In.Te.S.A. S.p.A.

Qualified Trust Service Provider

Manuale Operativo per le procedure di firma remota qualificata

ai sensi del Regolamento (UE) 910/2014 (eIDAS)

nell'ambito dei servizi di

Ig Markets Limited

Codice documento: *INTQS-MO_IGMKT*
OID: *1.3.76.21.1.50.6*
Redazione: *Antonio Raia*
Approvazione: *Franco Tafini*
Data emissione: *02/05/2018*
Revisione: *02*

Firmato da:
ANTONIO RAIA
Organizzazione: IN.TE.S.A. S.p.A./05262890014

An IBM Company
intesa
DIGITAL
BUSINESS SOLUTIONS

Revisioni

Revisione n°: 01	**Data Revisione:**	**4 marzo 2018**
Descrizione modifiche:	Nessuna	
Motivazioni:	Prima emissione	

Revisione n°: 02	**Data Revisione:**	**2 maggio 2018**
Descrizione modifiche:	Modifiche al paragrafo *F.1.1* relativo all'identificazione utenti	
Motivazioni:	Precisazioni rispetto all'adeguata verifica utilizzata nel contesto IG	

Sommario

Introduzione – Riferimenti Normativi & Acronimi

Riferimenti di legge

Testo Unico - DPR 445/00 e successive modificazioni e integrazioni	Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445. *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*". Nel seguito indicato anche solo come *TU*.
DLGS 196/03 e successive modificazioni e integrazioni	Decreto Legislativo n. 196 del 30 giugno 2003 "*Codice in materia di protezione dei dati personali*". Nel seguito indicato anche solo come *DLGS196/03*
CAD - DLGS 82/05 e successive modificazioni e integrazioni	Decreto Legislativo 7 marzo 2005, n. 82. "*Codice dell'amministrazione Digitale*". Nel seguito indicato anche solo come *CAD*.
DELIBERAZIONE CNIPA n. 45 e successive modificazioni e integrazioni	Deliberazione CNIPA 21 maggio 2009, n. 45. *"Regole per il riconoscimento e la verifica del documento informatico"*. Nel seguito indicato anche solo come *DELIBERAZIONE*
DPCM 22/02/2013 *Nuove Regole Tecniche* e successive modificazioni e integrazioni	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, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 comma 3, 32 comma 3 lettera b), 35 comma 2, 36 comma 2, e 71" (del CAD, ndr).* Nel seguito indicato anche solo come *DPCM*
DPCM 19/07/2012 e successive modificazioni e integrazioni	Decreto del Presidente del Consiglio dei Ministri 19 luglio 2012 "*Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma*".
Regolamento (UE) N. 910/2014 (eIDAS) e successive modificazioni e integrazioni	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *eIDAS*

Definizioni & Acronimi

Termine o acronimo	***Significato***
AgID	Agenzia per l'Italia Digitale (già CNIPA e DigitPA): www.agid.gov.it**.** Nel seguito anche solo *Agenzia*.
Certificato Qualificato	Attestato elettronico, che contiene un insieme di informazioni che creano una stretta e affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. È rilasciato da un Certificatore Accreditato
TSP	Trust service provider – Prestatore di servizi fiduciari (già *Certificatore*) Persona fisica o giuridica che presta uno o più servizi fiduciari.
Certificatore Accreditato	TSP presente nell'elenco pubblico dei Certificatori Accreditati tenuto da AgID. (nelle more del Regolamento (UE) N. 910/2014).
CP	Certificate Policy - Un insieme di norme, contraddistinto da un codice, che indica l'applicabilità di un certificato ad una particolare comunità e/o a una classe di applicazioni aventi comuni esigenze di sicurezza.
CPS	Certification Practice Statement - Una dichiarazione delle prassi seguite da un Certificatore / TSP nell'emettere e gestire certificati.
CRL	Certificate Revocation List - Un elenco firmato che riporta un insieme di certificati non più considerati validi dal Certificatore / TSP che li ha emessi.

Termine o acronimo	*Significato*
Doc. Informatico	Documento Informatico: documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Doc. Analogico	Documento analogico: rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
FEA	Firma elettronica Avanzata – ex Art.26 Reg. UE 910/2014 (eIDAS), la FEA soddisfa i segg. requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare 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 di tali dati.
Firma Digitale	Particolare tipo di firma 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
Firma remota	Particolare procedura di firma qualificata o di firma digitale che consente di garantire il controllo esclusivo del dispositivo di firma;
Firma automatica	Particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo
HSM	Hardware Security Module - Insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche
OID	Object Identifier - Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
PKI	Public Key Infrastructure - Insieme di hardware, software, persone, norme e procedure necessarie per creare, gestire, conservare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.
CA	Certification Authority: Entità della PKI che rilascia i certificati
RA Registration Authority	Autorità di Registrazione che su incarico del TSP esegue le registrazioni e le verifiche delle identità dei titolari dei certificati qualificati necessarie al TSP. In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è del TSP (INTESA S.p.A.).
Validazione temporale	Informazione elettronica contenente la data e l'ora che viene associata ad un documento informatico, al fine di provare che quest'ultimo esisteva in quel momento
Terzo Interessato	Il terzo interessato è il terzo dal quale derivino i poteri del Titolare medesimo.
Titolare	Persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica. Soggetto intestatario del certificato.
TSA	Time Stamping Authority - Autorità che rilascia marche temporali.

