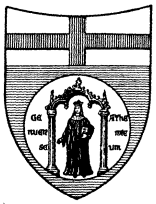


UNIVERSITA' DEGLI STUDI DI GENOVA

firmiAMO in digitale

Linee guida per l'uso del servizio di firma digitale all'interno dell'Università degli Studi di Genova

a cura di: Anna RAPALLO

INDICE

INTRODUZIONE

L'Università degli Studi di Genova negli ultimi anni ha avviato un processo di modernizzazione basato sia sull'innovazione tecnologica, intesa come uso di nuove tecnologie, che sulla rivisitazione dei processi e dei procedimenti; si è trattato di un processo alla cui realizzazione hanno partecipato diversi attori e diversi strumenti che hanno contribuito alla razionalizzazione e semplificazione dell'azione amministrativa.
Le azioni di e-government, in linea con la normativa vigente, assicurano infatti i seguenti risultati:
- Migliorano l'efficienza amministrativa della PA;
- Favoriscono l'interoperabilità tra le amministrazioni;
- Migliorano la trasparenza dei procedimenti;
- Consentono l'accesso ai servizi on-line di tutte le amministrazioni;
- Riducono i costi e tempi;
- Garantiscono un trattamento paritario per tutti i cittadini.

La dematerializzazione dei flussi documentali all'interno delle pubbliche amministrazioni non rappresenta solo un'opportunità o un percorso volto al raggiungimento di livelli di maggior efficienza, efficacia, trasparenza, semplificazione e partecipazione ma, come di seguito illustrato, rappresenta anche l'adempimento di un preciso ed improrogabile obbligo normativo.
All'interno dell'Università degli Studi di Genova le soluzioni adottate hanno riguardato principalmente l'utilizzo e l'integrazione dei seguenti strumenti informatici:

- Firma digitale;
- Posta elettronica certificata;
- Protocollo informatico (unica AAOO federata)
- SPID (in corso di realizzazione)

L'obiettivo del presente manuale è quello di fornire al personale dipendente dell'Ateneo le indicazioni operative per l'uso del servizio di firma digitale; in particolare, dopo un'introduzione normativa, saranno indicate le modalità per ottenere la firma digitale, sarà dimostrato come sottoscrivere un documento utilizzando il sito di Ateneo o il software Cryptoclient rilasciato dal Certificatore IT Telecom. Seguirà poi una dimostrazione su come procedere, in occasione del ricevimento di un documento firmato digitalmente, alla verifica della validità di una firma digitale utilizzando diversi software presenti in commercio.

CAPITOLO I

Normativa sulle firme elettroniche

I.1 NORMATIVA

Le modifiche al Codice dell'Amministrazione digitale apportate dal D.Lgs. 179/2016 hanno realizzato il coordinamento della normativa italiana con quella europea definita del Regolamento UE 910/2014 eIDAS (electronic IDentification Authentication and Signature). L'obiettivo della normativa comunitaria è infatti quello di potenziare la realizzazione di un mercato unico digitale e di compiere il definitivo passaggio dal cartaceo al digitale dell'intero ciclo di vita del documento, dalla creazione, alla gestione ed infine alla conservazione mediante un approccio che ridefinisca i processi e i modelli di gestione documentale e non si limiti solo a tradurre in digitale strumenti analogici e documenti cartacei.

Insieme al Regolamento Eidas e al CAD completano il quadro normativo i seguenti principali provvedimenti legislativi di cui occorre avere conoscenza per realizzare una corretta gestione documentale:

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto legislativo 20 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali;
- Decreto legislativo 22 gennaio 2004 n. 42 – Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137;
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 – Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della legge 16 gennaio 2003, n. 3;
- Decreto legislativo 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale;
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali;
- Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - Regole tecniche per il protocollo informatico;
- Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione;
- Regolamento eIDAS – Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 – Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014 – 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;
- Decreto legislativo 26 agosto 2016, n. 179 – Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.
- Decreto Legislativo 13 dicembre 2017, n. 2017 recante "Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche e

integrazioni al Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n 82, ai sensi dell'art. 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche". Il decreto entra in vigore dal 27 gennaio 2018.

I.2 FIRME ELETTRONICHE

Uno dei primi temi da affrontare in materia di dematerializzazione è quello della corretta formazione del documento informatico definito dall'art. 1 lett. p) del CAD "*il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"*; al riguardo è curioso rilevare come il legislatore consideri il documento informatico la norma mentre consideri la formazione in modalità analogica residuale definendola in negativo quale "*rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti"*.

Per le sue intrinseche caratteristiche il documento informatico ha bisogno di particolari accorgimenti in grado di garantire, durante l'intero ciclo di gestione dello stesso, il mantenimento del suo valore giuridico e legale; solo una corretta formazione del documento informatico, basata su regole e procedure giuridiche e archivistiche, ne consente una conservazione conforme alla normativa ed a costi ragionevoli.

Considerato che l'imputabilità di un documento ad un determinato soggetto è garantita dalla sottoscrizione, in tema di formazione e valore probatorio del documento informatico assume notevole importanza lo strumento della firma elettronica nelle sue diverse tipologie di seguito illustrate:

- **Firma elettronica (semplice o debole)**: art. 1 Regolamento eIDAS "*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare"*;
- **Firma elettronica avanzata:** art. 1 Regolamento eIDAS *"una firma elettronica che soddisfi i requisiti di cui all'articolo 26"*[1];
- **Firma elettronica qualificata:** art. 1 Regolamento eIDAS *"una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche"*;
- **Firma digitale** art. 1, lett. S del CAD: *"un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente*

[1] Art. 26 Regolamento eIDAS: Requisiti di una firma elettronica avanzata
Una firma elettronica avanzata soddisfa i seguenti requisiti:
a) è connessa unicamente al firmatario;
b) è idonea a indentificare il firmatario;
c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica

al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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";

I.3 IL VALORE PROBATORIO DELLE FIRME ELETTRONICHE

L'efficacia giuridica delle firme elettroniche è pertanto diversa in ragione delle caratteristiche di ognuna di esse partendo dal principio definito di "non discriminazione" sancito dall'art. 25 del Regolamento eIDAS[2] che attribuisce anche alla firma elettronica (semplice o debole) valore giuridico. L'attuale art. 20 del CAD stabilisce che nei casi di sottoscrizione con firma elettronica semplice "*l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità*".

Ciò vuol dire che in caso di contenzioso il giudice dovrà valutare, ex art. 116 del c.p.c., se in sede di generazione della firma sono state adottate idonee misure, tecnologiche e procedurali, atte a garantire in modo certo ed univoco la connessione tra il firmatario e il documento. Per attribuire valore giuridico ad un documento informatico sottoscritto con firma elettronica occorre pertanto archiviare e conservare insieme ai *bit* che rappresentano il documento anche le informazioni che caratterizzano il processo di firma in termini di qualità, sicurezza, integrità e immodificabilità[3].

L'uso di credenziali accesso (*user-id e password*) rappresentano, per esempio, la generazione di una firma elettronica con un basso profilo di affidabilità; tale livello può essere innalzato combinando più livelli di identificazione per esempio inserendo l'uso di un dispositivo (es. cellulare, carta bancomat) o un OTP (*One time password*). Generalmente tale tipo di firma elettronica viene utilizzato nei sistemi di gestione documentale per la formazione di atti endoprocedimentali sostituendosi al precedente "visto".

Dalla definizione di firma elettronica avanzata (art. 26 eIDAS) si evince che l'utilizzo di particolari dati, dispositivi e procedure permettono di affermare, con un elevato grado di sicurezza, che la firma è stata creata dal firmatario in quanto l'unico in grado di generarla con i mezzi in suo esclusivo possesso; ciò che comunque caratterizza la firma elettronica avanzata (FEA) rispetto alla firma elettronica semplice è la capacità della FEA di evidenziare le modifiche apportate al documento dopo la sottoscrizione garantendo così l'integrità e

---

[2] Art. 25 Regolamento eIDAS: Effetti giuridici delle firme elettroniche:

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per le firme elettroniche qualificate.
2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.
3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

[3] S. PIGLIAPOCO *Progetto Archivio Digitale-Metodologia Sistemi Professionalità* CIVITA 2016, pag. 30

l'immodificabilità delle dichiarazioni prodotte. Per la generazione della firma elettronica avanzata occorre rinviare a quanto indicato dal titolo V del D.P.C.M. 22 febbraio 2013 che, all'art. 55, prevede che "*la realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva*" e non è vincolata all'adozione di particolari piattaforme purché, siano soddisfatti i requisiti sopra indicati. Tuttavia la FEA, ai sensi dell'art. 60 del citato D.P.C.M. è utilizzabile limitatamente nei rapporti giuridici intercorrenti tra il sottoscrittore e l'ente che la propone come strumento per la produzione dei documenti informatici, fatto salvo quanto disposto dall'art. 27 del Regolamento eIDAS.
Ad oggi la FEA è principalmente utilizzata nel settore bancario e postale nella forma di firma grafometrica: con tale tipologia di firma si associa in modo univoco un documento informatico a parametri biometrici comportamentali rilevati mediante l'apposizione della firma autografa sul dispositivo (tablet) dotato di apposito software in grado di rilevare la pressione della mano, l'inclinazione della penna, la velocità di scrittura che sono proprie di ciascun individuo. Anche in questo caso i dati rilevati devono essere associati, con un processo che rilevi le eventuali modifiche, al documento a cui si riferiscono.

La firma elettronica qualificata (FEQ) è una firma avanzata basata su un certificato qualificato e creata con un dispositivo, definito "dispositivo di firma sicura", in possesso di caratteristiche tecniche stabilite dall'allegato II del Regolamento eIDAS[4]. Per la sua corretta creazione occorre l'intervento di un "prestatore di servizi fiduciario qualificato" competente al rilascio di certificati qualificati di firma. Il certificato qualificato di firma elettronica deve avere il contenuto indicato all'allegato I del Regolamento eIDAS :

[4] Allegato II Regolamento eIDAS: Requisiti per i dispositivi per la creazione di una firma elettronica qualificata
1. I dispositivi per la creazione di una firma elettronica qualificata garantiscono, mediante mezzi tecnici e procedurali appropriati, almeno quanto segue:
a) è ragionevolmente assicurata la riservatezza dei dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica;
b) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica possono comparire in pratica una sola volta;
c) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e la firma elettronica è attendibilmente protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;
d) i dati per la creazione di una firma elettronica utilizzati nella creazione della stessa possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi.
2. I dispositivi per la creazione di una firma elettronica qualificata non alterano i dati da firmare né impediscono che tali dati siano presentati al firmatario prima della firma.
3. La generazione o la gestione dei dati per la creazione di una firma elettronica per conto del firmatario può essere effettuata solo da un prestatore di servizi fiduciario qualificato.
4. Fatto salvo il punto 1, lettera d), i prestatori di servizi fiduciari qualificati che gestiscono dati per la creazione di una firma elettronica per conto del firmatario possono duplicare i dati per la creazione di una firma elettronica solo ai fini di back-up, purché rispettino i seguenti requisiti:
a) la sicurezza degli insiemi di dati duplicati deve essere dello stesso livello della sicurezza degli insiemi di dati originali;
b) il numero di insiemi di dati duplicati non eccede il minimo necessario per garantire la continuità del servizio.

- l'indicazione del fatto che il certificato è stato rilasciato quale certificato qualificato di firma elettronica;
- un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato e include almeno lo Stato membro in cui tale prestatore è stabilito;
- il nome del firmatario, o uno pseudonimo;
- dati di convalida della firma elettronica che corrispondono ai dati per la sua creazione;
- indicazione dell'inizio e della fine del periodo di validità del certificato;
- la firma elettronica avanzata del prestatore di servizi fiduciari qualificato che rilascia il certificato

A questi dati possono aggiungersi quelli indicati dall'art. 28 CAD quali ad esempio il codice fiscale, la qualifica del titolare (es. appartenenza ad ordine professionale, qualifica di pubblico ufficiale), i limiti di uso del certificato e eventuali limiti di valore degli atti per i quali il certificato può essere usato.
In sostanza il prestatore di servizi, terza parte fidata ed in possesso di determinati requisiti previsti dal CAD, rilascia un certificato qualificato a fronte di un'identificazione certa del titolare; ciò appunto è ciò che consente di dare valore alla FEQ.
Nella FEQ gli elementi di indeterminatezza che caratterizzano la FEA sono pertanto sostituiti da indicazioni tecnologiche e procedurali che garantiscono un più alto livello di sicurezza.

La firma digitale (FD) è un particolare tipo di FEQ basata su un certificato qualificato e su di un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e ad un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico. La FD è il risultato di un algoritmo crittografico a chiavi asimmetriche applicato all'impronta del file che contiene la rappresentazione digitale del documento, ed è generata con la funzione crittografica HASH SHA- 256 in conformità allo standard ISO 10118-3:2004.
Un algoritmo di chiavi asimmetriche necessita di una coppia di chiavi una pubblica (Kp) nota a tutti e una privata (Ks) conosciuta solo al titolare della coppia; se la codifica di un documento è avvenuta con la chiave di una coppia, la decodifica può avvenire solo con l'altra chiave della stessa coppia.
Ai documenti sottoscritti con firma elettronica qualificata o digitale, formati nel rispetto di quanto indicato dal D.P.C.M. 22 febbraio 2013, ai sensi dell'art. 20 del CAD è riconosciuta l'efficacia prevista dall'art. 2702 del c.c. e l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria. Il legislatore ricorre al meccanismo della presunzione *ex lege* dell'utilizzo del dispositivo di firma da parte del titolare; rispetto al disconoscimento della firma autografa si configura l'inversione dell'onere della prova: non è il soggetto che produce il documento in giudizio a dover dimostrare che la sottoscrizione non è autentica, ma è il titolare della firma digitale a dover dimostrare l'esistenza di un abuso nell'uso del dispositivo; ciò avviene in conseguenza del fatto che tra

gli obblighi a carico del titolare del certificato di firma vi è anche quello di assicurare la custodia del dispositivo di firma e di utilizzare personalmente il dispositivo di firma (art. 32 del CAD).

In conclusione, in tema di validità giuridica delle firme elettroniche, si può affermare che ai sensi dell'art. 20 e 21 del CAD il documento informatico:
- soddisfa il requisito della forma scritta ed è liberamente valutabile in giudizio se firmato con firma elettronica semplice;
- è pienamente valido, come qualsiasi scrittura privata ex art. 2702 c.c. se firmato con firma avanzata, qualificata o digitale;
- è pienamente valido solo se firmato con firma qualificata o digitale nel caso si tratti di una scrittura privata di particolare rilevanza (art. 1350 c.c. comma 1 dal n. 1 al 12), come per esempio la vendita di immobili, (a pena di nullità).

I.4 LA VALIDITA' NEL TEMPO DEL CERTIFICATO QUALIFICATO

Fondamentale quando si tratta valutare la validità di una FEQ o una FD è il tema della loro validità in termini temporali. Il certificato qualificato del titolare ha infatti, generalmente, una validità di tre anni, ma può essere anche sospeso o revocato prima della scadenza sia per volontà del certificatore, del titolare o del terzo interessato, in tutti quei casi in cui la sottrazione, lo smarrimento, la perdita del dispositivo o dell'esclusivo controllo su di esso facciano sorgere il ragionevole dubbio che il certificato possa essere utilizzato impropriamente da altri.
Le sospensioni e le revoche dei certificati qualificati sono giornalmente registrate dai prestatori di servizi fiduciari sulle CRL (Certificate Revocation List) che vengono consultate dai software in sede di verifica della firma digitale proprio con lo scopo di verificare se il certificato è valido o meno. L'art. 36 del CAD, al comma 3, infatti prevede che la revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione nella lista che lo contiene. Il momento della pubblicazione deve inoltre essere attestato mediante adeguato riferimento temporale.
Pertanto, ai sensi dell'art. 24 del CAD comma 4-bis, l'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma basata su un certificato qualificato revocato, scaduto o sospeso equivale a mancata sottoscrizione.
Quando si firma un documento è pertanto necessario accertarsi circa la validità del proprio certificato e sapere come agire per preservare l'autenticità dello stesso oltre il termine di scadenza. Per fare questo è necessario utilizzare un riferimento temporale opponibile ai terzi tramite il quale si associano al documento una data e un'ora certe con lo scopo di dimostrare che il documento è stato sottoscritto con un certificato qualificato valido dal punto di vista temporale, anche se la verifica viene fatta dopo la naturale scadenza. In questo caso infatti il software che effettua la verifica rileverà che il certificato è scaduto ma che è stato apposto un riferimento temporale che riporta il momento della sottoscrizione in un arco temporale di

validità del certificato. L'art. 62 del D.P.C.M. 22 febbraio 2013 stabilisce infatti il seguente principio *"Le firme elettroniche qualificate o digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un periodo precedente alla scadenza, revoca o sospensione del suddetto certificato".*

Il Regolamento eIDAS definisce la validazione temporale elettronica come *"dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che esistevano in quel momento"*[5] e la validazione temporale qualificata come *"una validazione temporale elettronica che soddisfa i requisiti dell'art. 42"*[6]. L'art. 20 del CAD stabilisce che *"La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida"* Ad oggi le disposizioni in tema di validazione temporale sono contenute nel D.P.C.M. 22 febbraio 2013 e D.P.C.M. 13 novembre 2014.

Il sistema più diffuso per la validazione temporale è costituito dalla c.d. "marca temporale" o "*time stamp*" che deve essere apposta da una terza parte fidata ed imparziale cioè un prestatore di servizi fiduciari qualificato. La marca temporale deve essere generata con un sistema che sia in grado di mantenere la data e l'ora in modo che non si discostino per più di un minuto primo dalla scala di tempo coordinato universale (UTC) (art. 51 del D.P.C.M. 22 febbraio 2013). La marca temporale contiene le informazioni minime indicate dall'art. 48 del citato D.P.C.M. ed in particolare:

- l'identificativo dell'emittente;
- il numero di serie della marca temporale;
- l'algoritmo di sottoscrizione della marca temporale;
- il certificato relativo alla chiave utilizzata per la verifica della marca temporale;
- il riferimento temporale della generazione della marca temporale;

---

5 Art. 41 Regolamento eIDAS - Effetti giuridici della validazione temporale elettronica
1.Alla validazione temporale elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata;
2.Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali data e ora sono associate;
3.Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri

6 Art. 42 Regolamento eIDAS - Requisiti per la validazione temporale elettronica qualificata
1.Una validazione temporale qualificata soddisfa i requisiti seguenti:
a) collega la data e l'ora ai dati in modo da esclude ragionevolmente la possibilità di modifiche non rilevabili dei dati;
b) si basa una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e
c) è apposta mediante una firma elettronica avanzata o sigillata con sigillo elettronico avanzato del prestatore di servizi fiduciario qualificato o mediante metodo equivalente;
d) La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al collegamento della data e dell'ora ai dati e a fonti accurate di misurazione del tempo. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il collegamento della data e dell'ora ai dati e alla fonte accurata di misurazione del tempo rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'art. 48, paragrafo 2.

- l'identificativo della funzione di hash utilizzata per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
- il valore dell'impronta dell'evidenza informatica del documento

Le marche temporale hanno una validità minima garantita di venti anni o per un periodo superiore previo accordo con il prestatore di servizi.

La richiesta di marca temporale avviene con la seguente procedura informatica:

- applicazione della funzione di *hash* al documento al quale va associata la marca e generazione dell'impronta a 256 *bit*;
- invio dell'impronta al prestatore di servizi fiduciario qualificato con la richiesta di marca temporale;
- generazione, firma e trasmissione della marca al richiedente;
- associazione al documento informatico

Ai sensi dell'art. 41, comma 4, del D.P.C.M. 22 febbraio 2013 costituiscono riferimenti temporali opponibili a terzi:

- il riferimento temporale contenuto nella segnatura di protocollo;
- il riferimento temporale ottenuto con la procedura di conservazione di documenti informatici;
- il riferimento temporale ottenuto attraverso l'uso della Posta elettronica certificata (PEC);
- il riferimento temporale ottenuto attraverso la marcatura postale elettronica ai sensi dell'art. 14, comma 1, punto 1.4. della Convenzione postale universale.

Tali sistemi di validazione temporale, a differenza della marcatura apposta al momento della sottoscrizione, sono asincroni rispetto alla sottoscrizione nel senso che sono e possono essere apposti solo in un momento successivo rispetto alla sottoscrizione; è pertanto consigliabile utilizzare tali sistemi di validazione entro breve termine rispetto al momento della sottoscrizione.

L'importanza della validazione temporale come strumento per controllare l'efficacia giuridica di una firma elettronica qualificata o digitale è confermata anche dall'art. 3, comma 7, del D.P.C.M. 13 novembre 2014 che ha introdotto l'obbligo di attribuire a tutti i documenti informatici un riferimento temporale rappresentato dall'informazione contenente la data e l'ora sincronizzata con il tempo coordinato universale.

