6 Mobile sono visibili nell'area *Documenti caricati in Dike* attraverso la funzione *Sfoglia documenti* ed è in quest'area che occorre selezionare i documenti da firmare, verificare.

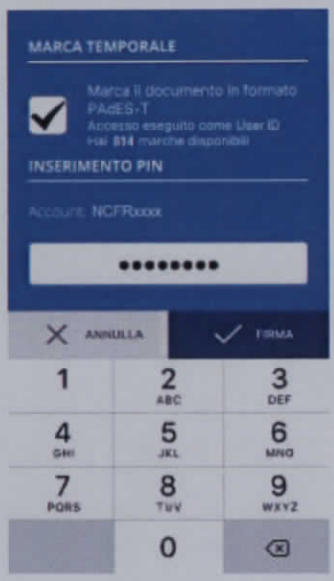


4.4.3 Firma di un documento

Una volta selezionato il documento, Dike 6 Mobile presenta il pannello di controllo per l'apposizione della firma digitale.

Al suo interno sono disponibili gli estremi del documento (tipo, dimensione, ecc.), le opzioni per scegliere la tipologia di firma e quella per apporre una marca temporale.

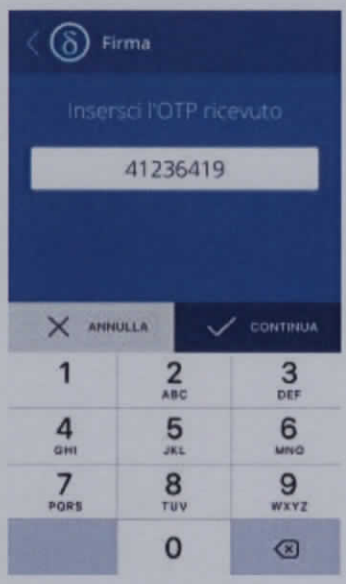
Una volte selezionata la tipologia di firma, ed eventualmente la marca temporale, occorre inserire il PIN di protezione del certificato nel campo *Inserisci PIN* proseguendo poi con la selezione del comando *Firma*.



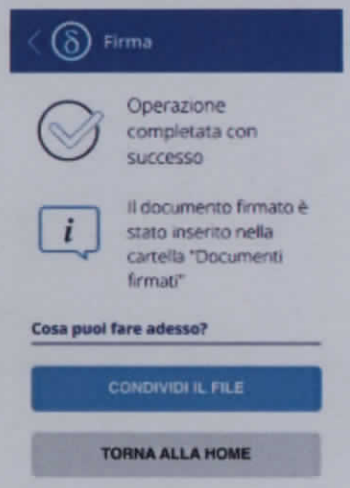
Se è stato preventivamente configurato il generatore di codici OTP, le cifre che lo compongono saranno disponibili già all'interno del campo *Inserisci l'OTP ricevuto/generato*.

In caso contrario sarà inviato un messaggio SMS al cellulare personale e dovranno essere riportate le cifre che compongono l'OTP nel campo dedicato.

Si prosegue selezionando il comando *Continua*.



Al termine dell'operazione di firma sarà inviato un messaggio di conferma. I documenti firmati digitalmente e quelli firmati digitalmente e marcati temporalmente sono salvati all'interno dell'area *Documenti firmati* attraverso la funzione *Sfoglia documenti*.



4.4.4 Verifica della validità di un documento

La verifica di un documento firmato digitalmente e/o marcato è importante tanto quanto lo è l'attività di firma e di marcatura temporale.

Dike 6 Mobile mette a disposizione la funzione *Verifica* con la quale è possibile selezionare il documento firmato e/o marcato da verificare richiamandolo all'interno dell'app.

La risposta di Dike 6 è diretta e consiste nella presentazione delle informazioni sulla firma, sul firmatario e sul certificato utilizzato per firmare.

Se il documento è marcato temporalmente saranno disponibili le informazioni di dettaglio sulla marca temporale apposta.

Tra le informazioni è presente anche la data di aggiornamento della *lista CRL*, ovvero la lista che fornisce informazioni sui certificati revocati, sospesi o scaduti.

4.4.5 Chiusura delle attività

Al termine delle attività di firma di un documento, o di verifica della validità di una firma, occorre uscire da Dike 6 Mobile secondo le modalità previste dal sistema operativo.