A. Il Manuale Operativo

A.1. Proprietà intellettuale

Questo documento è il *Manuale Operativo per le procedure di firma remota qualificata nell'ambito dei servizi di IG Markets Limited, Codice Fiscale 06233800967, n. di iscrizione al Registro delle Imprese di Milano MI – 1878663, Sede Legale Via Paolo da Cannobio 33, 20122 Milano, Italia* (di seguito anche solo *IG*).

Il Manuale Operativo descrive le procedure e relative regole utilizzate dal *Prestatore di Servizi Fiduciari Qualificato In.Te.S.A. S.p.A.* (di seguito anche solo *QTSP* o *INTESA*) per l'emissione dei Certificati Qualificati, la generazione e la verifica della firma elettronica qualificata nell'ambito dei servizi offerti da IG.

Il contenuto di questo Manuale Operativo è conforme a quanto stabilito dalle regole tecniche contenute nel Decreto del Presidente del Consiglio dei Ministri del 22 Febbraio 2013 (di seguito anche solo *DPCM*) e dal Decreto Legislativo 7 marzo 2005, n. 82, recante il "Codice dell'Amministrazione Digitale" come successivamente modificato e integrato (di seguito anche solo *CAD*) e in particolare:

- il capo II, Sez. II che disciplina le firme elettroniche e i certificatori,
- il capo VII, che prevede le modalità con le quali vengono dettate le regole tecniche previste dal Codice.

Le attività descritte sono svolte in conformità con il Regolamento (UE) 910/2014 (eIDAS).

Per quanto non espressamente previsto nel presente Manuale Operativo si fa riferimento alle norme tempo per tempo vigenti.

In questo contesto, i Titolari di un Certificato Qualificato sono solo i soggetti riconosciuti dalla Registration Authority ovvero dalla stessa IG, la quale, in virtù di specifico accordo con il Certificatore, è autorizzata a svolgere la funzione di Registration Authority.

Il processo prevede che il Titolare possa avviare la procedura di Firma Remota di documenti nell'ambito dei servizi offerti da IG.

A.2. Validità

Quanto descritto in questo documento si applica al Certificatore, cioè alle sue infrastrutture logistiche e tecniche e al suo personale, ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma elettronica qualificata relativa ad essi, anche avvalendosi delle marche temporali emesse da INTESA.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'Art.5 del DPCM, al comma 4. Ai fini del presente decreto, le chiavi di creazione e verifica della firma e i correlati servizi, si distinguono secondo le seguenti tipologie:

a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati qualificati, alle informazioni sullo stato di validità del certificato ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e delle relative regole utilizzate dal certificatore accreditato INTESA per l'emissione di certificati qualificati.

Tale impianto di regole e procedure scaturisce dall'ottemperanza alle attuali normative in merito la cui osservanza permette ad INTESA di essere inserita nell'elenco dei certificatori accreditati.

Pertanto, in funzione delle normative menzionate, vengono coinvolte più entità che saranno meglio identificate nel prosieguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n.02 del Manuale Operativo del Certificatore Accreditato In.Te.S.A. S.p.A. per le procedure di firma remota nell'ambito dei servizi offerti da *IG Markets*, rilasciato il 02/05/2018, in conformità con l'Art.40 del DPCM.

L'object identifier (OID) di questo documento è **1.3.76.21.1.50.6**.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica anche presso l'indirizzo Internet:

http://e-trustcom.intesa.it/DOCS/mo_ig.pdf

La pubblicazione di versioni aggiornate del presente Manuale Operativo potrà avvenire sul sito sopra indicato solo successivamente al loro inoltro all'Agenzia per l'Italia Digitale.

Lo stesso manuale operativo viene pubblicato e aggiornato in simultanea anche sul sito di IG.

B.2. Dati identificativi del Certificatore

Il Certificatore, ai sensi dell'Art.29 del CAD, è la società INTESA S.p.A., di cui di seguito sono riportati i dati identificativi.