I.5 LA FORMAZIONE DEL DOCUMENTO INFORMATICO

L'importanza che assume il momento della formazione del documento informatico è fondamentale poiché solo la corretta formazione del documento ne garantisce la corretta gestione e conservazione. In ambiente digitale la conservazione dei documenti informatici non deve essere considerata un'attività posta in essere alla fine del processo di gestione documentale, ma deve essere considerata una fase fondamentale del processo di formazione del documento poiché è proprio in tale fase che vanno adottati tutti quegli accorgimenti

tecnologici e archivistici differenti in ragione della tipologia documentale e della destinazione. Anche nella fase di formazione del documento va pertanto richiesto l'intervento degli archivisti, a cui compete la tenuta degli archivi digitali, che devono contribuire con le loro conoscenze e abilità alla definizione delle soluzioni tecnologiche necessarie alla conservazione a lungo termine.

In primo luogo infatti va scelto il formato elettronico, escludendo quelli non idonei alla conservazione a lungo termine; vanno analizzati i singoli procedimenti per determinare quale firme utilizzare a seconda degli effetti giuridici prodotti; vanno individuati, già in fase di formazione del documento, i metadati che consentiranno in futuro la gestione, la conservazione e la fruizione dello stesso.

Per quanto riguarda la scelta del formato occorre attenersi alle indicazioni dell'allegato 2 del D.P.C.M. 3.12.2013 sulla conservazione e del D.P.C.M. 13 novembre 2014 in base al quale vanno privilegiati i formati con le seguenti caratteristiche:

- "aperti" cioè conformi a specifiche pubbliche disponibili a chiunque abbia interesse ad utilizzare quel formato;
- "non proprietari" cioè formati che sono indipendenti dalle piattaforme tecnologiche utilizzate per la formazione dei documenti;
- "robusti" in grado di recuperare in tutto o in parte il contenuto del file eventualmente corrotto o danneggiato;
- "stabili" cioè compatibili con le versioni precedenti e future;
- "sicuri" in relazione al grado di protezione dai virus;
- non contenenti macroistruzioni.

I formati da privilegiare per la conservazione a lungo termine sono pertanto i seguenti in relazione alla diversa tipologia documentale:

- PDF
- PDF/A
- TIFF utilizzato per la memorizzazione delle immagini;
- ODF
- OOXML
- XML
- TXT
- RFC 2822/MIME per i messaggi di posta elettronica

La scelta del formato deve essere indicata nel Manuale di gestione di ciascun ente che, in quanto documento pubblico, rende i terzi (cittadini, imprese, studenti…) informati su quali formati possono e devono essere utilizzati per la produzione dei documenti.

Come già accennato per una corretta formazione degli archivi digitali è necessario associare al documento informatico, in fase di formazione, i relativi metadati: *"Essi costituiscono una componente fondamentale dell'archivio digitale in quanto descrivono le unità che ne fanno parte, permettendone la ricerca e l'acquisizione, forniscono le indicazioni che ne assicurano*

l'accessibilità nel rispetto delle norme in materia di privacy, documentano le attività che le hanno riguardate sia durante la fase di gestione che in quella successiva di conservazione"[7].
Per quanto riguarda la scelta dei metadati occorre riferirsi a quanto indicato dall'allegato 5 dei predetti D.P.C.M. che individuano *l'insieme mimino* di metadati del documento informatico, del documento amministrativo informatico (inteso il documento protocollato ai sensi dell'art. 53 del D.P.R. 445/2000), e del fascicolo informatico[8].
In tema di formazione del documento informatico merita un particolare approfondimento l'art. 3 del D.P.C.M. del 13 novembre 2014 che elenca le modalità con cui può formarsi un documento informatico che soddisfi i requisiti di integrità e immodificabilità; occorre pertanto far riferimento a queste disposizioni per scegliere la modalità di redazione adatta alle nostre esigenze:
1) documento informatico creato con appositi strumenti software; per tali tipi di documenti le caratteristiche di immodificabilità e integrità sono garantite da una o più delle seguenti operazioni:

---

[7] S. PIGLIAPOCO *Progetto Archivio Digitale-Metodologia Sistemi Professionalità* CIVITA 2016, pag.72

8 In particolare per quanto riguarda il documento informatico l'insieme dei metadati minimi è costituito da:
a) l'identificativo univoco e persistente;
b) il riferimento temporale rappresentato dalla data e ora sincronizzata con il tempo coordinato e universale (UTC);
c) l'oggetto;
d) il soggetto che ha formato il documento;
e) l'eventuale destinatario;
f) l'impronta del documento informatico generata con la funzione di HASH SHA-256
Eventuali ulteriori metadati sono definiti in funzione del contesto e delle necessità gestionali e conservative.

Per quanto riguarda il documento amministrativo informatico l'insieme dei metadati è costituito dai seguenti dati in parte contenuti già nella segnatura di protocollo:
a) codice identificativo dell'amministrazione;
b) codice identificativo dell'area organizzativa omogenea;
c) codice identificativo del registro nel quale sono annotati i documenti;
d) data di protocollo generata automaticamente dal sistema;
e) numero progressivo di protocollo generato automaticamente dal sistema;
f) oggetto del documento;
g) dati identificativi del mittente per i documenti ricevuti o del destinatario/i per i documenti inviati;
h) data e numero di protocollo del documento ricevuto, se disponibili;
i) impronta del documento informatico, se trasmesso per via telematica;
j) indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento;
k) indici di classificazione;
l) identificazione degli allegati;
m) informazioni sul procedimento a cui afferisce e sul trattamento da applicare al documento.

L'insieme minimo dei metadati da associare alle aggregazioni documentali informatiche (ADI) o ai fascicoli informatici comprende:
a) codice identificativo dell'amministrazione titolare;
b) codice identificativo dell'AAOO e dell'unità organizzativa produttrice del fascicolo/ADI;
c) codice identificativo univoco e persistente del fascicolo/ADI costituito dal numero progressivo del fascicolo all'interno della classe di titolario; (a differenza del numero di protocollo a fine anno non si azzera);
d) oggetto del fascicolo/ADI;
e) data di costituzione o apertura del fascicolo/ADI;
f) data di conclusione o chiusura del fascicolo/ADI;
g) elenco dei codici identificativi dei documenti che afferiscono al fascicolo/ADI;

- sottoscrizione con firma qualificata o digitale;
- apposizione di una validazione temporale
- trasferimento a terzi con pec con ricevuta completa;
-memorizzazione su un sistema di gestione documentale che adottino idonee politiche di sicurezza;
-versamento in un sistema di conservazione
2) documento informatico acquisito per via telematica o su supporto informatico (es. messaggi ricevuti via mai o pec), o il documento ottenuto mediante un processo di digitalizzazione di documenti analogici. Per tali tipi di documenti le caratteristiche di immodificabilità e integrità sono garantite con dalla memorizzazione del documento in un sistema di gestione informatica dei documenti o in un sistema di conservazione;
3) generazione di un insieme di dati o registrazioni, provenienti da una o più base di dati, secondo una struttura logica predeterminata e memorizzata in forma statica; rientra in questa ipotesi la raccolta telematica di dati attraverso formulari in rete; in questo caso le caratteristiche di immodificabilità e integrità sono realizzate attraverso la conservazione della base di dati e dei relativi log di sistema, oppure mediante l'estrazione statica di dati trasmessi ad un sistema di conservazione.
In tutti i casi ai sensi dell'art. 3, comma 7, laddove non sia già presente al documento informatico immodificabile è associato un riferimento temporale.

I.6 IL DECRETO CORRETTIVO DEL CAD

In data 12 gennaio 2018 è stato pubblicato in Gazzetta Ufficiale (GU n.9 del 12-1-2018) il Decreto Legislativo 13 dicembre 2017, n. 2017 recante "*Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche e integrazioni al Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n 82, ai sensi dell'art. 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"*. Il decreto entra in vigore dal 27 gennaio 2018.
Ai fini del presente Manuale è opportuno rilevare che sono stati riformulati gli artt. 20 e 21 del CAD in tema di documento e firme elettroniche; oltre alla FD, FEQ e alla FEA è stato introdotto un nuovo processo di firma. E' quello che prevede che il documento sia formato "*previa identificazione del suo autore, attraverso un processo avente i requisiti fissati dall'AgID in base all'art. 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore*".
Si tratta in sostanza di un nuovo processo di firma elettronica "avanzata" che sarà presumibilmente realizzato con SPID, il sistema di identificazione digitale già introdotto nel 2016.
Il legislatore manifesta la volontà di valorizzare lo SPID e l'art. 64 risulta così integrato "*L'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica avviene tramite SPID*". Il nuovo art. 65 prevede inoltre che le

istanze e le dichiarazioni possono essere trasmesse alla pubblica amministrazione in una delle forme di cui all'art. 20 e quindi con il nuovo processo di firma elettronica avanzata che prevede l'uso di SPID.
La disciplina dei documenti informatici sottoscritti con FD, FQ e FEA sostanzialmente rimane invariata; tutti integrano la forma scritta e hanno l'efficacia probatoria della scrittura privata ex art. 2702 del c.c., senza spazio per la valutazione del giudice.
La validità giuridica dei documenti informatici senza firma o sottoscritti con firma elettronica debole rimangono liberamente valutabili in giudizio sulla base dei criteri di qualità, sicurezza, integrità e immodificabilità.
E' inoltre confermato il principio della presunzione che l'utilizzo del dispositivo di firma, nella FD e nella FQ, sia riconducibile al titolare salvo che questi dia prova contraria.

CAPITOLO II

Il servizio di firma digitale all'interno dell'Università degli Studi di Genova

II.1 REGOLAMENTO DI ATENEO IN MATERIA DI FIRMA DIGITALE

Nel rispetto del quadro normativo nazionale e dell'Unione Europea, l'Università degli Studi di Genova ha emanato un proprio regolamento interno per disciplinare le modalità di rilascio, gestione e utilizzo della firma digitale; tale Regolamento è pubblicato nel sito dell'Università degli Studi di Genova nella sezione Regolamenti - Altri Regolamenti.

Al fine di agevolare il rilascio dei certificati qualificati su tutto il territorio in cui opera l'Ateneo genovese, il Regolamento prevede che all'interno di ciascuna struttura vi sia un "*incaricato di Ateneo*" - che opera su espressa delega del "*prestatore di servizi fiduciari*" - con il principale compito di procedere all'identificazione del richiedente, al rilascio del certificato qualificato e alla contestuale consegna dei codici segreti.

Il Regolamento prevede inoltre una struttura piramidale all'interno della quale gli incaricati di Ateneo sono identificati e coordinati, da un punto di vista gestionale, dal "*primo incaricato*" di Ateneo e, da un punto di vista tecnico informatico, dal "*referente informatico".*

Nel Regolamento è illustrata la procedura per procedere all'identificazione del titolare e alla registrazione dell'utente sul *software* fornito dal prestatore di servizi; sono indicate altresì, in conformità alla normativa vigente, le cause e le modalità di revoca, sospensione e riattivazione del certificato qualificato. In particolare la procedura prevede che il certificato possa essere sospeso, appena si renda necessario, dal titolare di firma (mediante chiamata al numero verde del prestatore di servizi) o dall'incaricato (operando sul *software*) in modo da evitarne qualunque uso fraudolento; la sospensione viene poi comunicata al "primo incaricato di Ateneo" che provvederà, per il tramite del prestatore di servizi, alla revoca definitiva con pubblicazione del nuovo stato sulle CRL.

Ai sensi dell'art. 3 del Regolamento di Ateneo e del DR 51 del 8.02.2013 possono essere titolari di firma digitale gli appartenenti alle seguenti categorie, in ragione della funzione che svolgono all'interno dell'Ateneo:

- **titolari di diritto:** Rettore, Prorettore, Delegati del Rettore, Direttore Generale, Presidi di Scuola, Direttore di Dipartimento, Presidente e Direttore del Centro di Servizi Bibliotecario, di CSITA (ora Cedia) e dei Centri di Servizio, Centri universitari, interuniversitari e di eccellenza; Presidenti e Direttori della Biblioteca di Scuola; Dirigenti e Capi Servizio dell'Amministrazione Centrale; Responsabili Amministrativi/Segretari Amministrativi delle Scuole e di Dipartimento;
- **su autorizzazione del Direttore del Dipartimento**: personale docente (professori ordinari, associati, ricercatori, professori a contratto) in relazione alle attività di didattica e ricerca;

Per sopperire a specifiche e motivate esigenze di servizio il certificato di firma digitale può essere rilasciato ad altri dipendenti di Ateneo su autorizzazione del Rettore (per il personale docente) o Direttore Generale (per il personale tecnico amministrativo).

II.2 LA FIRMA DIGITALE RILASCIATA DALL'ATENEO

L'apposizione della firma con il certificato qualificato rilasciato dall'Ateneo genovese realizza una vera e propria firma digitale (FD) con gli effetti giuridici trattai al capitolo I.3; in particolare, trattandosi di firma basata sulla crittografia asimmetrica a chiave pubblica e privata, garantisce l'autenticità, l'integrità e il non ripudio del documento.

La chiave privata del certificato qualificato è contenuta nel dispositivo sicuro che è rappresentato dalla SIM (numero cellulare) alla quale viene associato il codice fiscale del titolare. Non è pertanto necessario procedere al rilascio di un nuovo certificato di firma digitale in caso di cambio del gestore telefonico se la SIM (numero di cellulare) rimane la stessa.

Le fasi per la generazione della firma digitale, dal lato utente, possono essere così riassunte:

- caricare il documento da firmare su apposito software e richiedere la firma digitale;
- telefonare al numero verde visualizzato sullo schermo;
- a specifica richiesta digitare il codice OTP (di quattro cifre) visualizzato sullo schermo;
- a specifica richiesta digitare il PIN personale (di otto cifre) rilasciato dall'incaricato di Ateneo al momento del rilascio del certificato qualificato;

L'autenticazione è quindi garantita:

- dalla telefonata che al numero verde che riconosce il numero chiamante (associato al codice fiscale al momento dell'identificazione);
- dalla digitazione del codice OTP fornito dal sistema che associa temporaneamente la chiamata all'operazione di firma di quel documento;
- dalla digitazione del codice PIN personale che consente di apporre la firma digitale in sicurezza.

Le fasi per la generazione della firma digitale, dal lato *Certification Authority*, possono essere così riassunte:

- a fronte della richiesta di firma di un documento informatico generazione dell'impronta digitale mediante la funzione di *hash*;
- cifratura con la chiave privata dell'impronta digitale: in questo modo la firma risulterà legata, attraverso la chiave privata, al sottoscrittore e, attraverso l'impronta, al documento;
- apposizione della firma digitale all'interno della busta informatica insieme al certificato del firmatario al fine di poter effettuare le operazioni di verifica.

II. 3 FIRMA CADES E PADES

Una firma digitale può essere apposta con modalità diverse: le più diffuse sono le firme CAdES e PAdES. Abbiamo già visto nel paragrafo precedente che con l'apposizione di una firma digitale si crea la cd "*busta crittografica*" che è un *file* che al racchiude al suo interno il documento originale, la firma digitale e la chiave di verifica che è contenuta nel certificato del sottoscrittore.

La busta che si crea utilizzando una firma CAdES è un *file* con estensione *.p7m*, il cui contenuto è visualizzabile solo utilizzando idonei software in grado di "sbustare" il documento sottoscritto; presenta quindi il vantaggio di essere in grado di firmare qualsiasi formato di documento ma ha lo svantaggio che il destinatario del documento avrà bisogno dell'installazione sul pc di un software specifico.

La firma digitale PAdES genera un file con estensione *.pdf* leggibile con i comuni *reader* disponibili per questo formato, ma può essere utilizzata solo per firmare file *.pdf*.

Un altro vantaggio che presenta questo tipo di firma è il fatto che consente di gestire diverse versioni dello stesso documento senza invalidare le firme digitali apposte; consente cioè di apportare modifiche al documento sottoscritto, come ad esempio i dati degli estremi di protocollo che sono disponibili solo successivamente alla sottoscrizione del documento stesso. Occorre però prestare attenzione perché ad una prima lettura il file potrebbe apparire corrotto in quanto modificato dopo la firma, tuttavia nella busta PAdES rimane presente ed accessibile anche la versione non modificata del documento che conserva piena efficacia giuridica[9].

In conclusione per scegliere se apporre una firma CAdES o PAdES occorre preliminarmente far riferimento al destinatario del documento ed accertarsi che, in caso di firma CAdES, sia in possesso di idonei strumenti alla lettura; per tale motivo in tema di pubblicazione di provvedimenti sui siti delle Pubbliche Amministrazioni è consigliata la firma PAdES.

Per lo scambio di documenti tra le Pubbliche Amministrazioni generalmente si usa la firma CAdES; l'Università degli Studi di Genova, con apposita determinazione comunicata all'Agid e pubblicata sul proprio sito, sezione News, ha espressamente dichiarato che nell'ambito di qualsiasi procedimento amministrativo accetta il formato PAdES oltre che CAdES.

[9] Per una più approfondita analisi sulle modalità di apposizione delle firme CAdES e PAdES si rinvia al documento dell'Agenzia per l'Italia Digitale *"L'apposizione di firme e informazioni su documenti firmati"* pubblicato sul sito www.agid.gov.it

II.4 FIRMIAMO IN DIGITALE

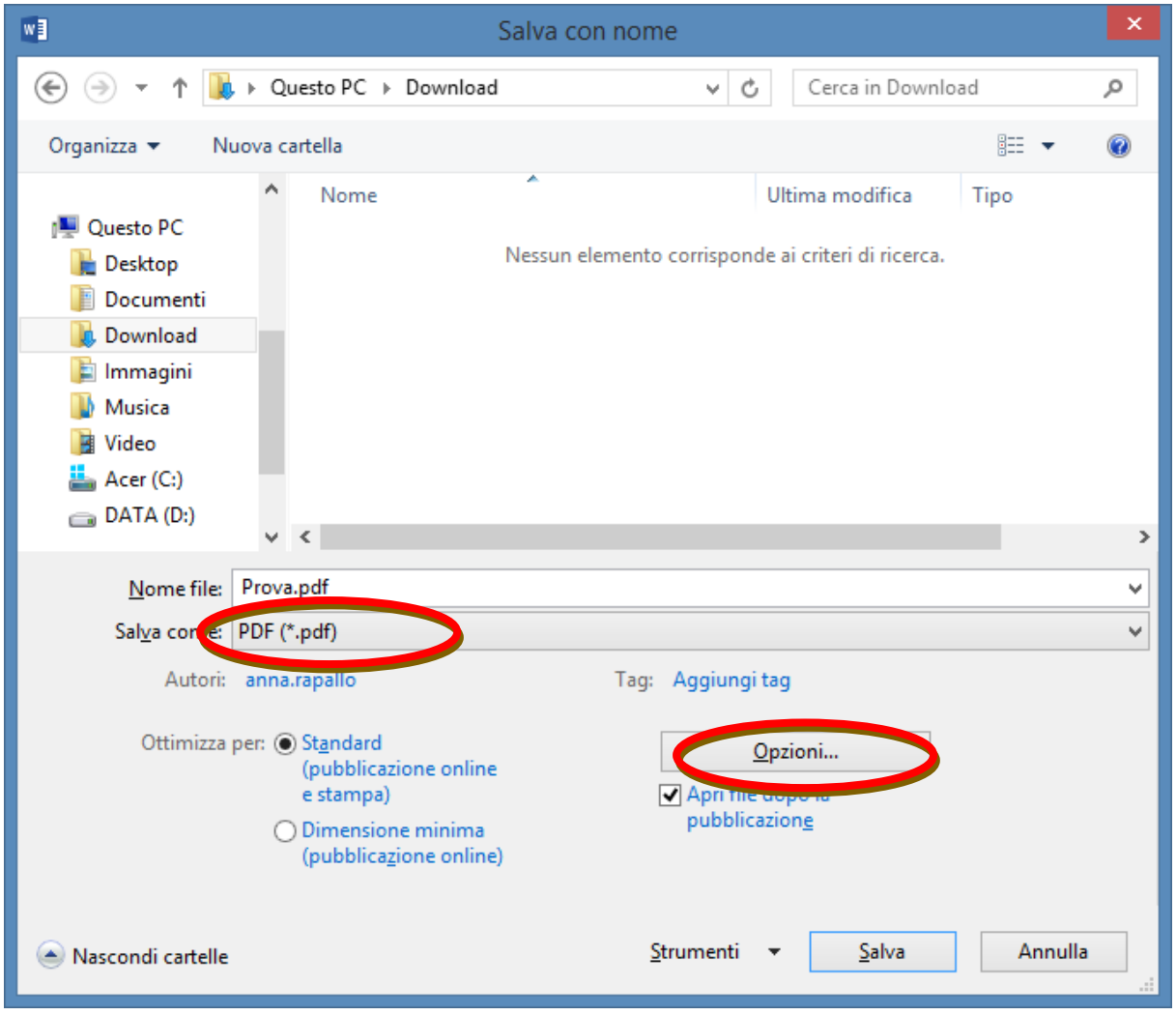
Analizziamo ora le procedure da seguire per firmare digitalmente un documento informatico che abbiamo creato e salvato sul nostro pc.