Denominazione sociale	**In.Te.S.A. S.p.A.**
Indirizzo della sede legale	**Strada Pianezza, 289** **10151 Torino**
Legale Rappresentante	**Amministratore Delegato**
Registro delle Imprese di Torino	**N. Iscrizione 1692/87**
N. di Partita I.V.A.	**05262890014**
N. di telefono (centralino)	**+39.011.19216.111**
Sito Internet	**www.intesa.it**
N. di fax	**+39.011.19216.375**
Indirizzo di posta elettronica	**marketing@intesa.it**
Indirizzo (URL) registro dei certificati	**ldap://x500.e-trustcom.intesa.it**
ISO Object Identifier (OID)	**1.3.76.21.1**

B.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo, ai sensi dell'Art.40 comma 3 lett. c) del DPCM, è del QTSP INTESA, che ne cura la stesura, la pubblicazione, l'aggiornamento e ogni eventuale revisione, in accordo e in collaborazione con IG.

Allo scopo di raccogliere eventuali osservazioni e richieste di chiarimenti, INTESA ha predisposto i seguenti strumenti:

un recapito di posta elettronica:	***e-trustcom@intesa.it***
un recapito telefonico:	+39 011.192.16.111
un recapito fax:	+39 011.192.16 375
un servizio di HelpDesk	per le chiamate dall'Italia 800.80.50.93 per le chiamate dall'estero +39 02.871.193.396

B.4. Entità coinvolte nei processi

All'interno della struttura del Certificatore vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati.

Tali attori operano in ottemperanza alle regole e ai processi posti in opera dal Certificatore espletando, per la parte di loro competenza, le attività a loro attribuite.

Il personale responsabile delle attività di certificazione, in conformità con l'Art.38 del DPCM, è articolato nelle figure seguenti:

a) Responsabile della sicurezza.
b) Responsabile del servizio di certificazione e validazione temporale.
c) Responsabile della conduzione tecnica dei sistemi.
d) Responsabile dei servizi tecnici e logistici.
e) Responsabile delle verifiche e delle ispezioni (auditing).

Le figure sopra elencate sono tutte appartenenti all'organizzazione del Certificatore INTESA.

B.4.1. Certification Authority (Certificatore Accreditato)

INTESA, operando in ottemperanza con quanto previsto dal DPCM e dal CAD, espleta le attività di Certificatore Accreditato. Tali attività prevedono l'emissione, la pubblicazione, la revoca e la sospensione di Certificati Qualificati per la firma digitale remota.

I dati identificativi del Certificatore Accreditato INTESA sono riportati nel paragrafo precedente.

B.4.2. Registration Authority (Ufficio RA)

Per la particolare tipologia di servizio offerto (Firma Remota nell'ambito delle applicazioni di firma descritte in questo Manuale Operativo), il Certificatore ha rilasciato mandato a svolgere le funzioni di Local Registration Authority (LRA) a IG. In particolare, la LRA potrà svolgere le seguenti attività:

- Identificazione del Titolare.

- Registrazione del Titolare.

IG, nello svolgimento della sua funzione di Registration Authority, deve vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente.

C. Obblighi

C.1. Obblighi del Certificatore Accreditato

Nello svolgimento della propria attività, il Certificatore Accreditato opera in conformità con quanto disposto dal:

- Decreto Legislativo del 7 marzo 2005, n.82 e successive modifiche.
- Decreto Presidente del Consiglio dei Ministri 22 Febbraio 2013.
- Decreto Legislativo 30 giugno 2003, n.196, e successive modificazioni, recante codice in materia di protezione dei dati personali.
- Regolamento (UE) 910/2014 (eIDAS)

In particolare il Certificatore Accreditato:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo sicuro per la generazione delle firme (HSM) abbia le caratteristiche e i requisiti di sicurezza previsti dall'Art.35 del CAD e all'Art.11 del DPCM;
- rilascia e rende pubblico il certificato qualificato, se non diversamente specificato dal Titolare, secondo quanto stabilito all'Art.32 del CAD;
- informa i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali (DLgs 196 30/06/2003);
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del Terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra queste citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il Certificatore;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.

Secondo quanto stabilito dall'Art.14 del DPCM, il Certificatore fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Inoltre, il Certificatore:

- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate dall'Agenzia per l'Italia Digitale per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati (Art.42 del DPCM);
- garantisce l'interoperabilità del prodotto di verifica, di cui all'Art.14 del DPCM, ai documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica amministrazione e successive modifiche tecniche e organizzative;
- mantiene copia della lista, sottoscritta dall'Agenzia per l'Italia Digitale, dei certificati relativi alle chiavi di certificazione (di cui all'Art.43 del DPCM), e la rende accessibile per via telematica (Art.42, comma 3 del DPCM).

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato digitale per i servizi descritti nel presente Manuale Operativo potrà ricevere un certificato qualificato di firma per sottoscrivere atti e documenti nell'ambito dei servizi di firma remota offerti da IG.

Il Titolare è tenuto a conservare le informazioni necessarie all'utilizzo della chiave privata di firma in modo adeguato e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (CAD, Art.32, comma 1).

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal Certificatore, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- mettere a disposizione del Certificatore, tramite IG, eventuali variazioni alle informazioni fornite all'atto della registrazione, avvenute durante il periodo di validità del certificato digitale: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- revocare immediatamente il certificato digitale in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma;
- revocare o sospendere il certificato digitale secondo quanto indicato nel presente Manuale Operativo.