Per prima cosa dobbiamo accertarci di avere a disposizione il dispositivo di firma (cellulare) e il PIN personale di otto cifre che ci è stato rilasciato dall'Incaricato di Ateneo al momento dell'identificazione.

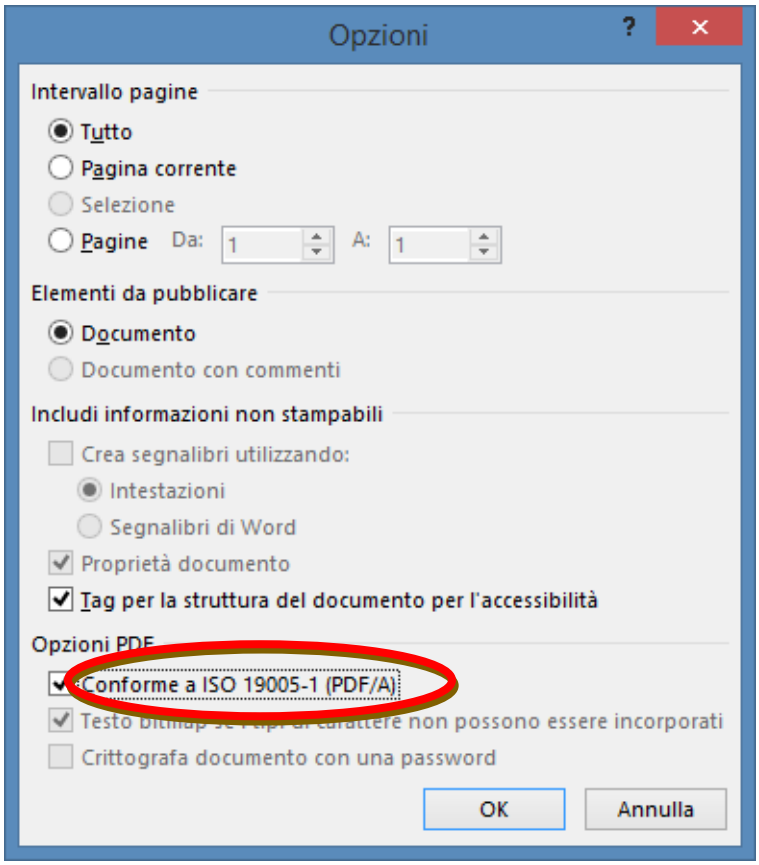
CREAZIONE DI UN PDF/A

Per prima cosa si consiglia di salvare il documento in formato .pdf/A il formato idoneo all'archiviazione seguendo la seguente procedura

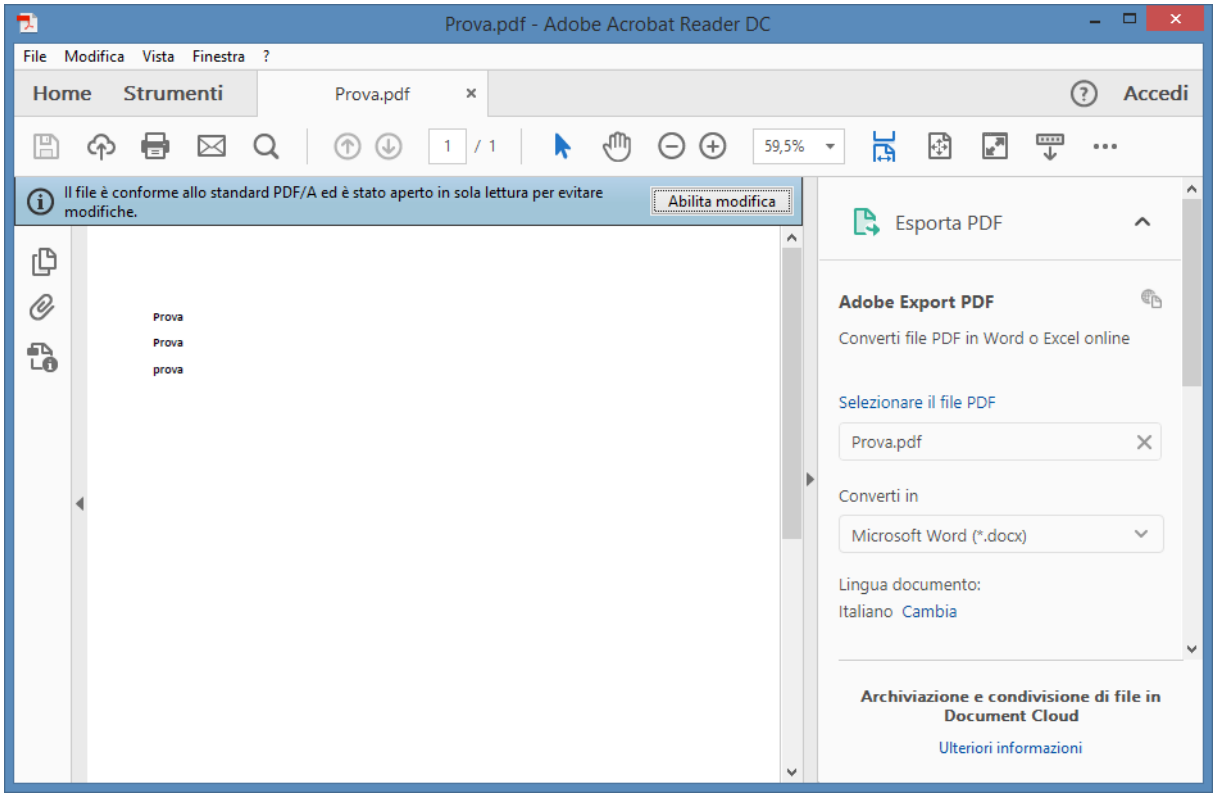
1) Creare il documento informatico es. in formato word;
2) Al momento del salvataggio cliccare su "file" – "salva con nome"
3) All'apertura della seguente schermata, dopo aver scelto dove salare il file, cliccare nel campo "salva come" e scegliere il formato PDF, poi cliccare sul tasto "opzioni";



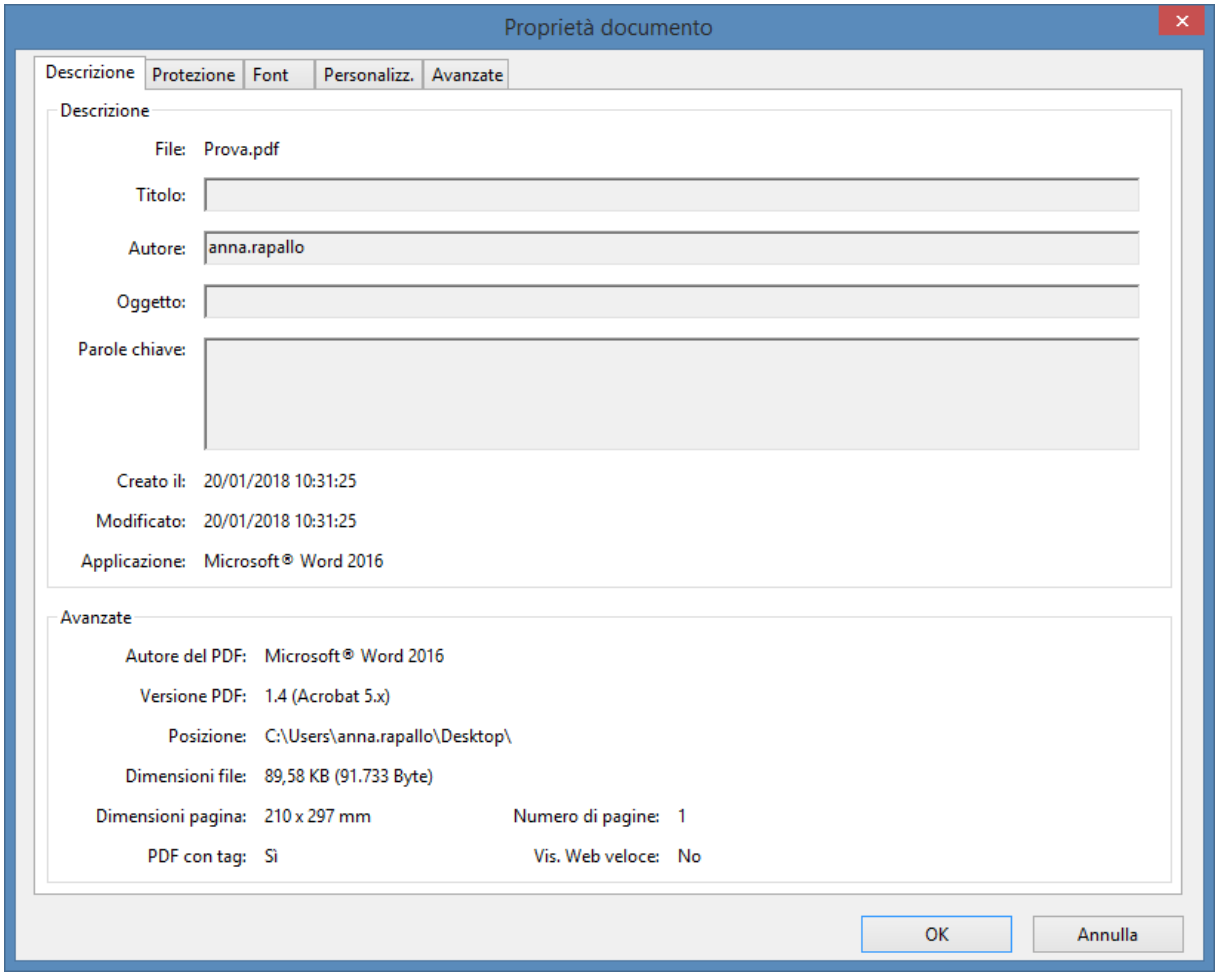
4) Nel campo opzioni PDF mettere il flag su “Conforme a ISO 19005-1 (PDF/A) e cliccare sul tasto OK



5) A questo punto il file è salvato in formato PDF/A e all’apertura risulterà così visualizzato



6) Per scopi archivistici finalizzati alla ricerca occorre inserire i cd “metadati” cliccando su “file” – “proprietà” e compilando la seguente schermata



7) Al termine della compilazione cliccare su “OK”

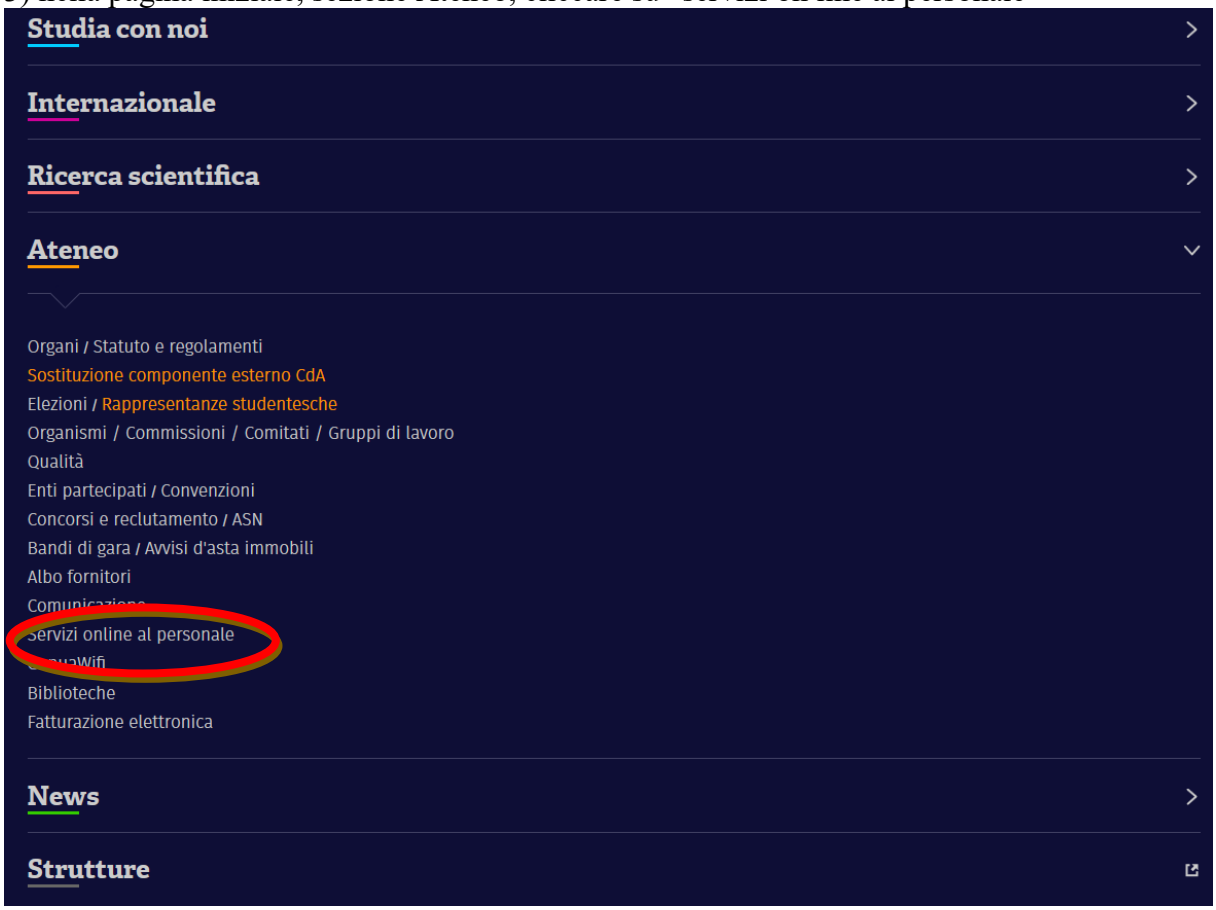
APPOSIZIONE DELLA FIRMA DIGITALE UTILIZZANDO IL SITO DI ATENEO

Come firmare digitalmente un documento utilizzando il sito di Ateneo:

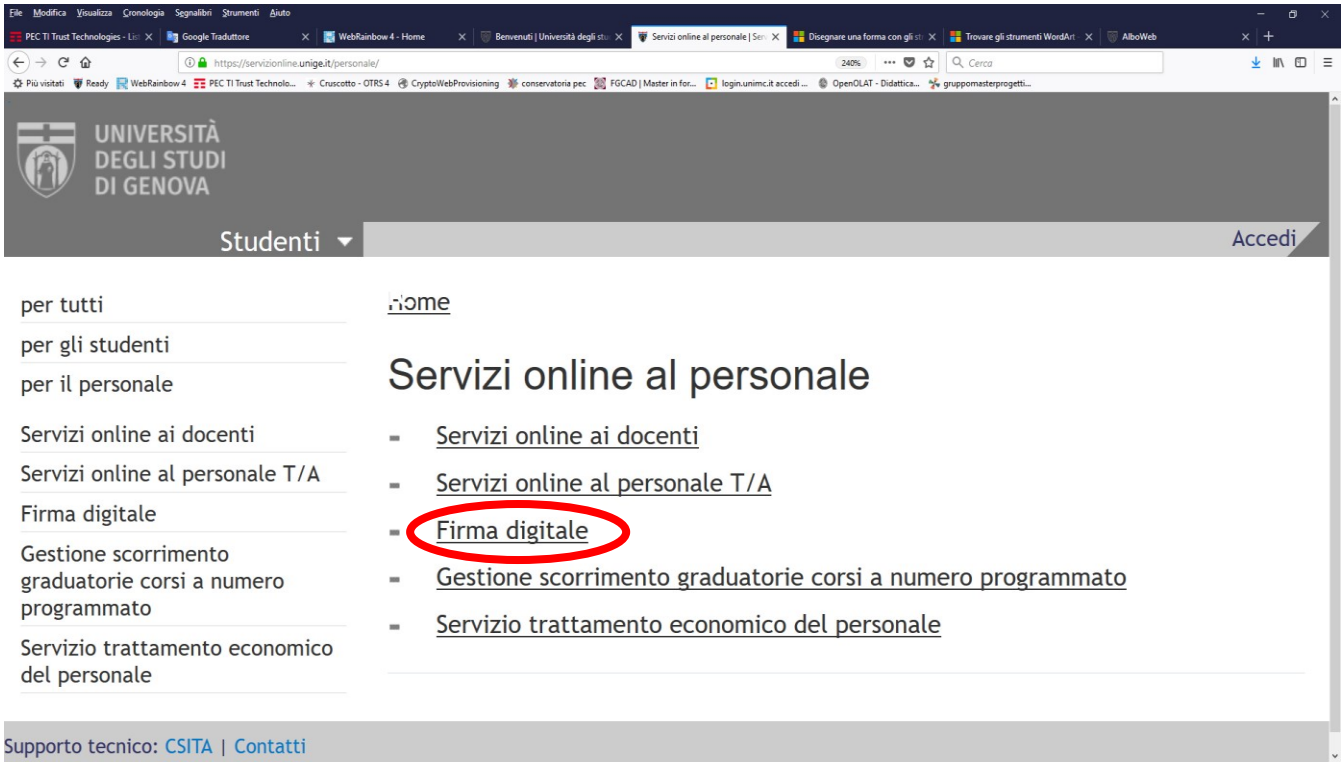
1) Preparare il documento da firmare digitalmente in formato .pdf o .pdf/a e salvarlo sul proprio desktop o in apposita cartella del proprio pc;

2) collegarsi all'indirizzo: https://unige.it e tenere a disposizione il dispositivo di firma (cellulare) e i codici PIN forniti al momento dell'attivazione della firma digitale;

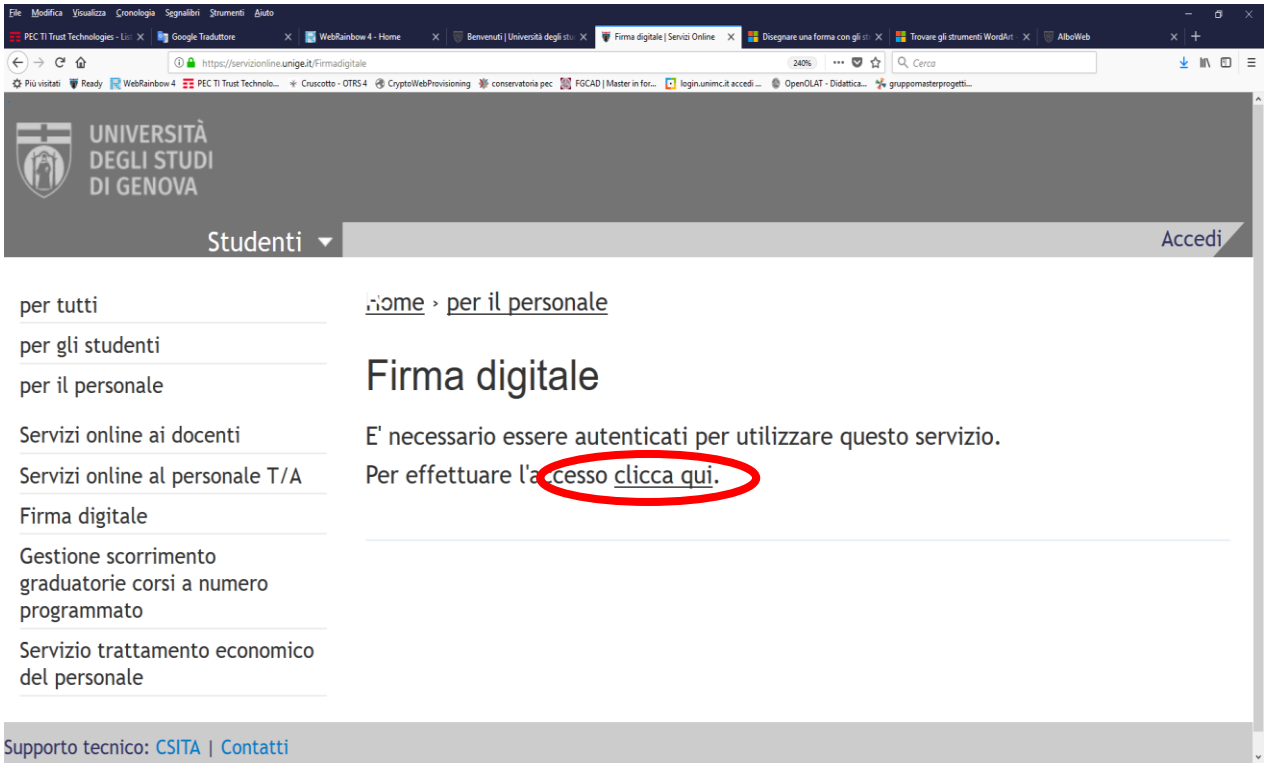
3) nella pagina iniziale, sezione Ateneo, cliccare su "servizi on line al personale"



4) cliccare su “Firma digitale”

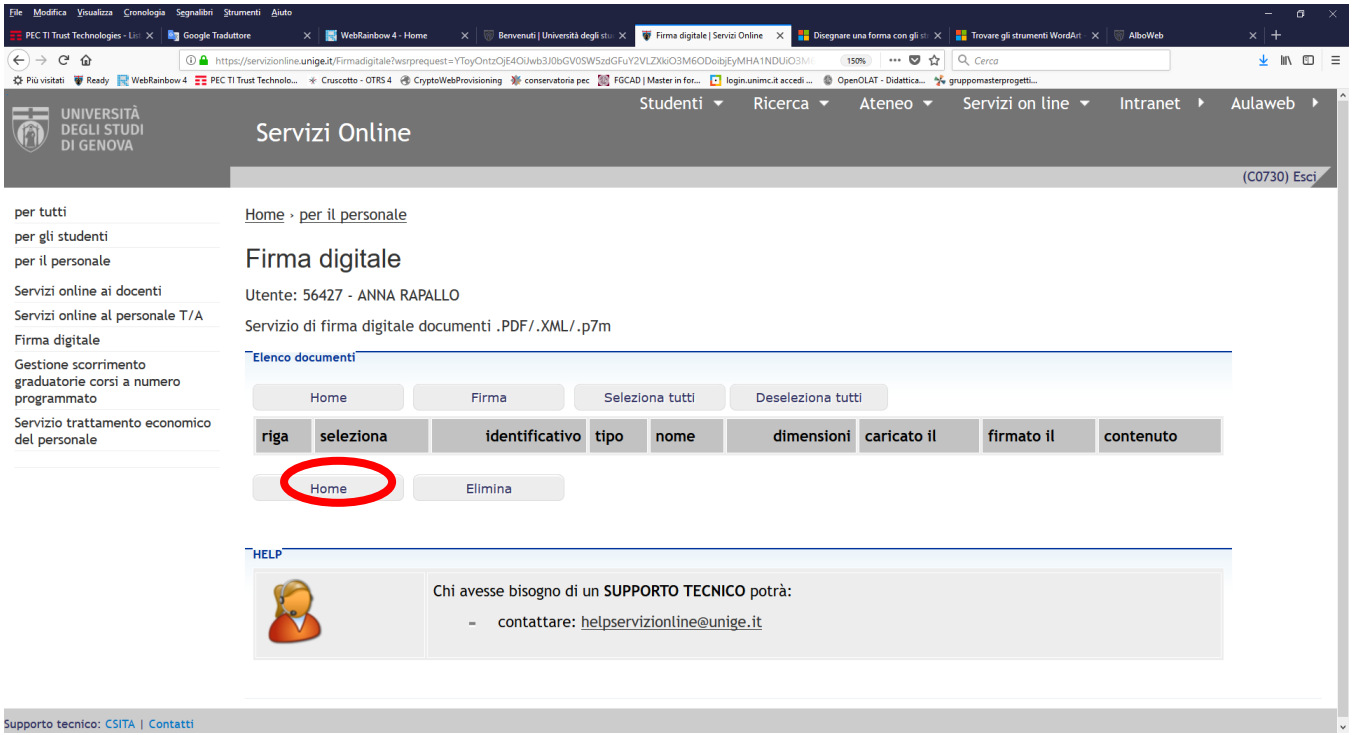


5) cliccare su “clicca qui”

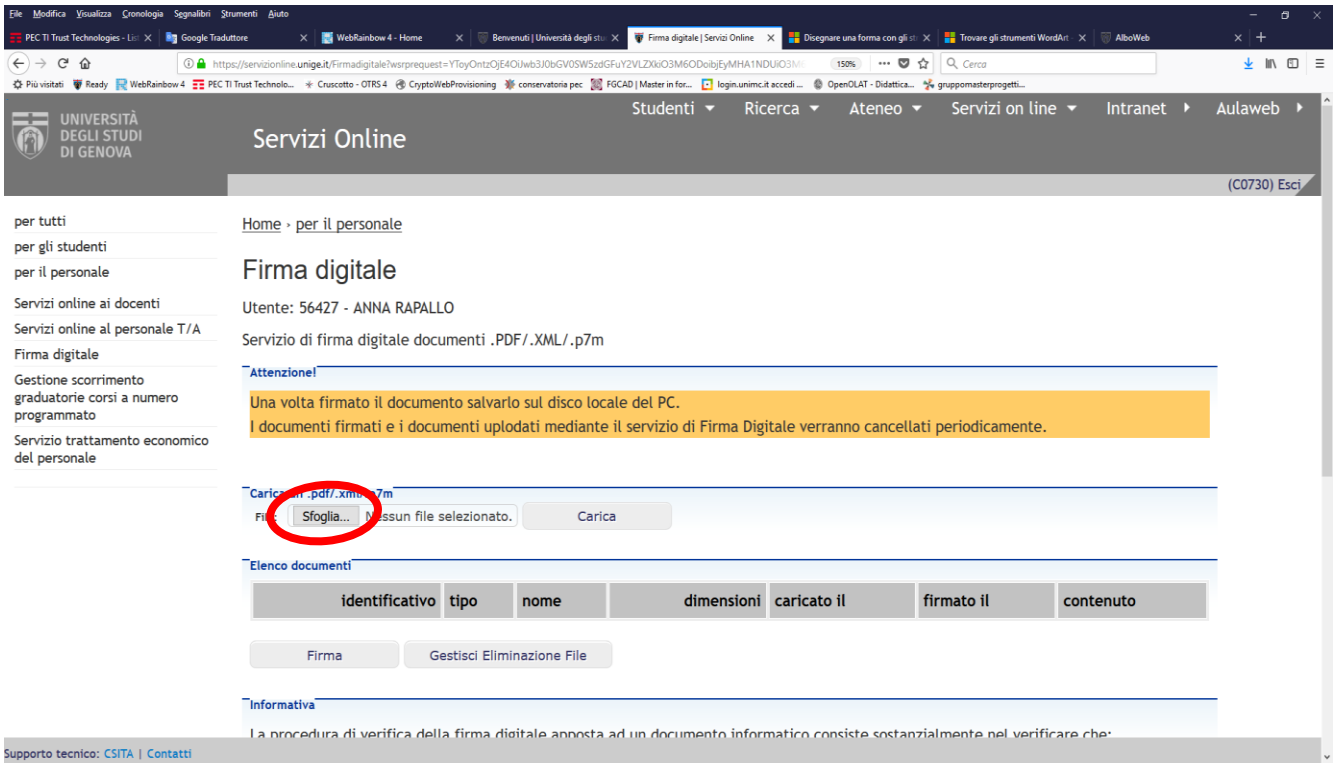


6) Inserire le proprie credenziali Unigepass (quelle utilizzate per la posta elettronica)

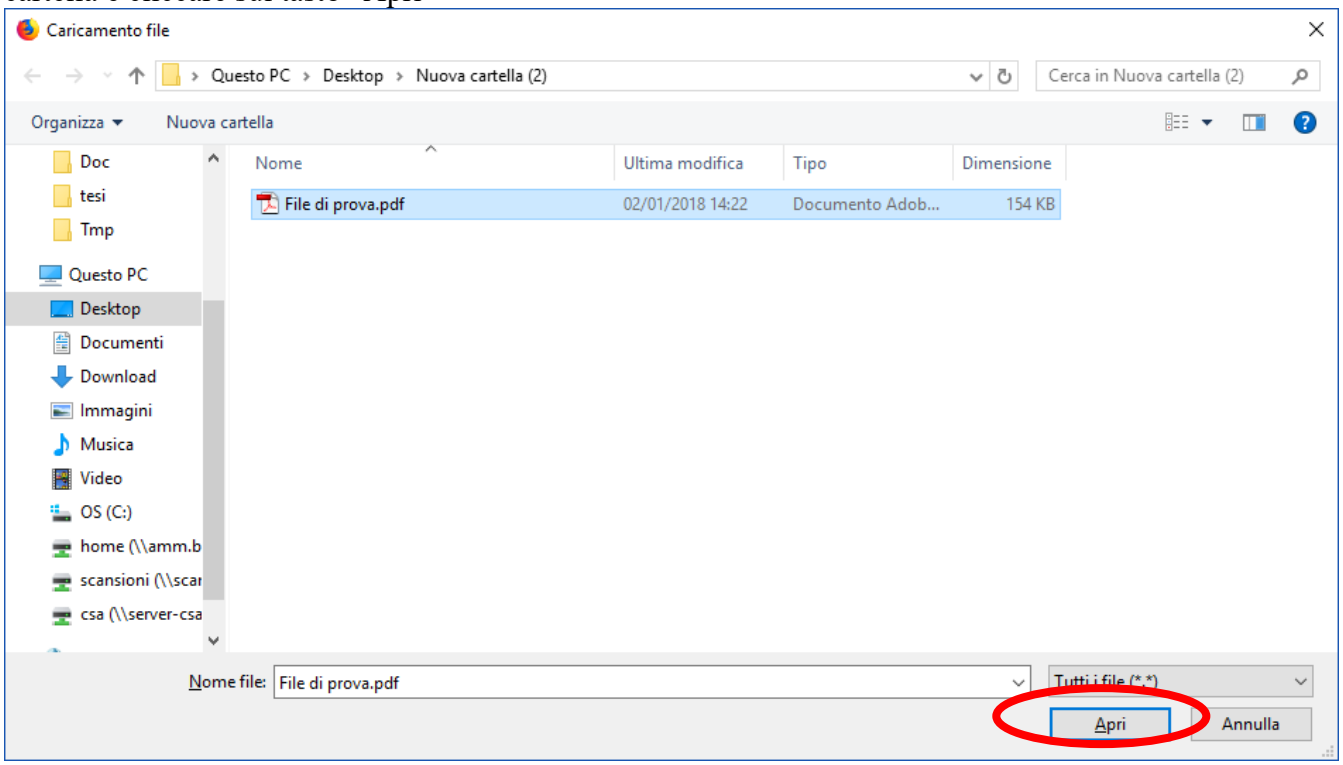
7) Si aprirà la seguente schermata nella quale dovrà essere inserito il documento da firmare digitalmente cliccando sul tasto "Home"



8) cliccare sul tasto “Sfoglia”

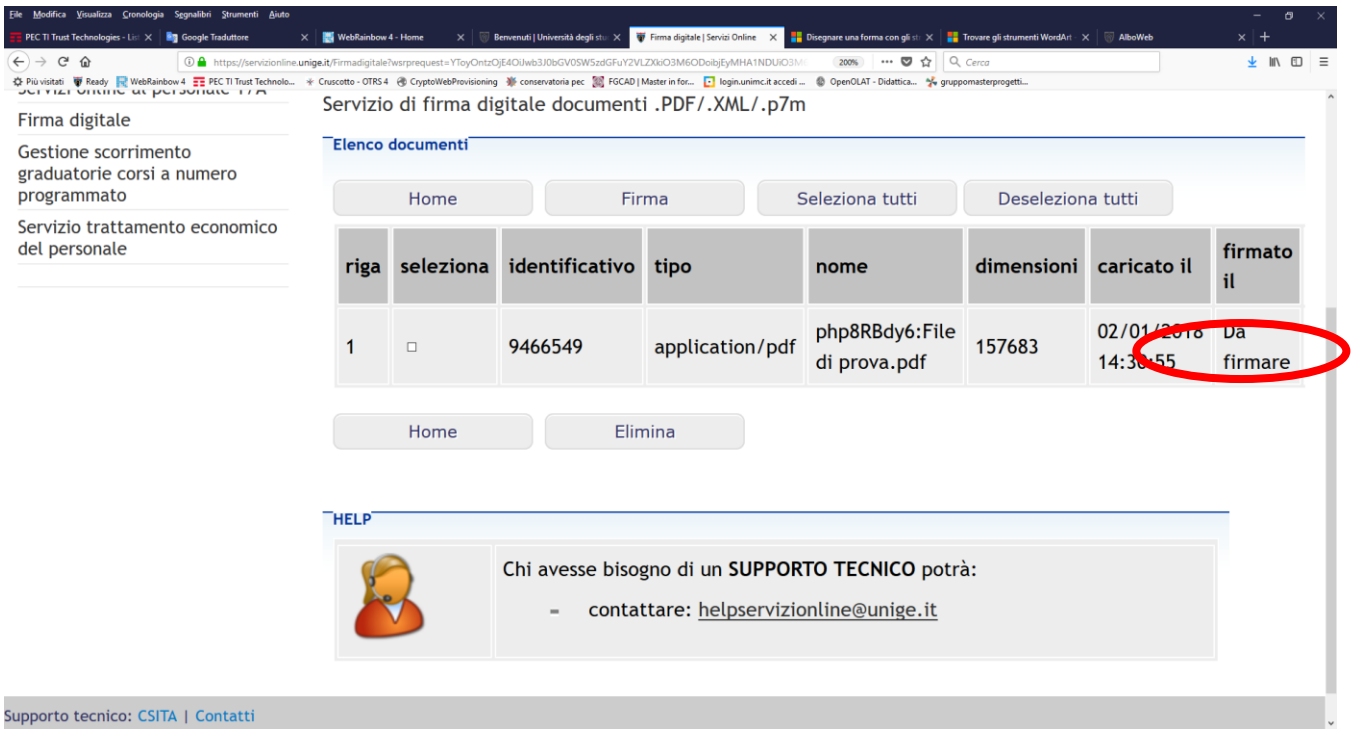


9) recuperare il documento da firmare digitalmente dal proprio desktop o nell’apposita cartella e cliccare sul tasto “Apri”

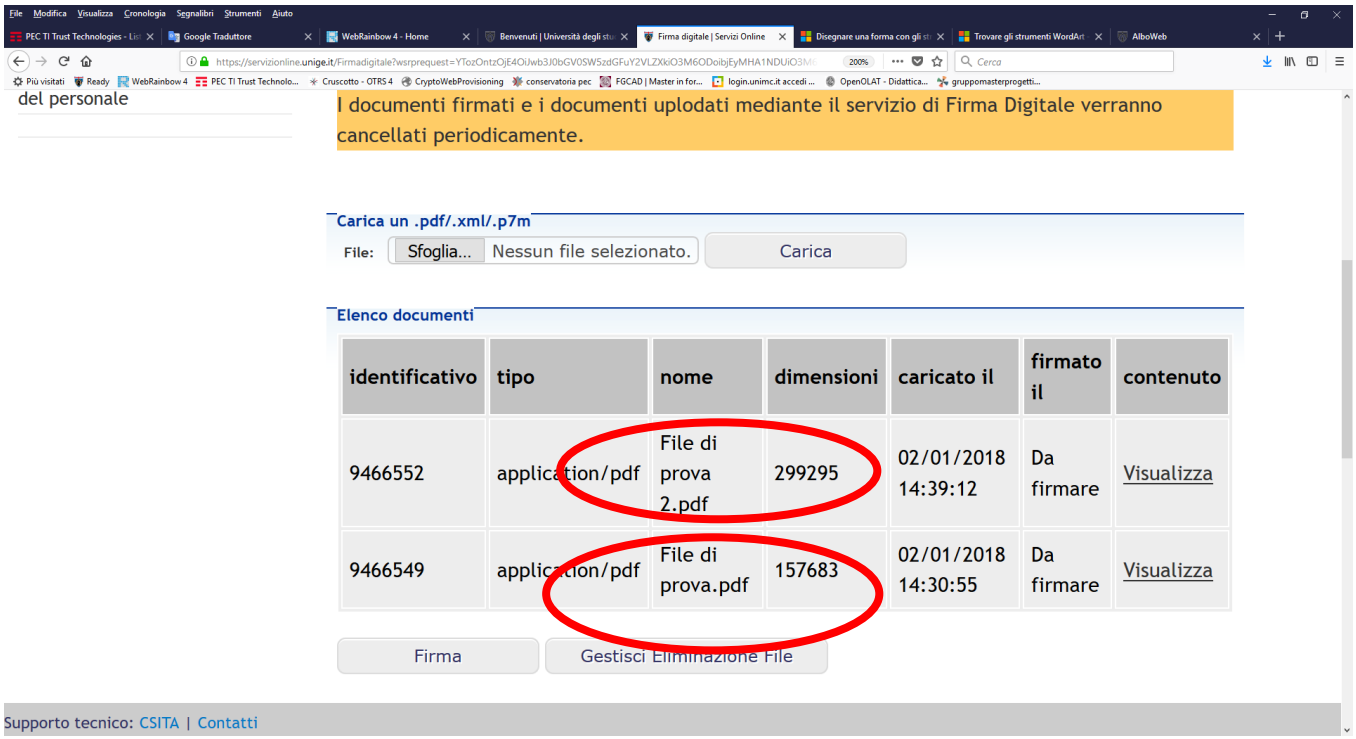


10) a questo punto il file viene visualizzato nella schermata ed occorre cliccare sul tasto "Carica"

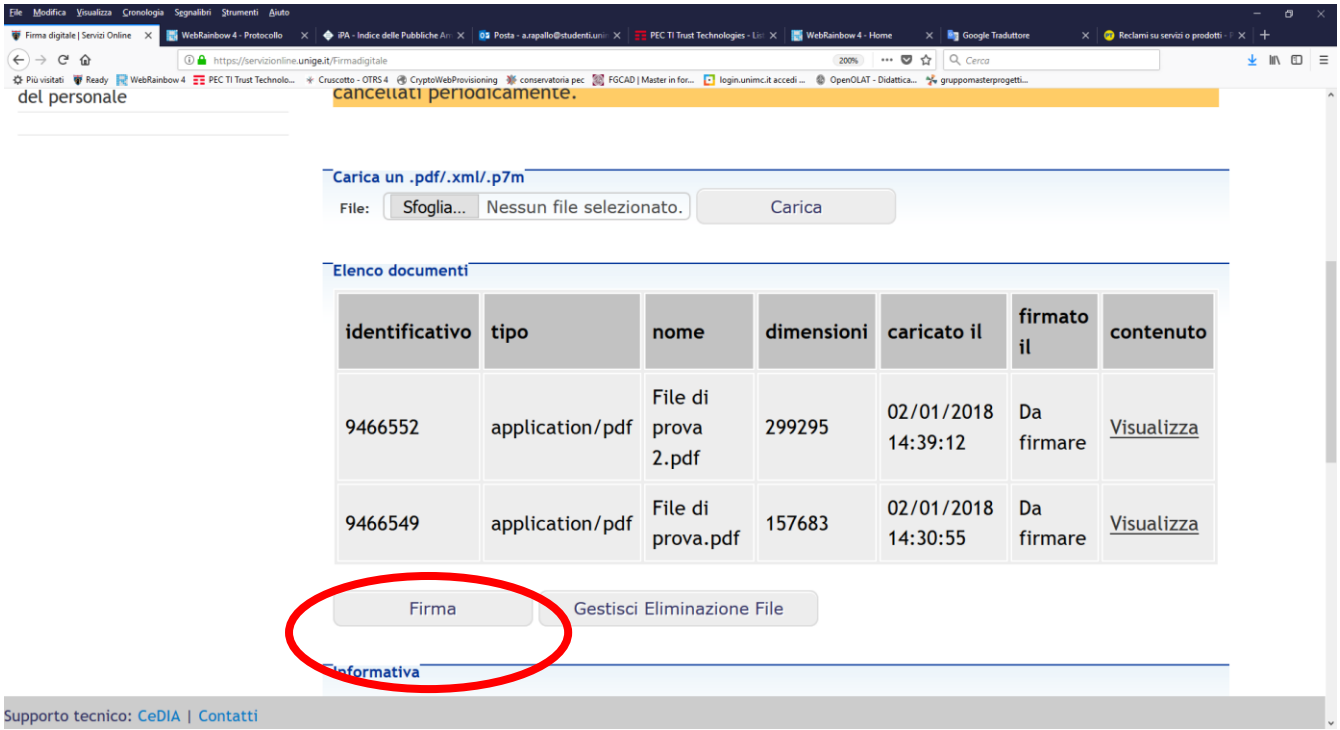
11) a questo punto il file risulta correttamente caricato ed è pronto per essere firmato;