C.3. Obblighi degli utilizzatori dei certificati

Coloro che intendano verificare la validità di un documento firmato digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato allo standard ISO 9594-8;
- verificare l'assenza del certificato dalle Liste di Revoca (CRL) dei certificati e la loro validità;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei certificatori;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo del Certificatore che ha emesso il certificato di colui che ha sottoscritto il documento informatico.

Gli obblighi sopra descritti sono automaticamente espletati dai Software di Verifica conformi alle normative vigenti (Art. 14 del DPCM) ed implementati nei servizi offerti dal Certificatore sul portale di IG.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato provvederà all'inoltro delle richieste di revoca o sospensione nei casi e nelle modalità previste dal presente Manuale Operativo.

C.5. Obblighi della Registration Authority esterna

Il Certificatore, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale di ulteriori soggetti (nel seguito anche denominati *LRA – Local Registration Authority*) per svolgere una parte delle attività proprie dell'Ufficio di registrazione. In particolare, la LRA deve espletare le seguenti funzioni:

- identificazione certa del Titolare del certificato;
- registrazione del Titolare;
- consegna al Titolare dei codici che gli permettano di accedere alla propria chiave di firma nel rispetto degli Artt. 8 e 10, comma 2, del DPCM.

Il Certificatore ha rilasciato mandato a svolgere la funzione di Registration Authority (RA) a IG (LRA) mediante la stipula di un Contratto di Mandato sottoscritto da entrambe le parti.

In tale contratto sono esplicitati gli obblighi cui si deve attenere la Local RA cui INTESA assegna l'incarico di RA; in particolare si richiede di:

- vigilare affinché l'attività di riconoscimento posta in essere si svolga nel rispetto della normativa vigente (CAD e successive modificazioni);
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il DLgs. 196/03.
- rendere disponibile per il Certificatore il materiale raccolto nella fase di identificazione e l'autorizzazione all'uso dei dati personali.

La documentazione relativa alle attività di cui sopra e necessaria all'emissione del Certificato Qualificato viene conservata secondo gli obblighi di legge, per 20 (venti) anni.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del Certificatore – Limitazione agli indennizzi

Conformemente a quanto previsto dal CAD, dal DPCM e dal D.Lgs. 196/03, INTESA è responsabile, verso i Titolari per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal DPCM, dal DLgs 196/03 e dal CAD e successive modificazioni e integrazioni (vedi *C.1 - Obblighi del Certificatore Accreditato*).

INTESA, fatto salvo i casi di negligenza, dolo o colpa grave, non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dall'Art.5 del DPCM, e in particolare dal mancato rispetto da parte del Titolare e dal Terzo Interessato di quanto indicato nel presente Manuale Operativo e/o dalla mancata osservanza da parte degli stessi della normativa vigente.

Parimenti, INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo esemplificativo: calamità naturali, disservizi e/o disfunzioni tecniche e logistiche al di fuori del proprio controllo, interventi dell'Autorità, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività INTESA si avvale per la prestazione dei propri servizi di certificazione.

Il Certificatore non sarà responsabile per i danni derivanti da un utilizzo non conforme del Certificato Qualificato per la Firma digitale Remota in relazione alla limitazione d'uso come specificata al paragrafo *F.1.2*.

D.2. Assicurazione

INTESA è beneficiaria di contratti assicurativi per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.
Di tale contratto è inviata ad AgID apposita dichiarazione di stipula.

E. Tariffe

Per la particolarità del servizio oggetto di questo Manuale Operativo il Certificatore non indica delle tariffe per l'emissione, il primo rinnovo, la revoca e la sospensione dei certificati.

Queste verranno eventualmente indicate nei contratti che verranno stipulati fra IG e il Titolare.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

Il Certificatore deve verificare con certezza l'identità del richiedente alla prima richiesta di emissione di certificato qualificato.

Questa operazione viene demandata alla Local Registration Authority (IG), ed è svolta in ottemperanza con quanto previsto dalla vigente normativa e secondo le modalità descritte nel seguito.

Fra i dati di registrazione necessari all'avviamento del servizio ricordiamo:

- Nome e Cognome;
- Data di nascita;
- Comune o stato estero di nascita;
- Codice fiscale;
- Indirizzo di residenza;
- Domicilio presso il quale saranno inviate le comunicazioni cartacee;
- Numero di telefono cellulare;
- Indirizzo di posta elettronica;
- Tipo e numero del documento d'identità esibito;
- Autorità che ha rilasciato il documento, data e luogo del rilascio, data di scadenza.

Pertanto, la LRA, in ottemperanza con quanto previsto dalla vigente normativa e dalle normative interne, svolge tutte le operazioni necessarie all'identificazione e registrazione del richiedente.

La documentazione relativa alla registrazione dei Titolari viene conservata dalla LRA che ha effettuato l'identificazione per 20 (venti) anni.