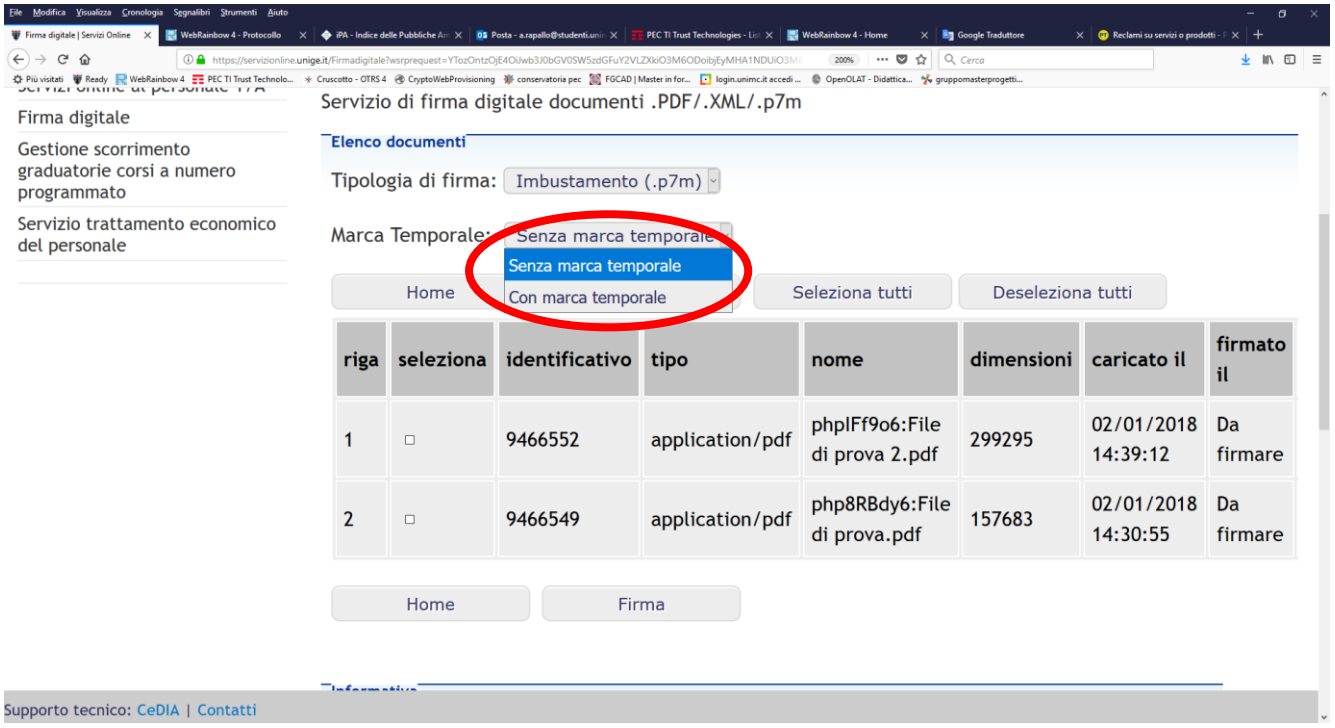
12) ripetendo la procedura indicata dal punto 7 al punto 11, possono essere caricati più file (fino ad un massimo di 50) per essere firmati insieme con un'unica telefonata o in diversi momenti



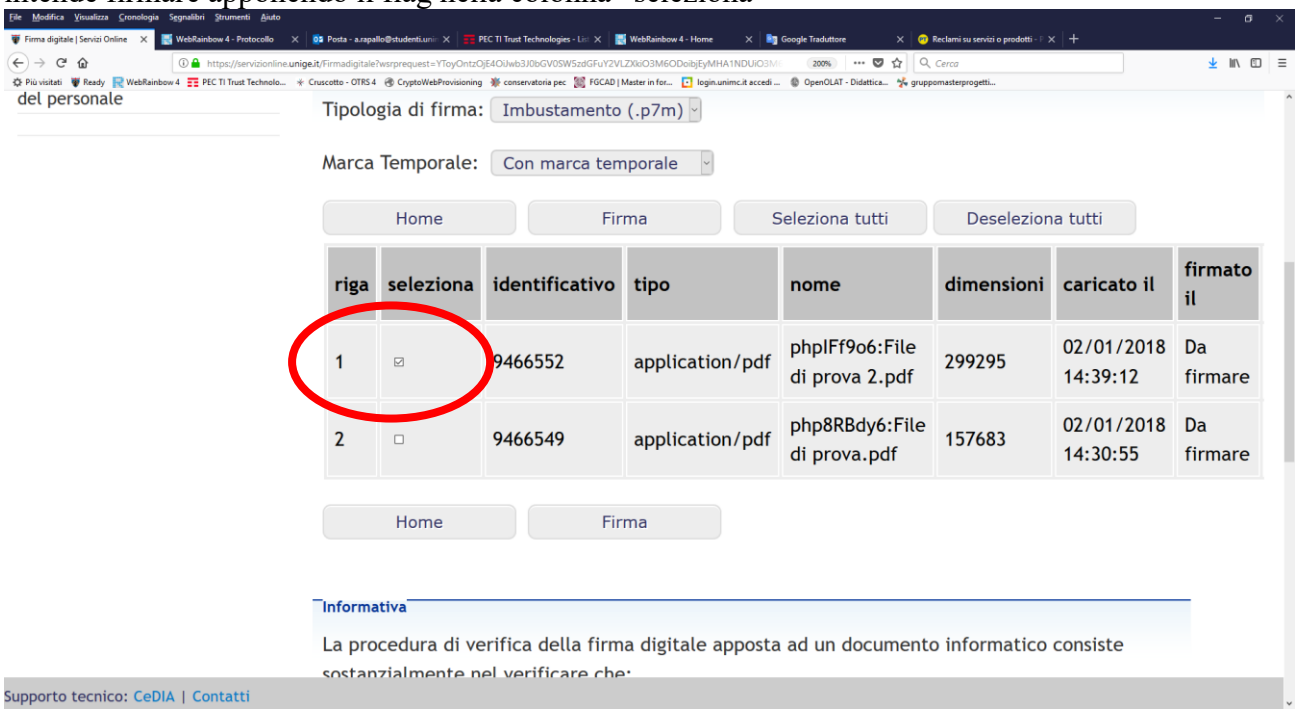
13) caricato il documento/i che si intendono firmare per procedere all'operazione di firma occorre cliccare sul tasto "Firma"



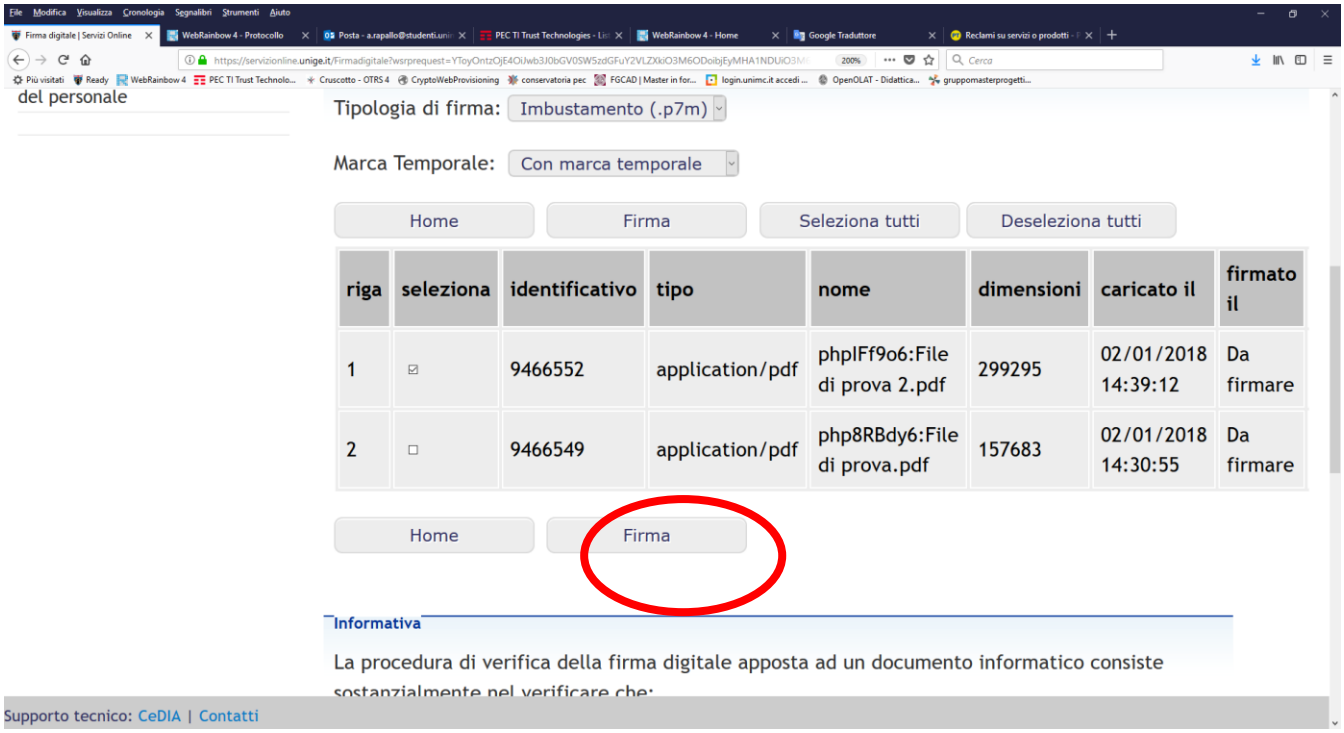
14) a questo punto compare le seguente schermata dalla quale possiamo scegliere (se preventivamente autorizzati) se firmare il documento apponendo la marca temporale o no



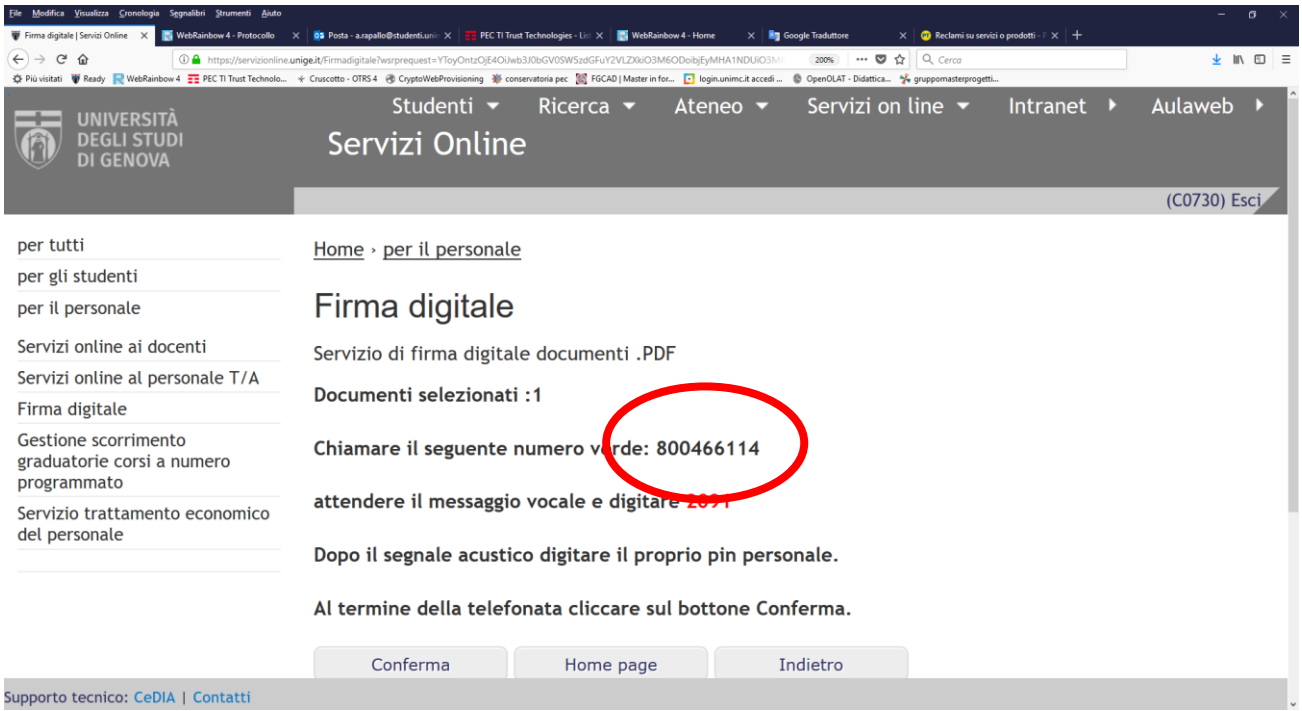
15) Una volta effettuata la scelta di cui al punto precedente selezionare il documento/i che si intende firmare apponendo il flag nella colonna “seleziona”



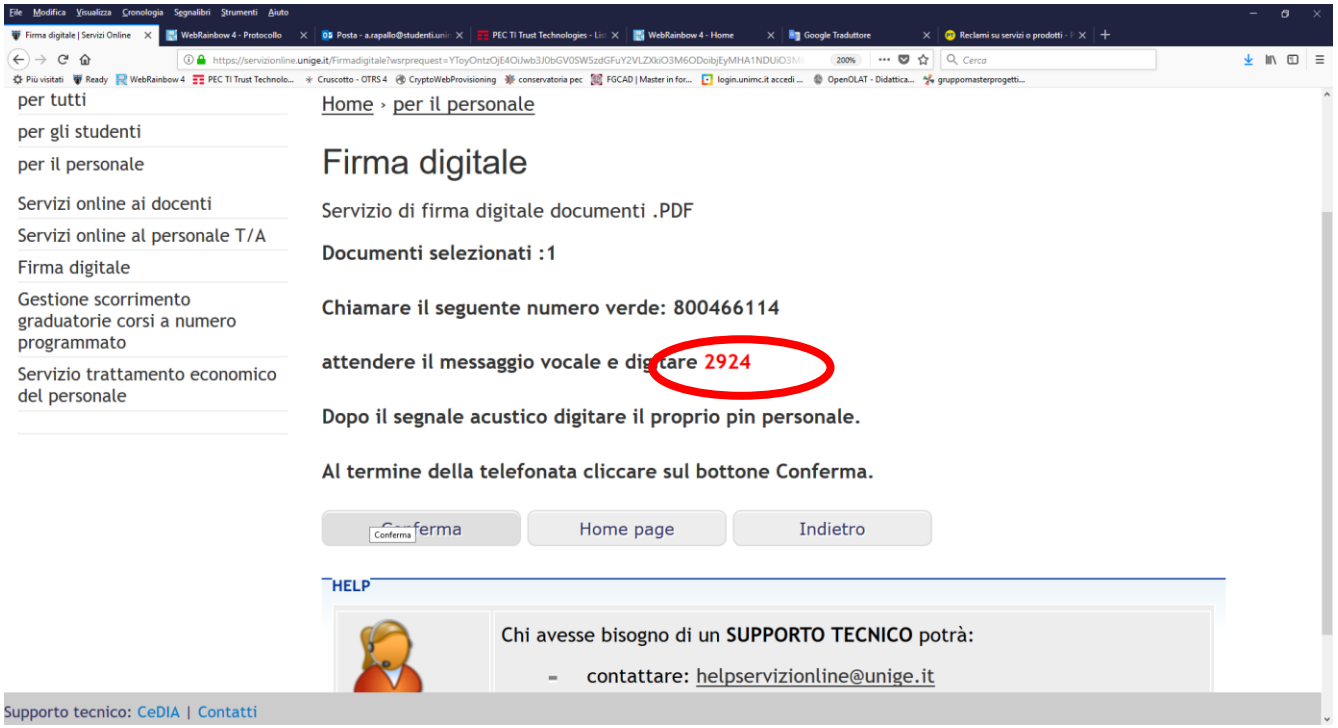
16) cliccare il tasto “firma”:



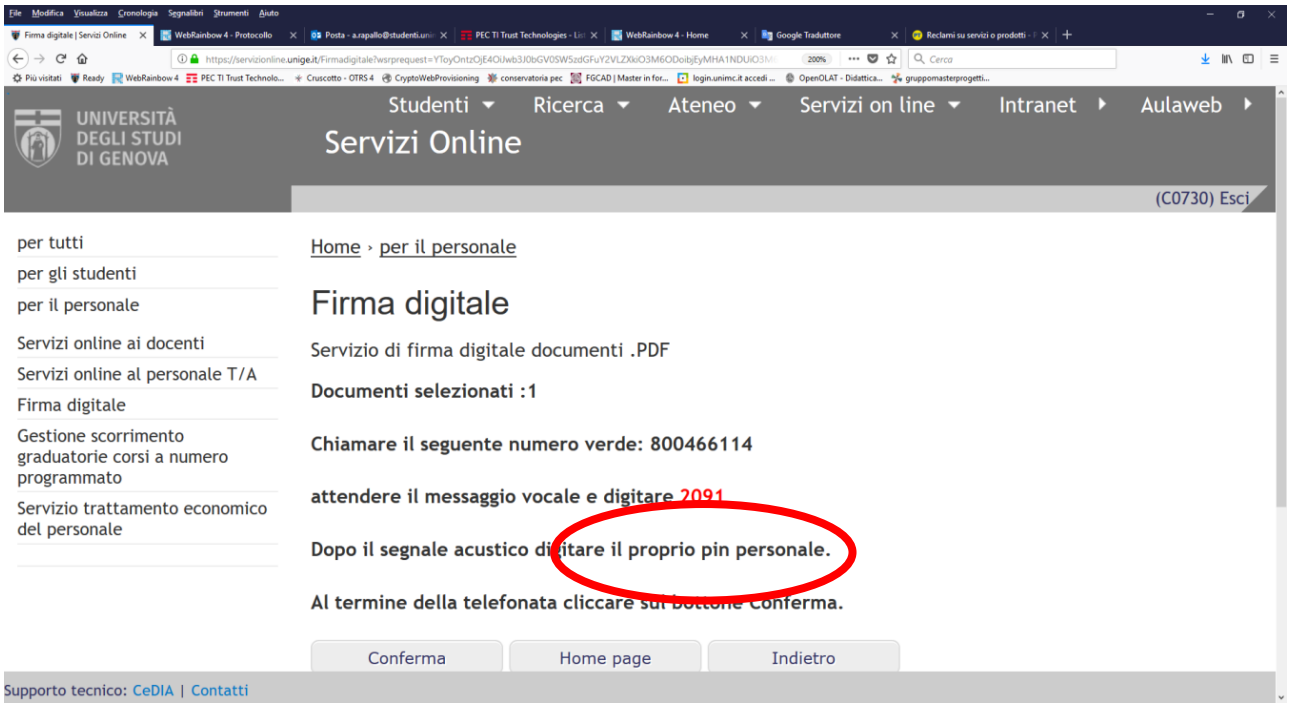
17) a questo punto compare la seguente schermata contente le indicazioni da seguire per terminare l’operazione di firma; in particolare occorre chiamare, dal cellulare abilitato, il numero di telefono indicato



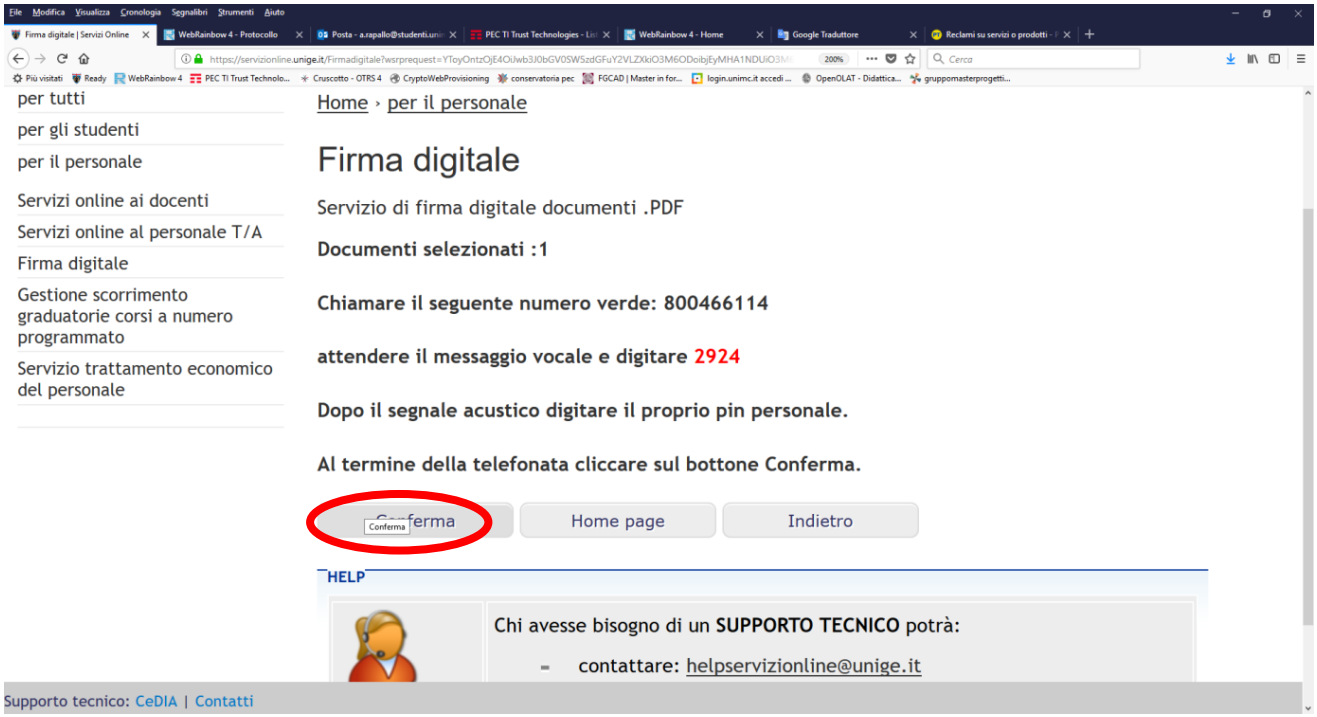
18) quando la voce registrata chiede di “digitare il codice di quattro cifre che vi è stato indicato” va selezionato, sul cellulare, il codice evidenziato



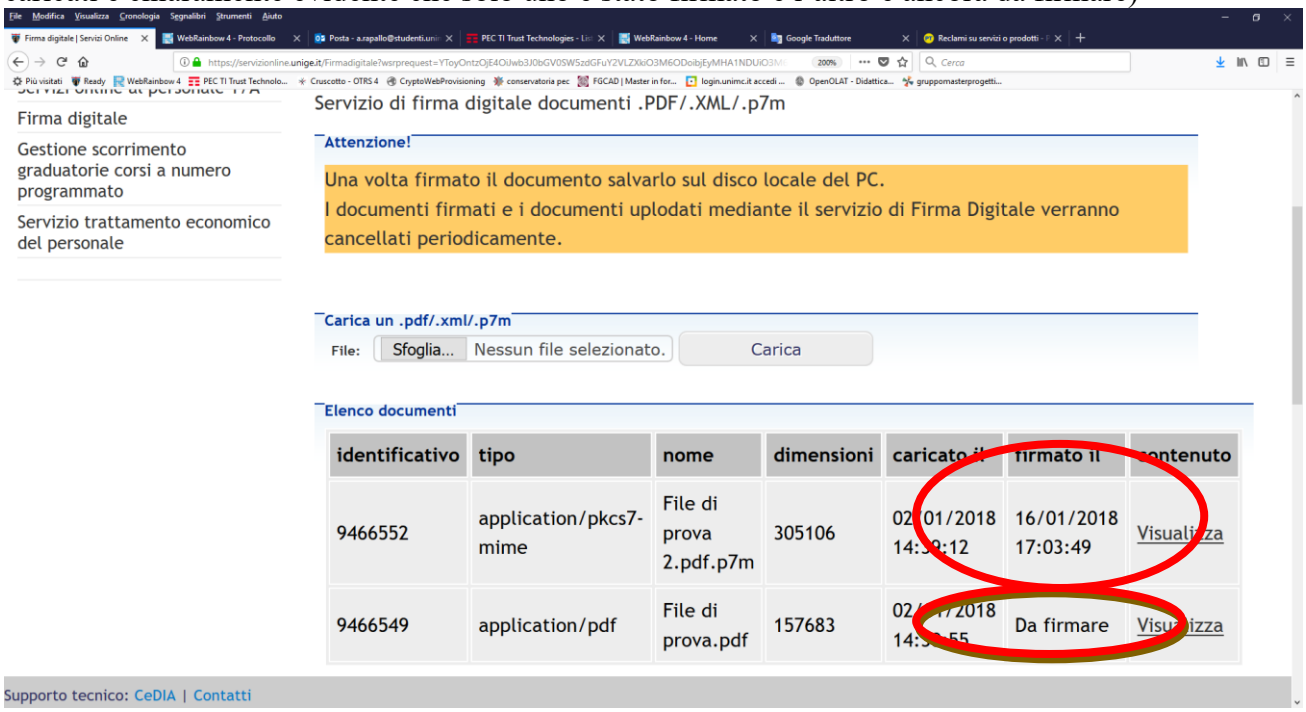
19) alla richiesta della voce registrata, va selezionato il PIN personale di 8 cifre rilasciato in sede di attivazione della firma digitale



20) per completare l'operazione di firma occorre cliccare sul tasto "conferma" e terminare la chiamata dal cellulare



21) a questo punto compare la seguente schermata dalla quale si evince che il documento è stato firmato digitalmente (nell'esempio avendo al punto 15 selezionato un solo file dei due caricati è chiaramente evidente che solo uno è stato firmato e l'altro è ancora da firmare)



22) l'operazione di firma è conclusa ed è necessario salvare il documento firmato digitalmente sul proprio pc per poterlo gestire.

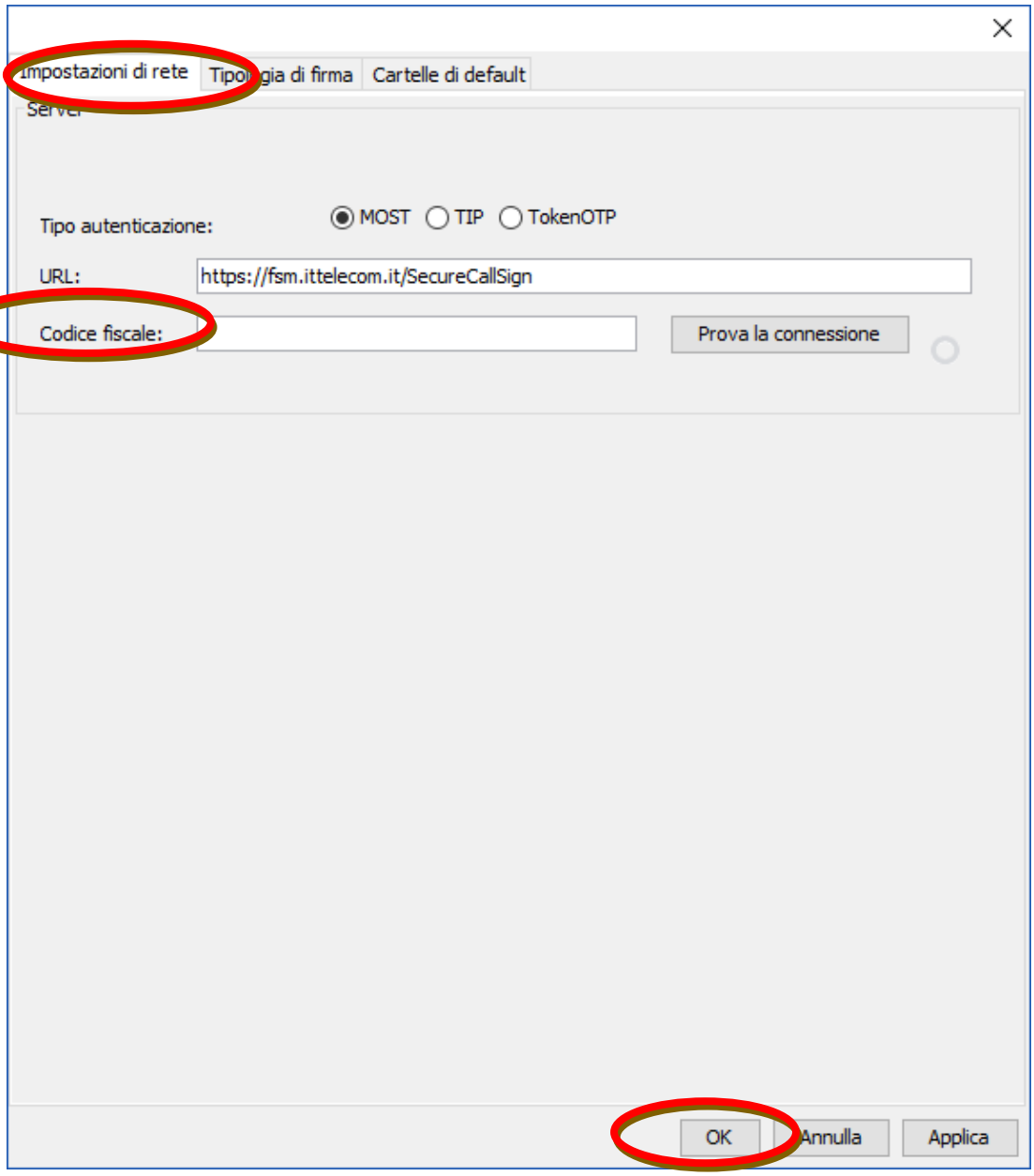
APPOSIZIONE DELLA FIRMA DIGITALE UTILIZZANDO IL CRYPTOCLIENT

1) Scaricare il programma CryptCclient dal sito www.csita.unige.it

2) Aprire il programma

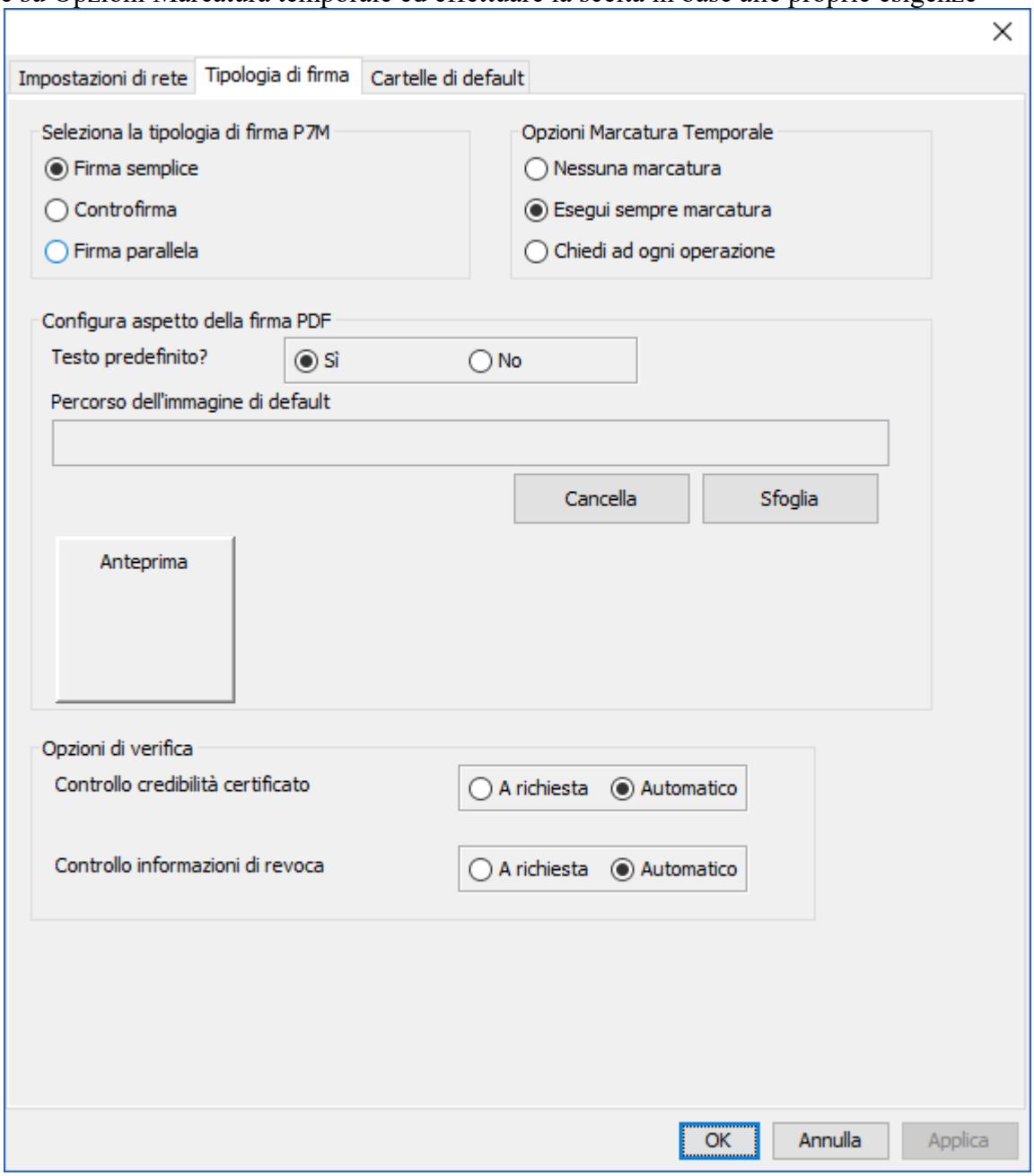
3) La prima volta che si utilizza il programma cliccare sulla seguente icona

Cliccare su impostazioni di rete ed inserire il CF del soggetto che appone la firma e cliccare su OK



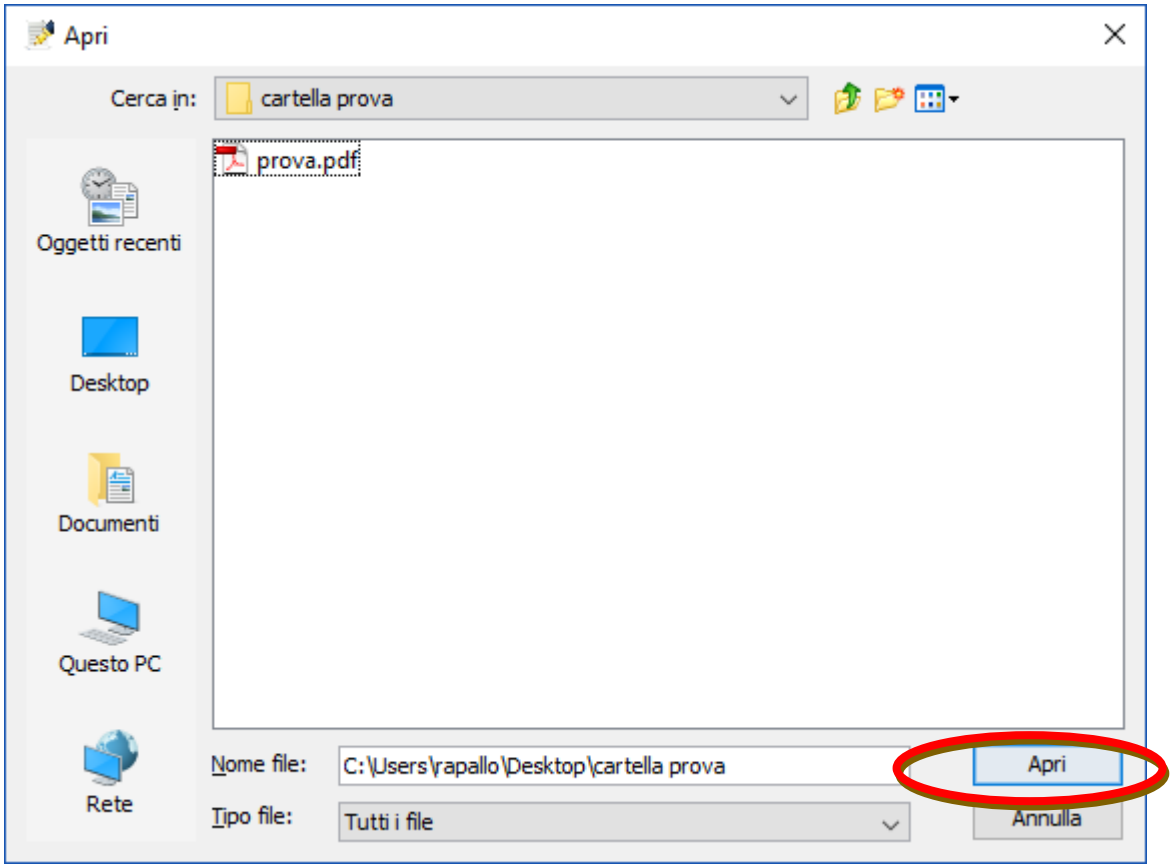
4) Cliccare su “Tipologia di firma” ed operare la scelta tra quelle previste (firma semplice se il documento è firmato da un solo soggetto, controfirma per i documenti firmati da più soggetti tra i quali esiste un rapporto gerarchico, firma parallela per i documenti firmati da più soggetti tra i quali non esiste un rapporto gerarchico)

Cliccare su Opzioni Marcatura temporale ed effettuare la scelta in base alle proprie esigenze

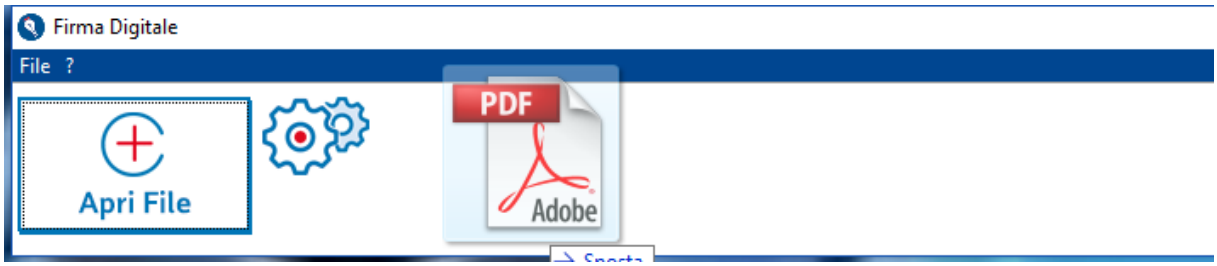


5) Ritornare alla schermata iniziale e cliccare su “Apri file”

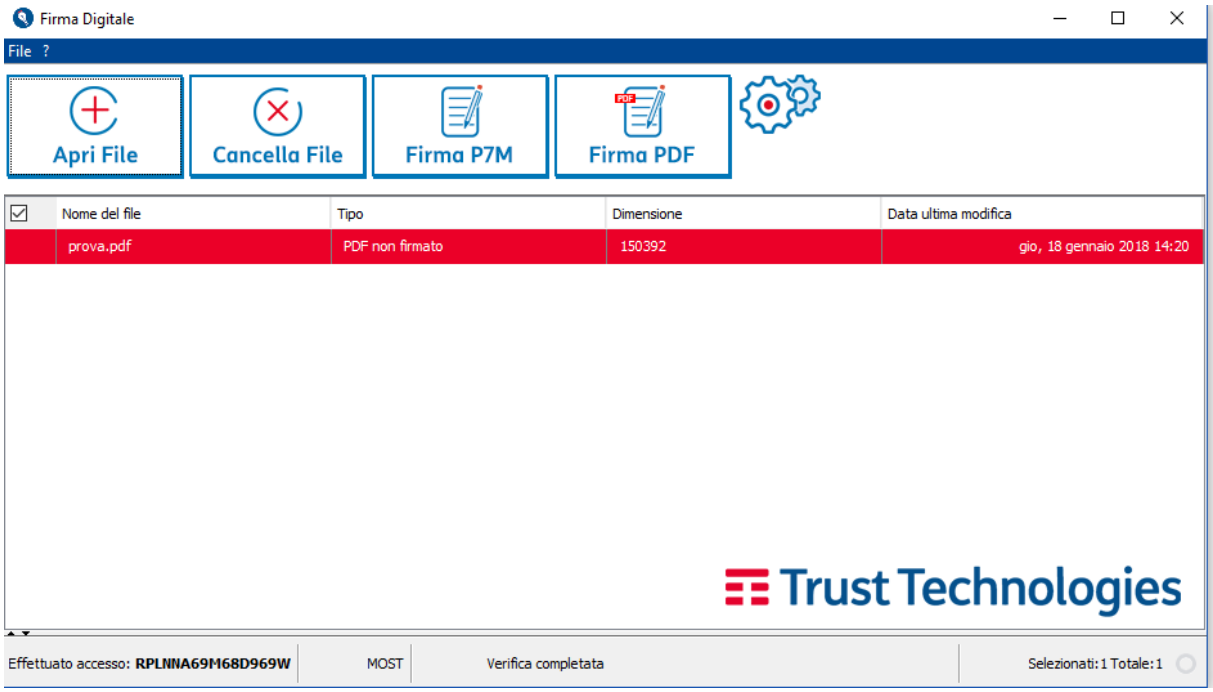
6) selezionare il file che si vuole firmare e cliccare il tasto apri



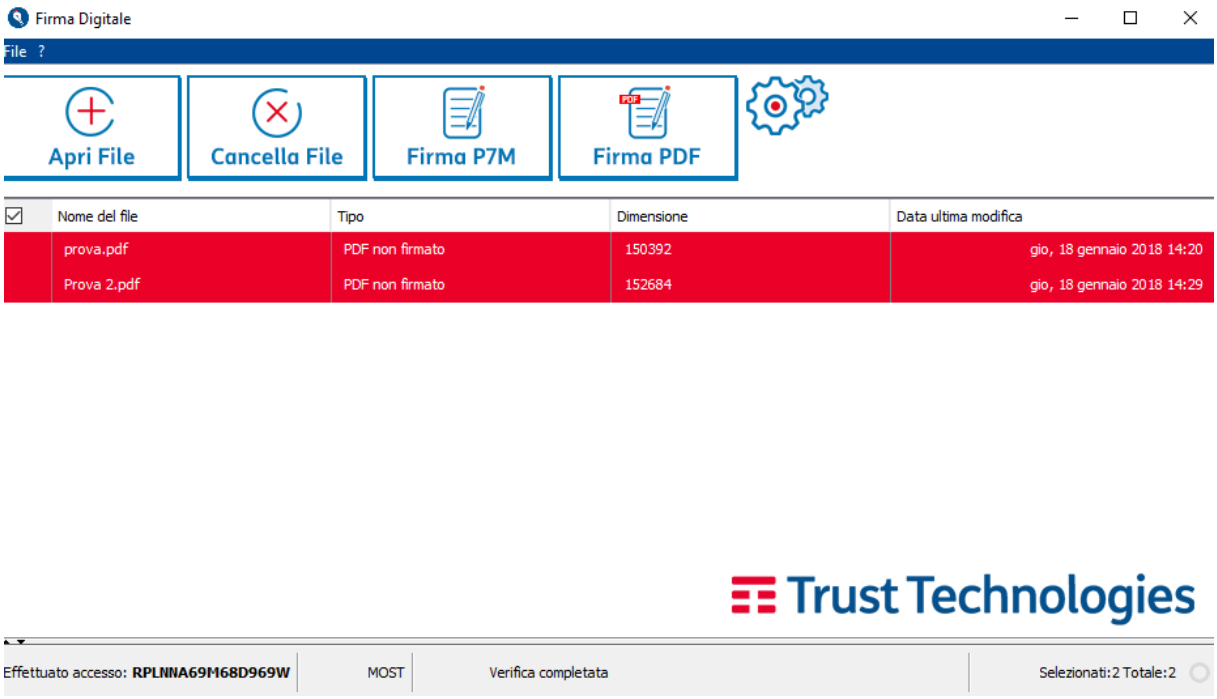
7) in alternativa dal punto 5 è possibile caricare il file anche mediante trascinamento del file nella schermata