F.1.1. Identificazione tramite riconoscimento precedente

Il Certificatore si avvale del riconoscimento già effettuato da un Intermediario finanziario o da altro Soggetto Esercente Attività Finanziaria, che, ai sensi delle norme Antiriciclaggio tempo per tempo vigenti, è obbligato al riconoscimento dei propri clienti.

Questa operazione viene, pertanto, demandata alla Local Registration Authority in ottemperanza con quanto previsto dall'adempimenti degli obblighi di adeguata verifica.

Per verificare l'identità del Richiedente, durante il processo di adesione IG, agendo da LRA, ne acquisisce i dati anagrafici e copia di un documento d'identità. oltre che dei dati bancari che potranno essere funzionali a tale obiettivo.

Il personale IG verifica quindi la validità dei documenti forniti e la loro corrispondenza con i dati anagrafici indicati.

I dati identificativi del Titolare raccolti all'atto della registrazione sono quindi utilizzati per l'emissione del certificato "one-shot" a lui intestato, previa sua conferma dei dati anagrafici e accettazione delle condizioni contrattuali per il rilascio del certificato e delle modalità operative per l'apposizione della firma digitale.

Il servizio non ha cannone, ma tutto il costo di gestione è compreso nelle commissioni che il cliente paga per negoziare i prodotti finanziari

F.1.2. Limitazioni d'uso

Nel Certificato Qualificato per la Firma Digitale, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti da IG, è inserito il seguente limite d'uso:

"*Il presente certificato è valido solo per firme apposte con procedura automatica per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti da IG.*"

"*This certificate may only be used for unattended/automatic digital signature for the signature of documents and/or contracts concerning products and/or services offered by IG.*".

G. Modalità operative per la sottoscrizione di documenti

Il Certificatore, attraverso i servizi di IG, rende disponibile ai Titolari quanto necessario a generare delle firme elettroniche qualificate conformemente a quanto previsto dalla normativa vigente.

La particolare tipologia del servizio non richiede la fornitura di un'applicazione di firma da installare sul proprio personal computer, ma piuttosto delle funzionalità di firma richiamabili via internet o accedendo ai servizi offerti da IG.

Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno conformi a quanto previsto dal DPCM all'Art.3 comma 2 relativamente agli algoritmi utilizzati.

Inoltre tali documenti, come richiesto dall'Art.3 comma 3 del DPCM; non conterranno macro istruzioni o codici eseguibili tali ad attivare funzionalità che possano, all'insaputa del sottoscrittore, modificare atti, fatti e dati nei documenti stessi rappresentati.

G.1. Firma con certificato One-Shot

Il Certificatore offre un servizio Firma Digitale, generata su HSM e conforme alla normativa vigente, mediante l'utilizzo di un certificato "one-shot", cioè una particolare tipologia di certificato per la quale è prevista una validità temporale limitata all'apposizione della prima firma.

Per richiedere l'emissione di tale tipologia di certificato e la successiva firma elettronica qualificata, il Titolare:

- Si connette al portale messo a disposizione da IG;
- Prende visione, oltre che del presente documento, di un'informativa contenente una descrizione del processo che verrà messo in atto per l'emissione del certificato e la firma del documento;
- Si autentica tramite la verifica di un codice OTP ricevuto sul numero di cellulare precedentemente indicato;
- Visualizza il documento in modalità digitale;
- Richiede l'emissione del certificato "one-shot" e la firma del documento;

L'emissione e la firma potranno avvenire solo dopo che siano state espletate le procedure di adeguata verifica che garantiscono l'identificazione certa (cfr. *F.1*).

Una volta identificato il Titolare, conformemente a quanto specificato dall'informativa di processo visionata dal Titolare, la CA provvede a:

- Generare il certificato qualificato one-shot su di un HSM custodito e gestito sotto la responsabilità del Certificatore accreditato.
- Firmare il documento in modalità automatica, utilizzando il certificato "one-shot" appena emesso;
- Conformemente alla normativa, viene inserita anche la marca temporale generata dal servizio di validazione temporale del Certificatore descritto alla sezione *H.2*;
- Al termine della firma, le chiavi di sottoscrizione sono cancellate dall'HSM, rendendo così inutilizzabile il certificato per ulteriori sottoscrizioni.

G.2. Modalità operative per la verifica della firma

I documenti che verranno sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF; tale formato di sottoscrizione (previsto dall'Art.21, comma 8 e 15 della Deliberazione) è considerato infatti di facile utilizzo nell'ambito delle applicazioni di firma remota.

Infatti, la verifica dei documenti sottoscritti potrà essere agevolmente effettuata utilizzando il software *Acrobat Reader DC* scaricabile gratuitamente dal sito *www.adobe.com*.