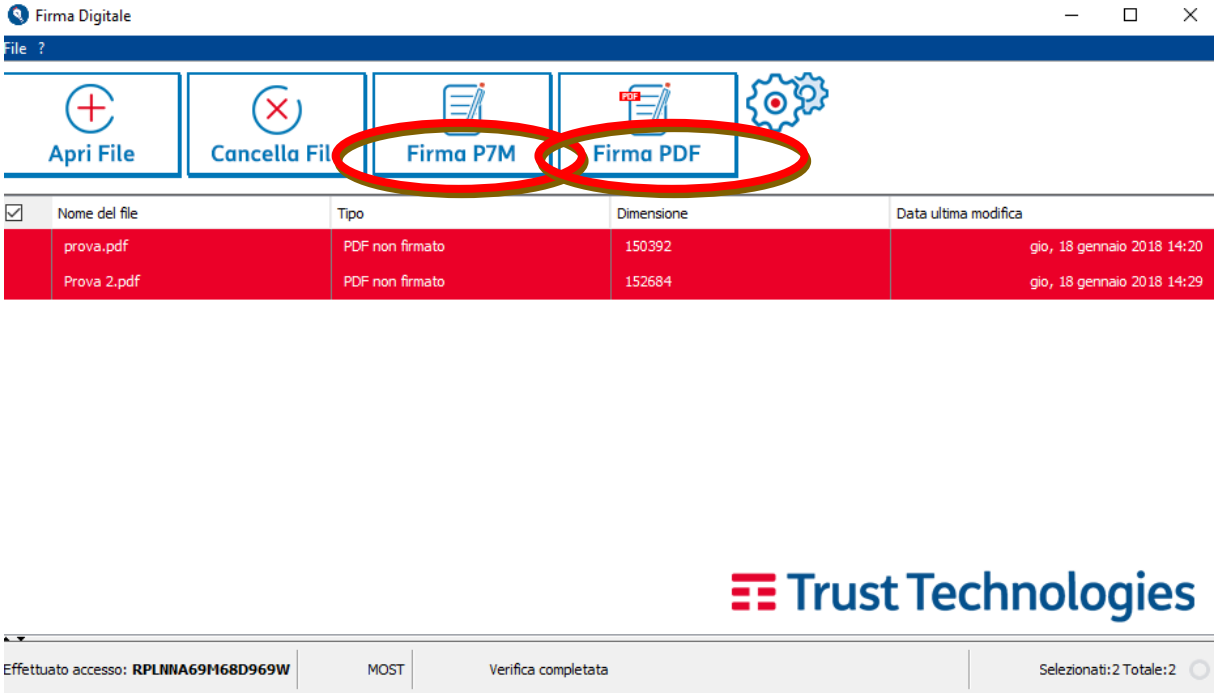
8) il file risulterà caricato



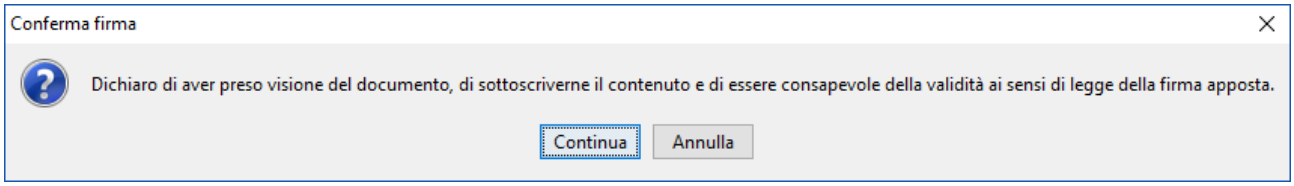
9) è possibile caricare più file, evidenziarli e firmarli con un'unica telefonata



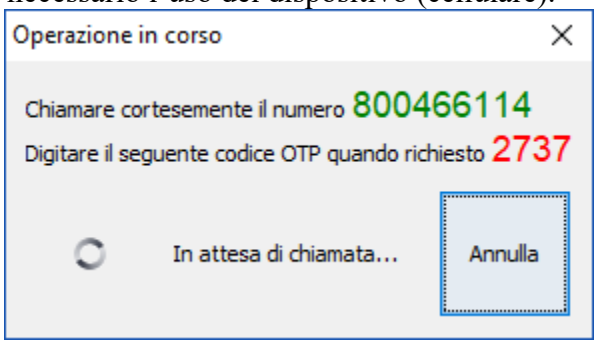
10) a questo punto il firmatario deve scegliere che tipo di firma apporre Cades (.p7m) o Pades (.pdf) e cliccare sul tasto corrispondente



11) A questo punto verrà chiesto al firmatario se vuole visualizzare il documento e la conferma di voler sottoscrivere il contenuto del documento



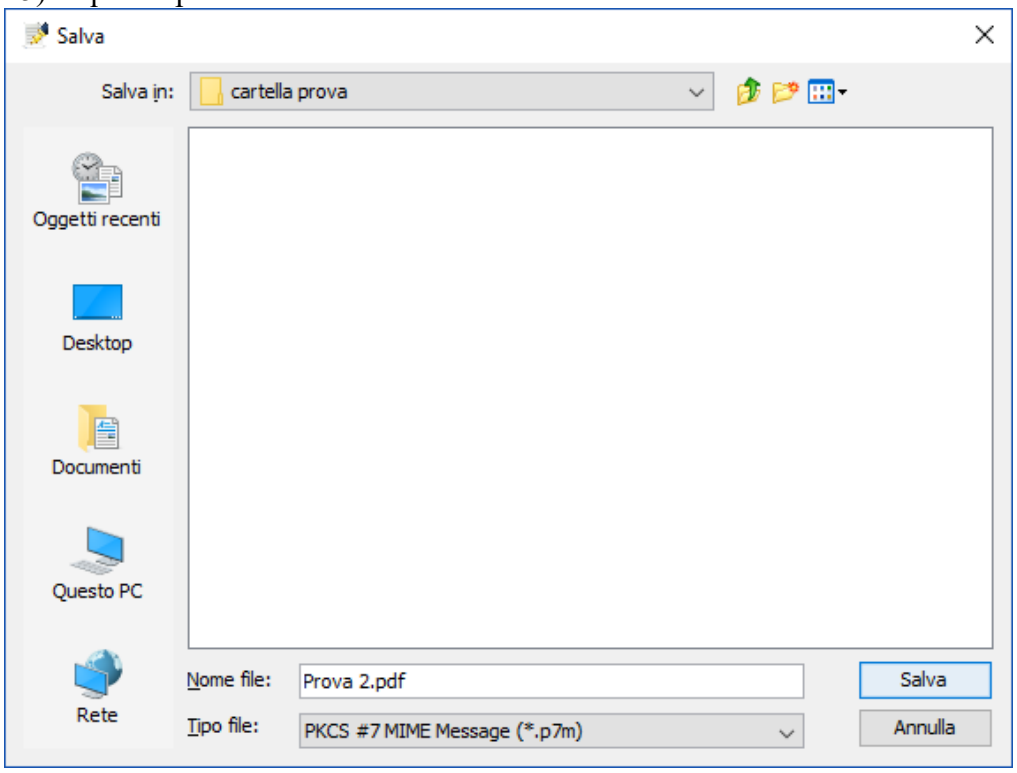
12) Una volta cliccato sul tasto continua inizia l'operazione di firma per lo svolgimento della quale è necessario l'uso del dispositivo (cellulare).



13) occorre chiamare il numero verde visualizzato sul pc e quando la voce registrata chiede di "digitare il codice di quattro cifre che vi è stato indicato" va selezionato, sul cellulare, il codice evidenziato in rosso;

14) alla richiesta della voce registrata, va selezionato il PIN personale di 8 cifre rilasciato in sede di attivazione della firma digitale;

15) a questo punto il documento è stato firmato ed occorre indicare la cartella dove salvarlo



FIRMA DEI VERBALI DI ESAME

Ai sensi dell'art. 48 del Decreto Legge febbraio 2012, n. 5 *"Disposizioni urgenti in materia di semplificazione e di sviluppo"* a decorrere dall'anno accademico 2013-2014, la verbalizzazione e la registrazione degli esiti degli esami, di profitto e di laurea, sostenuti dagli studenti universitari avvengono esclusivamente con modalità informatiche e le Università adeguano conseguentemente i propri regolamenti.

Il sistema di gestione dei verbali digitali d'esame consente ai docenti titolari di insegnamento di verbalizzare gli esami on line inserendo per ciascun studente gli argomenti trattati ed il voto conseguito e di firmare digitalmente il verbale.

Le istruzioni operative da seguire per la presente procedure sono state redatte a cura del Centro Dati, Informatica e Telematica di Ateneo (CeDIA) e pubblicate sul sito all'indirizzo http://www.csita.unige.it/servizionline/docenti/supporto

II. 5 VERIFICHIAMO UN FILE FIRMATO DIGITALMENTE

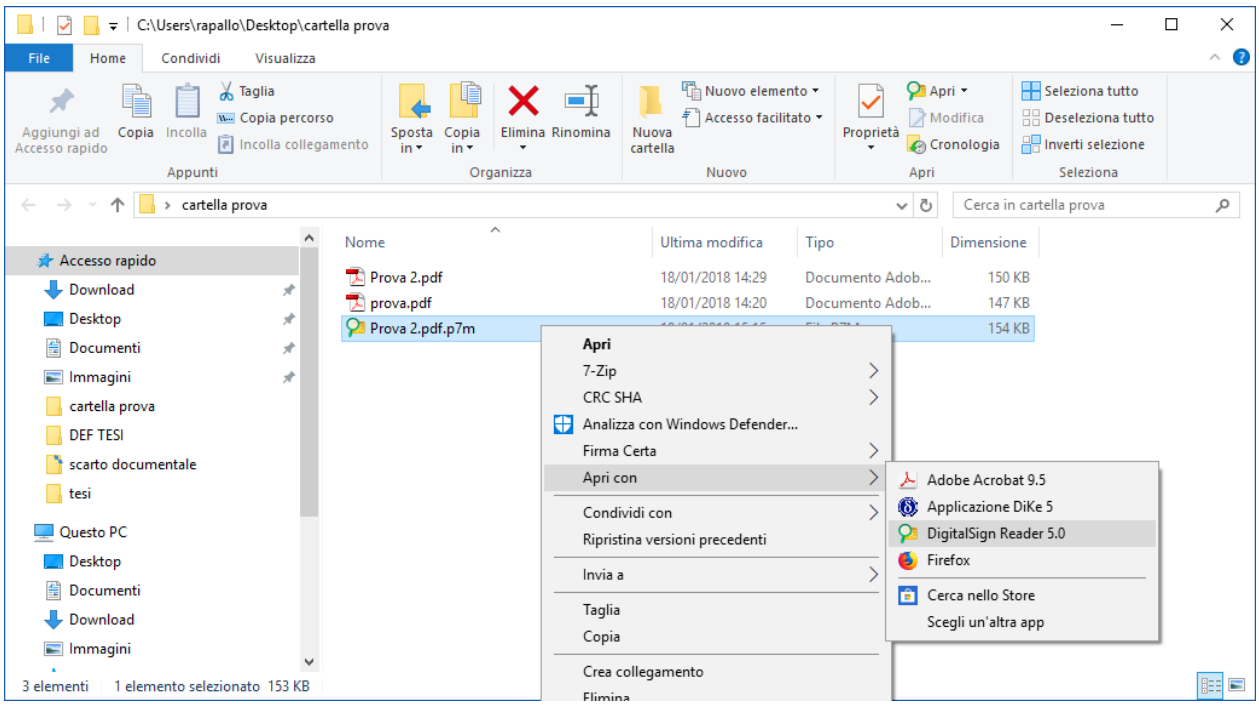
Quando si riceve un file firmato digitalmente occorre procedere alla verifica della firma per accertarsi che il certificato di firma utilizzato sia valido (rilasciato da un prestatore di servizi qualificato, in corso di validità da un pdv temporale, non sospeso né revocato).

Per leggere e procedere alla verifica di un file firmato CAdES occorre dotarsi di un apposito programma; in Ateneo vengono generalmente utilizzati i software Digitalsign Reader e Cryptoclient.

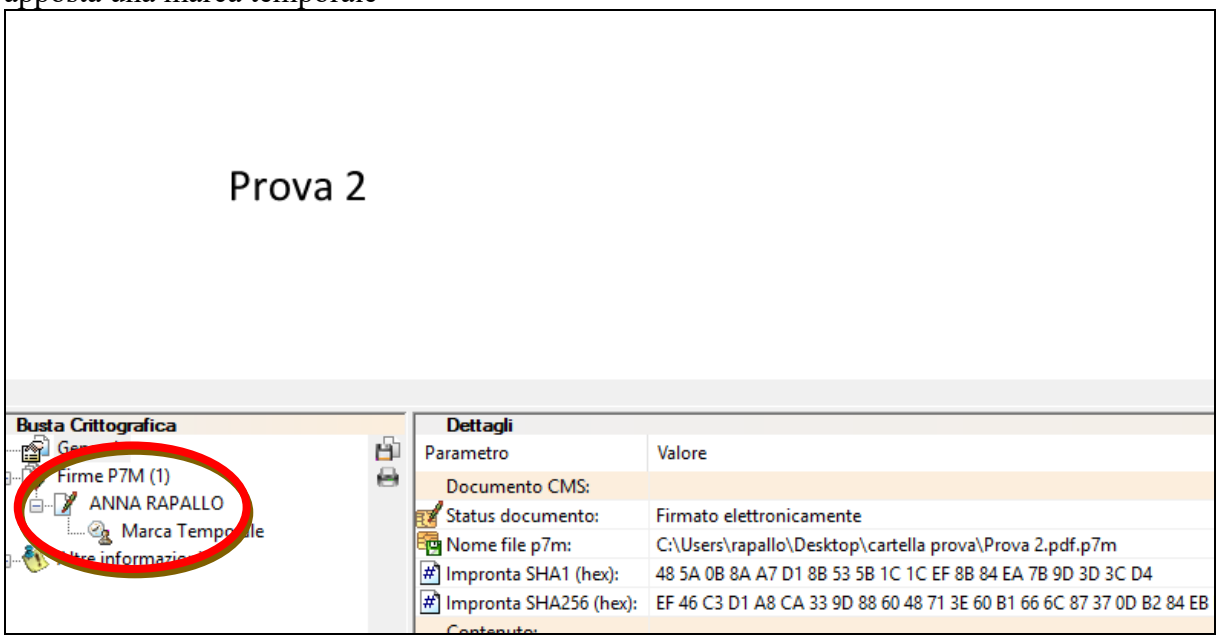
VERIFICA DI FIRMA DIGITALE CON DIGITALSIGN READER

1) Accertarsi di aver installato il software;

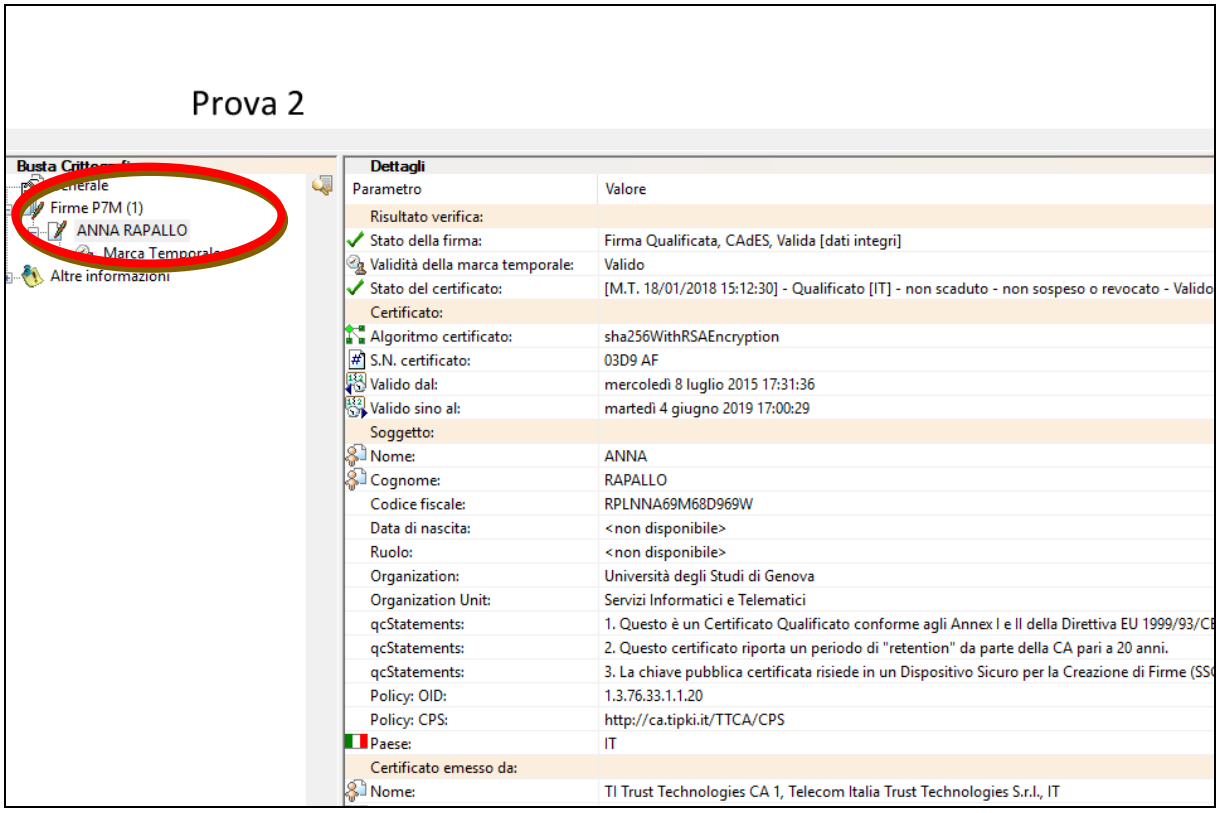
2) Aprire il file che abbiamo ricevuto con il programma DigitalSign installato sul proprio pc



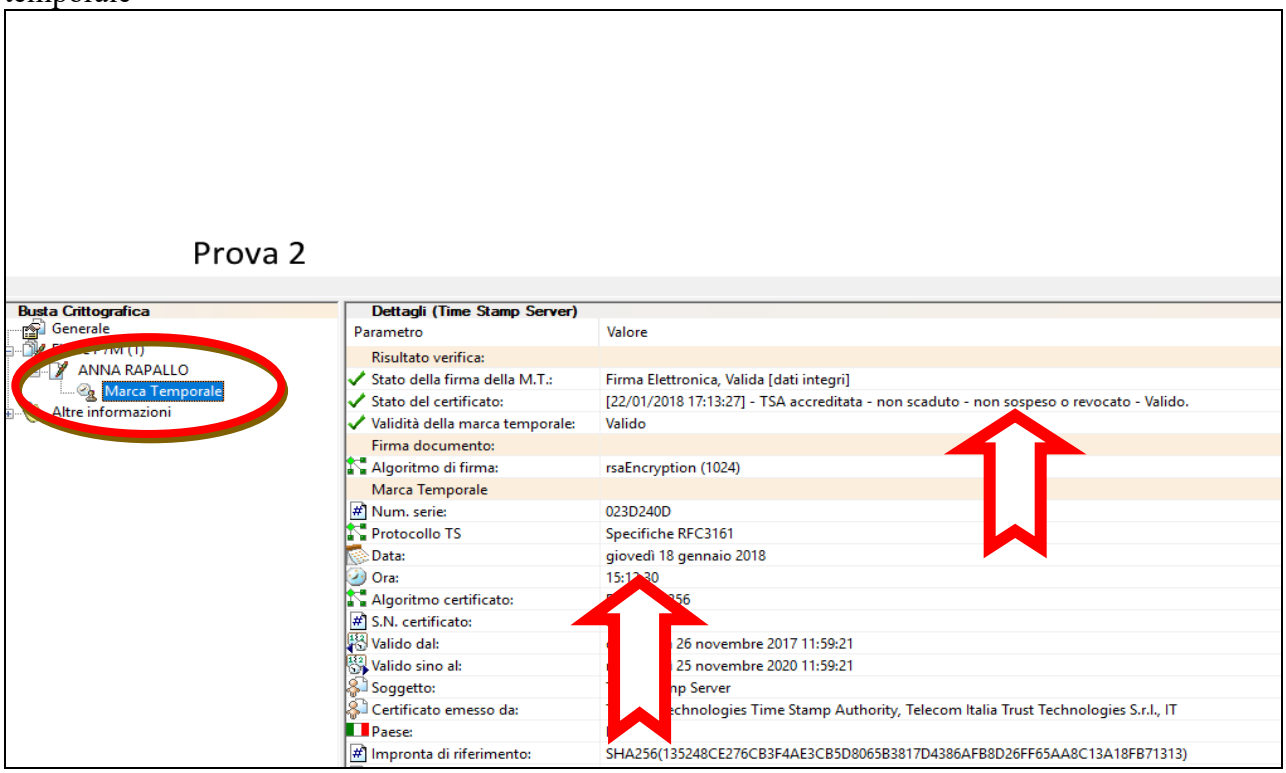
3)Una volta aperto compare questa schermata dove nella parte superiore si può leggere il documento e nella parte sottostante vengono visualizzate le informazioni sul certificato digitale; dalla schermata risulta che il file è firmato digitalmente in formato p7m ed è stata apposta una marca temporale



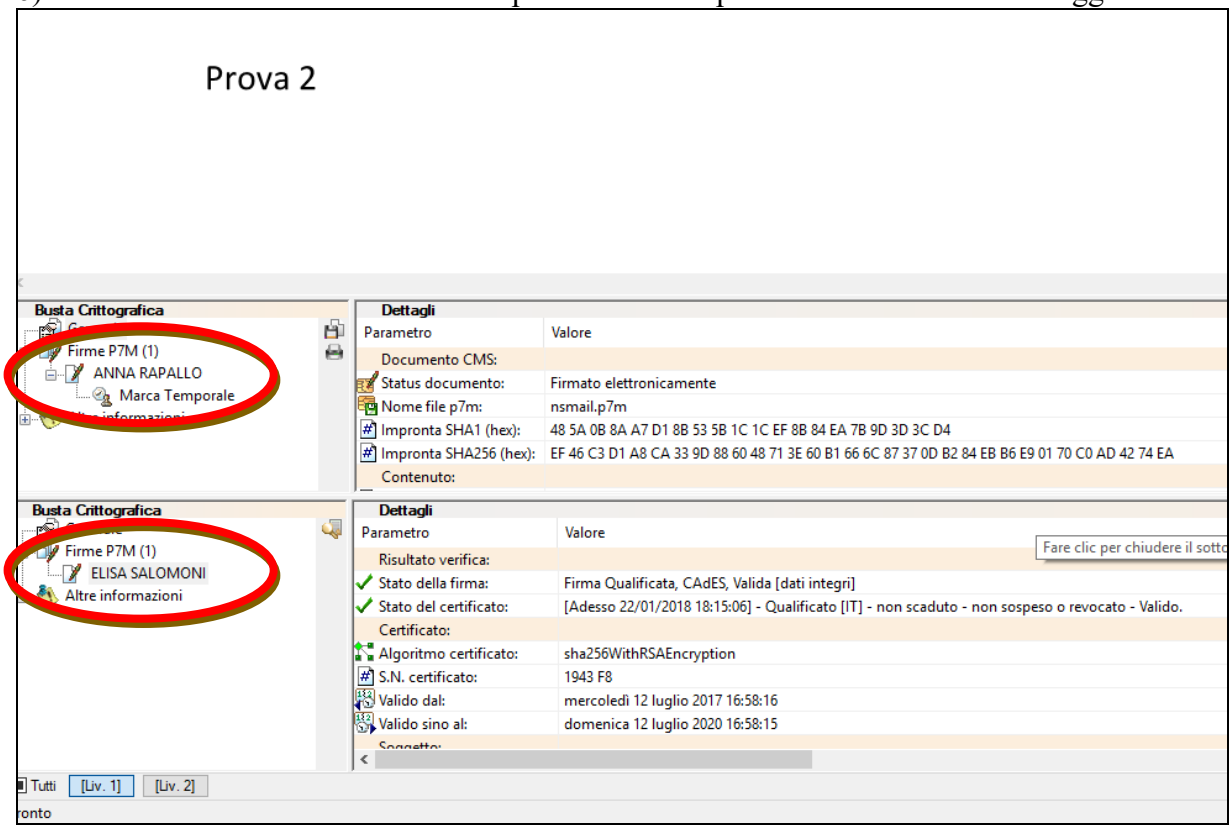
4) Cliccando sul nome del titolare vengono evidenziate le informazioni sul certificato del titolare



5) Cliccando su Marca Temporale vengono evidenziate le informazioni sulla marcatura temporale



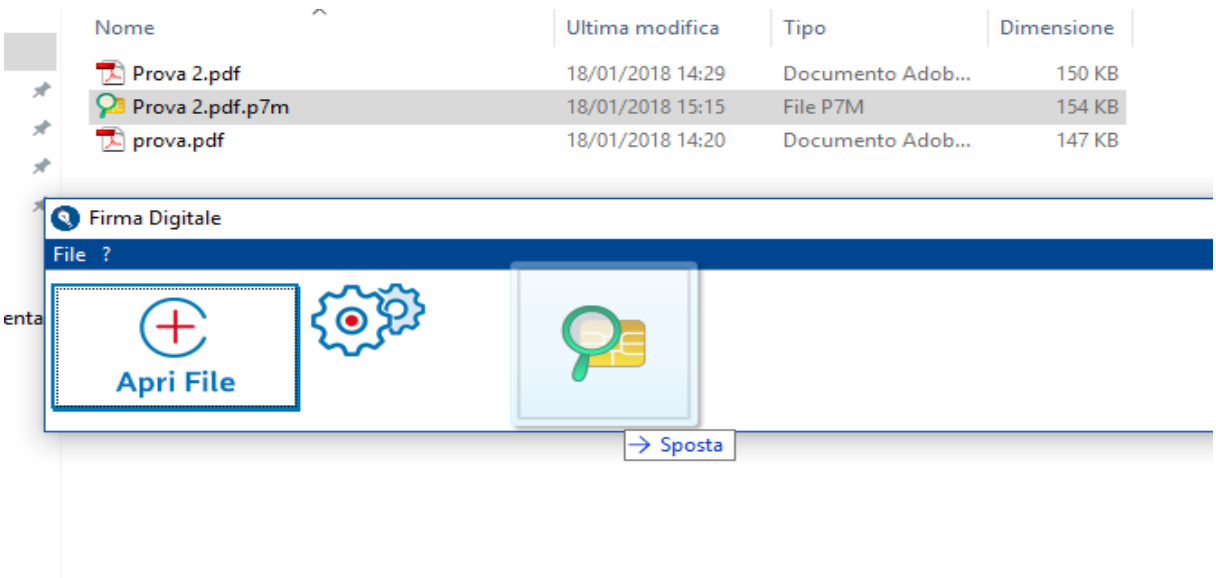
6) Nella schermata sottostante è riportato un esempio di file firmato da due soggetti



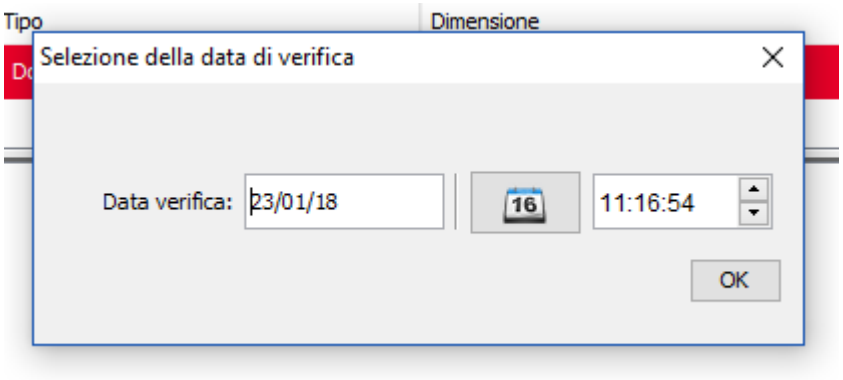
VERIFICA DI FIRMA DIGITALE CON CRYPTOCLIENT

1) Accertarsi di aver installato il software;

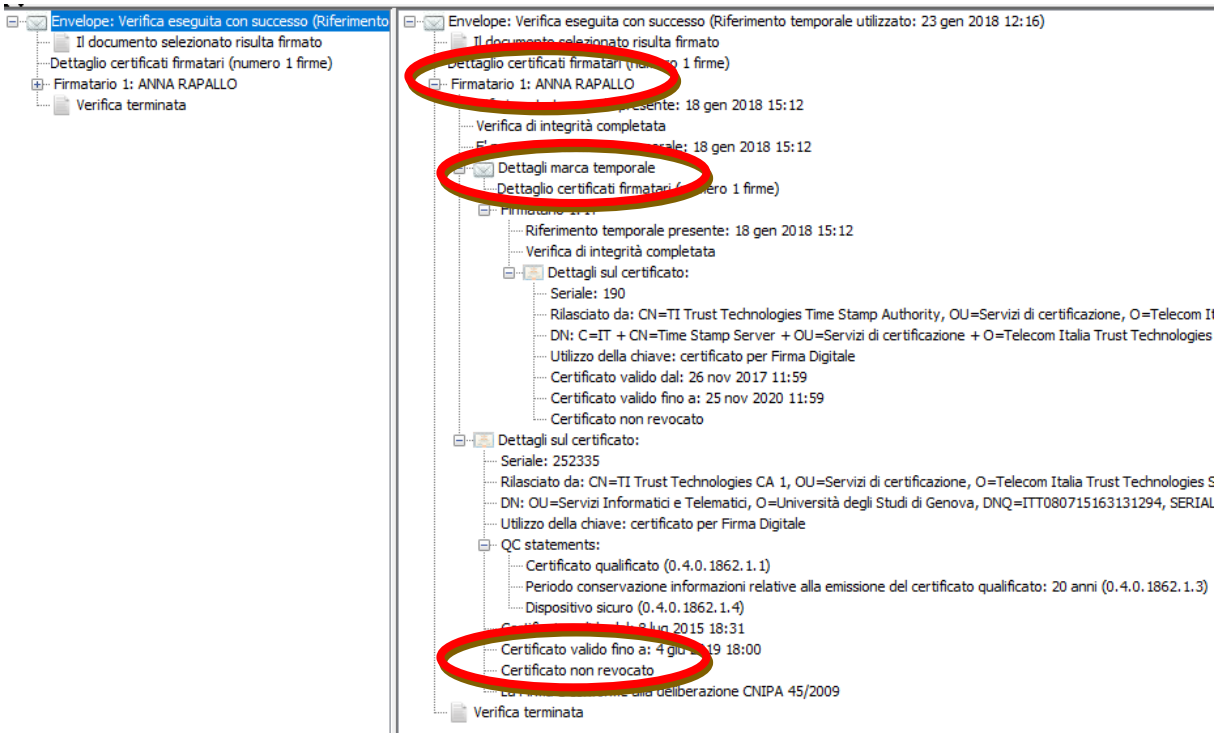
2) Aprire il file che abbiamo ricevuto con il trascinandolo su Cryptoclient



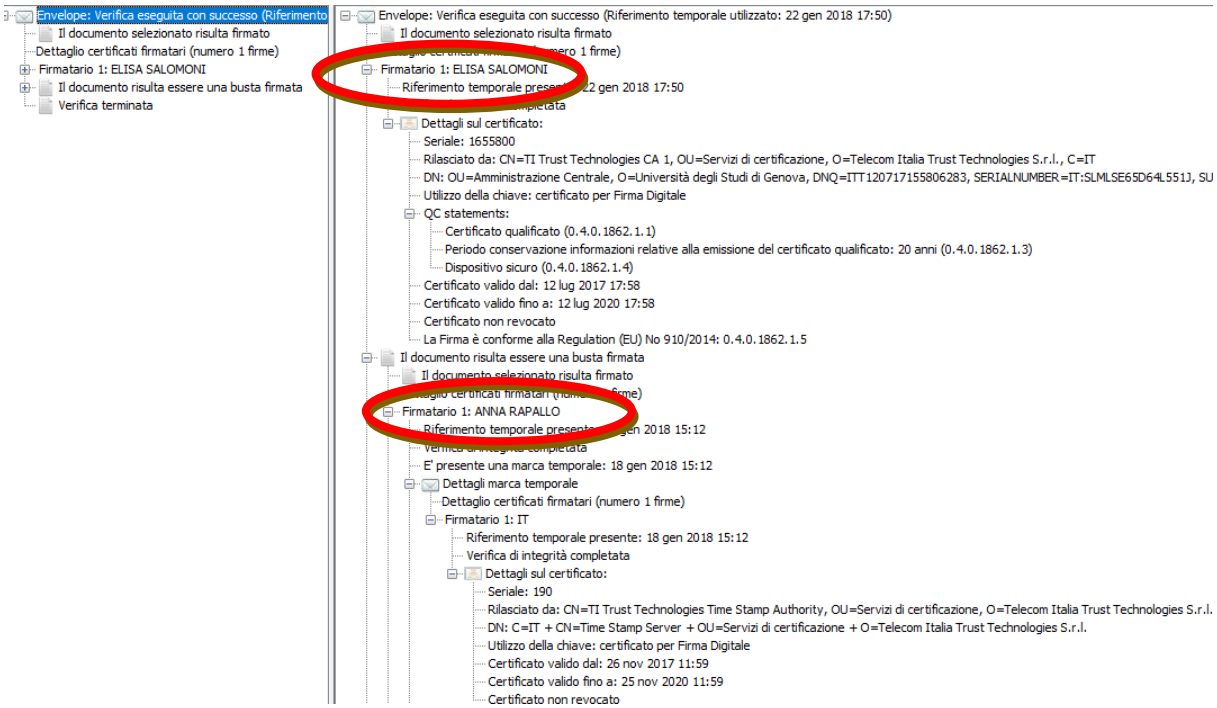
3) Cliccare su ok



4)Questa è la schermata che viene visualizzata con il documento con un firmatario e marca temporale



5) Questa è la schermata che viene visualizzata con il documento con due firmatari



II. 6 SEGNATURA DI PROTOCOLLO DI UN FILE FIRMATO DIGITALMENTE

Ogni messaggio protocollato deve riportare alcune informazioni archivistiche fondamentali, per facilitare il trattamento dei documenti da parte del ricevente. I dati della segnatura di protocollo di un documento informatico sono contenuti in un file XML conforme alle specifiche indicate nella Circolare AgID 60 del 23 gennaio 2013 "*Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni*".

Le informazioni contenute nella segnatura sono memorizzate nel sistema di gestione dei documenti della AOO mittente e in quello delle AOO destinatarie realizzando l'interoperabilità tra sistemi.

Il contenuto minimo obbligatorio della segnatura informatica è composto dalle seguenti informazioni:

a) numero progressivo di protocollo;

b) data di registrazione;

c) indicazione della amministrazione mittente;

d) indicazione della AOO mittente;

e) indicazione del registro nell'ambito del quale è stata effettuata la registrazione.

f) informazioni che descrivono l'organizzazione strutturata e il contenuto del messaggio protocollato.

Di seguito si riporta un esempio di segnatura di protocollo:

segnatura.xml - Blocco note

File Modifica Formato Visualizza ?

```
<?xml version="1.0" encoding="UTF-8"?>

<Segnatura xmlns:tns="http://www.digitPa.gov.it/protocollo/"
targetNamespace="http://www.digitPa.gov.it/protocollo/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="segnature.xsd">
  <Intestazione>
    <Identificatore>
      <CodiceAmministrazione>TEST</CodiceAmministrazione>
      <CodiceAOO>AOO000</CodiceAOO>
      <CodiceRegistro>Registro Unico</CodiceRegistro>
      <NumeroRegistrazione>0003075</NumeroRegistrazione>
      <DataRegistrazione>2018-01-17</DataRegistrazione>
    </Identificatore>
    <Origine>
      <IndirizzoTelematico tipo="smtp">protocollo@pec.unige.it</IndirizzoTelematico>
      <Mittente>
        <Amministrazione>
          <Denominazione>AMMTEST</Denominazione>
          <UnitaOrganizzativa>
            <Denominazione>DIRDA - Settore Gestione documentale e archivi digitali</Denominazione>
            <IndirizzoTelematico>Anna.Rapallo@unige.it</IndirizzoTelematico>
          </UnitaOrganizzativa>
        </Amministrazione>
        <AOO>
          <Denominazione>Area Archivio Protocollo</Denominazione>
        </AOO>
      </Mittente>
    </Origine>
    <Destinazione>
      <IndirizzoTelematico tipo="smtp">mbac-sab-lig@mailcert.beniculturali.it</IndirizzoTelematico>
      <Destinatario>
        <Amministrazione>
          <UnitaOrganizzativa>
            <Denominazione>Soprintendenza Archivistica e Bibliografica per la Liguria</Denominazione>
            <IndirizzoPostale>
              <Toponimo dug="Passo">Santa Caterina Fieschi Adorno</Toponimo>
```

CONCLUSIONI

La reingegnerizzazione dei processi all'interno di una organizzazione, o il semplice cambiamento delle procedure di svolgimento delle attività, generano spesso una serie di difficoltà legate alle cosiddette "*resistenze al cambiamento*". Affinché il progetto possa essere realizzato con successo è necessario fornire a tutti gli attori strumenti idonei ad accompagnarli verso le nuove procedure.

Il presente Manuale ha lo scopo di fornire una descrizione degli usi più comuni della firma digitale nella produzione documentale dell'Ateneo genovese nella speranza di semplificarne l'utilizzo e, conseguentemente, diffonderne l'uso.

Gli archivi digitali presentano notevoli vantaggi rispetto a quelli cartacei (es. tempi minimi di ricerca) ma presentano anche molti più rischi se i documenti non vengono gestiti correttamente; è pertanto necessario essere consapevoli che per garantire la corretta formazione e gestione di un archivio digitale occorre agire correttamente fin dalla fase di produzione del documento, tenendo presente non solo il contenuto del documento, ma anche gli aspetti legati alla forma e di conseguenza adottare tutte quelle misure idonee a garantirne la stabilità, genuinità e fruibilità nel corso del tempo.

BIBLIOGRAFIA

ALLEGREZZA S. I formati elettronici, in PIAGLIAPOCO S. (a cura di) Produzione e *conservazione del documento digitale. Requisiti e standard per i formati elettronici,* Macerata, EUM, 2008

FELICIATI P. *I metadati nel ciclo di vita dell'archivio digitale e l'adozione del modello PREMIS nel contesto applicativo nazionale,* in BONFIGLIO-DOSIO G., PIAGLIAPOCO S. (a cura di) *Formazione, gestione e conservazione degli archivi digitali. Il master FGCAD dell'Università degli Studi di Macerata,* Macerata, EUM, 2015

GUERCIO M. *Formazione e tenuta di memoria digitali: un rapporto cruciale* in GUERCIO M. *Conservare il digitale. Principi, metodi e procedure per la conservazione al lungo termine di documenti digitali*, Roma, Editori Laterza, 2013

PIGLIAPOCO S. *Progetto Archivio Digitale-Metodologia Sistemi Professionalità* CIVITA 2016

SITOGRAFIA

FINOCCHIARO G. Nuovo CAD, che cambia per le firme e il domicilio digitale - https://www.agendadigitale.eu/documenti/nuovo-cad-che-cambia-per-le-firme-e-il-domicilio-digitale/ (consultato a gennaio 2018)

MANCA G. Firma e domicilio digitale cosa cambia nel CAD firmato Piacentini http://cantieripadigitale.it/it/2017/09/12/firma-domicilio-digitale-cosa-cambia-nel-cad-firmato-piacentini/ (consultato a gennaio 2018)

L'apposizione di firme su documenti firmati http://www.agid.gov.it/sites/default/files/linee_guida/firme_multiple.pdf (consultato a gennaio 2018)

Firme elettroniche e firme digitali – http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche (consultato a gennaio 2018)

Segnatura informatica www.agid.gov.it/.../circolari/circolare_60_2013_segnatura_protocollo_informatico (consultato a gennaio 2018)

Onere probatorio in caso di disconoscimento di un atto - http://ilprocessotelematico.it/articoli/news/onere-probatorio-caso-di-disconoscimento-della-firma-digitale-di-un-atto (consultato a gennaio 2018)

ALTRE FONTI

DI MINCO S. Slides originali finalizzate all'attività di formazione nell'ambito del Master FGCAD dell'Università degli Studi di Macerata a.a. 2016/2017