H. Generazione delle chiavi di Certificazione, di Validazione Temporale e di sottoscrizione

H.1. Generazione delle chiavi di certificazione

La generazione delle chiavi di Certificazione all'interno dei dispositivi di firma custoditi nei locali del TSP avviene in presenza del *Responsabile dei servizi di certificazione*, come previsto dal DPCM (Art.7, comma 1) ed è preceduta dall'inizializzazione dei dispositivi di firma.

Il tutto avviene inoltre alla presenza di un numero di responsabili aziendali ritenuto adeguato e sufficiente ad evitare operazioni illecite.

Una volta generate le coppie di chiavi, quelle private vengono suddivise in più parti, ciascuna delle quali viene trascritta su più dispositivi di backup (token USB), secondo una logica *m di n*: gli n dispositivi sono suddivisi e consegnati alle n figure aziendali presenti, le quali vi associeranno una propria password.

I dispositivi sono conservati in modo sicuro, così come sono conservate in modo sicuro le relative password.

La lunghezza delle chiavi del sistema di certificazione è di 2048 bit.

H.2. Generazione delle chiavi del sistema di validazione temporale

La generazione delle chiavi di validazione temporale avviene secondo quanto stabilito dall'Art.49 del DPCM.

La lunghezza delle chiavi del sistema di validazione temporale è di 2048 bit.

H.3. Generazione delle chiavi di sottoscrizione

Completata la fase di registrazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del Certificatore, è possibile procedere alla generazione delle chiavi di sottoscrizione.

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato autenticandosi al sistema fornitogli da IG.

Le coppie di chiavi di sottoscrizione (la cui lunghezza è di almeno 2048 bit) vengono create su dispositivi sicuri, Hardware Security Module, conformi a quanto previsto dalla normativa vigente.

Una volta completata il processo di apposizione della firma sul documento da sottoscrivere, le chiavi del Titolare sono eliminate dal dispositivo HSM.

I. Modalità di emissione dei certificati

I.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo H.1, vengono generati i certificati delle chiavi pubbliche conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

I certificati delle chiavi di certificazione sono inviati all'Agenzia (AgID) attraverso il sistema di comunicazione di cui all'Art.16, comma 1, del DPCM.

Il Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori e lo pubblica nel proprio registro dei certificati. Il Certificatore deve poi mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, Art.42, commi 1 e 3).

I.2. Procedura di emissione dei Certificati di sottoscrizione

INTESA emette certificati con un sistema conforme con l'Art.33 del DPCM.

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel paragrafo H.3, è possibile generare una richiesta di nuovo certificato nel formato PKCS#10, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

Generate le chiavi, la richiesta di certificato sarà immediatamente inviata dall'applicazione di IG al Certificatore.

La generazione dei certificati è registrata nel giornale di controllo (DPCM, Art.18, comma 4).

I.3. Informazioni contenute nei certificati

I certificati INTESA sono conformi a quanto indicato nella deliberazione CNIPA n.45 del 21/05/09 e successive modificazioni e integrazioni.

Il Certificato Qualificato definisce con certezza il Certificatore che lo ha emesso e contiene i dati necessari per la verifica della Firma Digitale.

Ogni Certificato Qualificato per la Firma Digitale contiene, a titolo esemplificativo, ma non esaustivo, le seguenti informazioni:

- numero di serie;
- ragione o denominazione sociale del Certificatore;
- codice identificativo unico del Titolare presso il Certificatore;
- nome, cognome, codice fiscale del Titolare;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- tipologia delle chiavi;
- limitazioni nell'uso della coppia di chiavi.

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale conterranno sempre una limitazione d'uso (cfr. F.1.2).

J. Modalità di revoca e sospensione dei certificati

J.1. Revoca dei certificati

La revoca dei certificati viene asseverata dal loro inserimento nella lista CRL (Art.22 DPCM).

Il profilo delle CRL è conforme con lo standard RFC 3280.

La CRL, firmata dal Certificatore, viene aggiornata con periodicità prestabilita e ad ogni revoca o sospensione. La lista è disponibile anche sul registro dei certificati.

Ai sensi della Determinazione Commissariale 119/2016, le informazioni di revoca e sospensione sono anche disponibili attraverso il protocollo OCSP.

J.1.1. Revoca dei certificati di sottoscrizione

Data la natura del servizio, la revoca del certificato non si rende necessaria, in quanto le chiavi di sottoscrizione sono cancellate dal dispositivo di firma dopo l'utilizzo.

In ogni modo, il Titolare può richiedere la revoca del proprio Certificato, utilizzando i canali di comunicazione definiti con IG o contattando il Certificatore.

Il Certificatore provvederà all'immediata revoca del certificato e Titolare sarà avvisato dell'avvenuta revoca.

J.1.2. Revoca dei certificati relativi a chiavi di certificazione

Il Certificatore procede con la revoca dei certificati di certificazione e dei certificati di sottoscrizione firmati con la stessa chiave di certificazione nei casi di:

1. compromissione della chiave di certificazione,

2. guasto del dispositivo di firma (HSM) delle chiavi di Certificazione, nel caso sia compromessa la sicurezza delle chiavi ivi contenute,
3. cessazione dell'attività.

Entro 24 ore, il Certificatore notificherà la revoca all'Agenzia per l'Italia Digitale e ai Titolari.

J.2. Sospensione dei certificati

Il servizio oggetto di questo manuale non prevede la sospensione del certificato del Titolare, in quanto il certificato emesso all'atto della firma ha validità temporale limitata e le chiavi sono cancellate subito dopo la sottoscrizione.

K. Modalità di sostituzione delle chiavi

K.1. Sostituzione dei certificati qualificati e delle chiavi del Titolare

Per i servizi oggetto di questo manuale, i certificati digitali emessi dal Certificatore hanno una validità limitata legata all'utilizzo del certificato stesso e non ne è prevista la sostituzione alla scadenza. Le chiavi del Titolare sono cancellate dal dispositivo di firma immediatamente dopo la sottoscrizione.

K.2. Sostituzione delle chiavi del Certificatore

K.2.1. Sostituzione pianificata delle chiavi di certificazione

Con un periodo di tempo congruo alla normativa vigente, prima della scadenza del certificato relativo alle coppie di Chiavi di certificazione, utilizzate dal sistema di emissione dei certificati di sottoscrizione e dei certificati di TSU, in presenza del Responsabile del servizio di certificazione e di responsabili aziendali in numero sufficiente a garantire la sicurezza dell'operazione, si procederà alla generazione di nuove chiavi di certificazione.

L'attività è pianificata in modo da garantire la continuità dei servizi, compatibilmente al fatto che Il termine del periodo di validità di un certificato qualificato deve precedere di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità (DPCM, art.18, comma 3).

Quanto fatto sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza del certificato.

K.2.2. Sostituzione in emergenza delle chiavi del sistema di generazione dei certificati

Il procedimento utilizzato in caso di guasto del dispositivo di firma (HSM) o di disastro presso la sede centrale è trattato alla sezione *O*.

K.2.3. Sostituzione pianificata delle chiavi del sistema di validazione temporale

In conformità con quanto indicato all'Art.49, comma 2, del DPCM, ai fini di limitare il numero di marche temporali generate con la medesima coppia di chiavi di marcatura temporale, queste sono sostituite entro 90 (novanta) giorni dalla data della loro emissione. Contestualmente, un certificato è emesso relativamente alla nuova coppia di chiavi, senza revocare il precedente, relativo alla coppia di chiavi sostituita. L'operazione è svolta in presenza del *Responsabile del Servizio*.

K.2.4. Sostituzione in emergenza delle chiavi del sistema di validazione temporale

Il procedimento utilizzato in caso di guasto del dispositivo di firma (HSM) o di disastro presso la sede centrale è descritto alla sezione O.

L. Registro dei certificati

L.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

1. I certificati delle chiavi di sottoscrizione e del sistema di validazione temporale.
2. I certificati delle chiavi di certificazione.
3. I certificati emessi a seguito della sostituzione delle chiavi di certificazione.
4. Certificati per le chiavi di firma dell'Agenzia per l'Italia Digitale (DPCM Art.42, comma 1).
5. Le liste di revoca e sospensione.

Le operazioni che coinvolgono il registro dei certificati vengono svolte soltanto dalle persone a ciò autorizzate, presenti in quantità adeguata a impedire azioni illecite da parte di un limitato numero di addetti.

Il Certificatore mantiene una copia di riferimento del registro dei certificati inaccessibile dall'esterno: questa aggiorna in tempo reale la copia operativa, accessibile da parte degli utenti con protocollo LDAP.

La verifica di rispondenza tra copia di riferimento e copia operativa è fatta sistematicamente.

L.2. Accesso logico al Registro dei certificati

La copia di riferimento è collocata all'interno di una rete dedicata protetta da adeguati dispositivi, per cui non è accessibile ad altri che dal server di emissione dei certificati, che vi registra i certificati emessi e le CRL/CSL.

L'accesso è possibile all'indirizzo ***ldap://x500.e-trustcom.intesa.it***.

Il Certificatore consente l'accesso a CRL/CSL via Internet attraverso il protocollo http.

Ai sensi della Determinazione Commissariale 119/2016 e del Regolamento eIDAS, le informazioni di revoca e sospensione sono anche disponibili attraverso il protocollo OCSP.

L.3. Accesso fisico ai locali dei sistemi preposti al registro dei certificati

Gli addetti abilitati alla gestione diretta del registro dei certificati possono accedere al locale ove il sistema è installato e operarvi solo se in modalità dual control ad evitare azioni illecite.

Gli addetti alla gestione dei sistemi, alla gestione della rete, alla manutenzione, ecc., possono accedere al locale ove il sistema è installato e, per gli addetti specifici, operarvi solo in presenza di addetti abilitati alla gestione del registro dei certificati secondo le modalità precedentemente esplicitate per gli operatori abilitati.

M. Modalità di protezione della riservatezza

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure previste dal DLgs 196/03 e successive modificazioni e integrazioni.

N. Procedura di gestione della copie di sicurezza

Gli archivi informatici che sono oggetto di copie di sicurezza sono i seguenti:

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato alla sezione L.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato e le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del Certificatore (Art.36 del DPCM).

- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.53, comma 1, del DPCM).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (Art.52 del DPCM).

La conservazione, per tutte le copie di sicurezza descritte, è conforme a quanto previsto dalle normative vigenti in materia.

O. Procedura di gestione degli eventi catastrofici

Il Responsabile della sicurezza gestisce un piano di gestione degli eventi catastrofici che prevede le seguenti fasi:

- gestione dell'emergenza: in questa fase è garantita la continuità di accesso alle CRL/CSL; la loro emissione può subire ritardi derivanti dalla necessità di attivare il server di back up della CA, situato nel sito di back up;
- gestione del transitorio: in questo periodo è assicurata l'emissione dei certificati e il ripristino di ulteriori soluzioni di disaster recovery;
- ritorno dell'esercizio a regime: nel medesimo sito originale o in un altro alternativo, ma definitivo.

Va premesso che la presenza di repliche della copia operativa del registro dei certificati distribuite in più punti consente comunque, in caso di interruzione di funzionamento della sede principale, di accedere al contenuto del registro dei certificati aggiornato fino al momento dell'interruzione.

Per poter fare fronte alla gestione dell'emergenza è prevista la replica nel sito di backup del registro dei certificati, dei dati del sistema di emissione dei certificati e l'intervento entro 24 ore di personale atto ad attivare la funzionalità di emissione delle CRL/CSL. Di detto personale è curato l'addestramento, oltre che alla gestione del SW e HW, anche della situazione di emergenza. È previsto inoltre l'intervento, entro il medesimo lasso di tempo, dei depositari delle componenti della chiave privata della CA ai fini di ricostruirla nel dispositivo di firma (HSM) del sito di backup.

In tutte le località interessate dalla gestione degli eventi catastrofici è depositata copia cartacea del piano di emergenza.

P. Modalità per l'apposizione e la definizione del riferimento temporale

Tutte le macchine del sistema di PKI del Certificatore sono sincronizzate con l'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata da un software specifico installato su ogni server che, mediante il protocollo NTP (Network Time Protocol), si collega al server remoto configurato.

Il Network Time Protocol (NTP) permette di mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico a piramide.

L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi sono sincronizzati, attraverso un generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

Il software installato presso il Certificatore si collega al server remoto ad intervalli regolari di tempo e, dopo aver ottenuto l'ora corrente, provvede a correggere il clock della macchina locale mediante sofisticati algoritmi.

I riferimenti temporali apposti dalle applicazioni sono stringhe in formato data (DD/MM/YYYY hh:mm:ss), con la precisione del secondo, che rappresentano l'ora locale, in base alla configurazione della macchina. Tali riferimenti sono conformi al DPCM, Art.51.

Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (Art.41 del DPCM).

P.1. Modalità di richiesta e verifica marche temporali

Il Certificatore appone una marca temporale su tutti i documenti sottoscritti dal Titolare nell'ambito dei servizi descritti da questo Manuale Operativo. L'apposizione di detta marca è un processo integrato con l'operazione di firma e non richiede nessuna attività specifica da parte del Titolare.

Q. Riferimenti tecnici

RFC 5905	Network Time Protocol (Version 4) Specification, Implementation
ETSI TS 102 023	Deliverable ETSI TS 102 023 "Policy requirements for time-stamping authorities" – Aprile 2002
RFC 5280	RFC 3280 (2008): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 5816	RFC 5816 (2010): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"
ISO/IEC 9594-8 2001:(E)	Information Technology – Open Systems Interconnection – The Directory: Authentication 01/08/2001 Framework; ITU-T Recommendation X.509 (2001) | ISO/IEC 9594-8
RFC 2527	RFC 3647 (2003): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
RFC 3039	RFC 3739 (2004) Internet X.509 Public Key Infrastructure Qualified Certificates Profile
ETSI TS 102 778-1..5	ETSI TS 102 778-1..5) V1.1.1 "Electronic Signatures and Infrastructure (ESI); PDF Advanced Electronic Signature Profiles;" Electronic Signatures and Infrastructures (ESI); PDF Advanced Electroni c Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES Electronic Signatures and Infrastructures (ESI); PDF Advanced Electroni c Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000- 1 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles Electronic Signatures and Infrastructures (ESI); PDF Advanced Electroni c Signature Profiles ; Part 4: PAdES Long Term - PAdES- LTV Profile Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures
ETSI TS 101 733	ETSI TS 101 733 V1.5.1"Electronic Signatures and Infrastructure (ESI): Electronic Signature Formats" (2002-12)