CONDIZIONI GENERALI
DEL SERVIZIO DI CERTIFICAZIONE

Ai fini del presente contratto si intende per:

- **"Certificato Qualificato di firma elettronica**" o semplicemente **"Certificato**": un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento (UE) N. 910/2014.
- **"Contratto**": indica tutta la documentazione contrattuale comprensiva delle presenti Condizioni Generali di Contratto, della Richiesta di Attivazione, del PKI Disclosure Statement, del Manuale Operativo e dei documenti e atti in essi richiamati, i quali disciplinano i rapporti tra le Parti.
- **"Dominio**: Il dominio *web* del SP, dove è stato effettuato il *download* del presente documento o ai diversi ed eventuali altri siti che il SP utilizza o utilizzerà nei rapporti con il Titolare, così come descritto al 4.5.3 "Limiti d'uso e di valore" del Manuale Operativo pubblicato sul sito *www.infocert.it*.
- **"InfoCert" o "TSP" (Trust Service Provider):** InfoCert S.p.A. - Società soggetta alla direzione e coordinamento di TINEXTA S.p.A. - con sede legale in Roma, P.zza Sallustio n. 9-00187, P. IVA 07945211006, *call center* 199.500.130, fax 06/83669634, PEC *infocert@legalmail.it*, che opera in qualità di prestatore di servizi fiduciari qualificati, sulla base di una valutazione di conformità effettuata dal *Conformity Assesment Body* CSQA Certificazioni S.r.l., ai sensi del Regolamento (UE) 910/2014 e delle norme ETSI EN 319 401, ETSI EN 319 411-1; ETSI EN 319 411-2, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319 403 e UNI CEIISO/IEC 17065:2012. InfoCert aderisce al codice etico reperibile sul sito, mediante accesso al seguente *link:* https://www.infocert.it/pdf/infocert/codice-etico-InfoCert.pdf ed opera quale certificatore accreditato ai sensi dell'art. 29 del D.L.vo 82/2005 e ss.mm.ii.("**Codice dell'Amministrazione Digitale**", di seguito denominato brevemente "**CAD**").
- "**PKI Disclosure Statement**" o "**PDS**": documento denominato "*Public Key Infrastructure Disclosure Statement*", cod. ICERT-INDI-PDS (redatto nel rispetto dei requisiti di pubblicazione previsti dallo Standard Europeo ETSI EN 319 411-1), che descrive il servizio di certificazione offerto da InfoCert S.p.A., le caratteristiche tecniche, la legislazione applicabile, le policy e gli standard relativi all'uso del Servizio, e le best practice che il Richiedente è obbligato ad adottare, allegato al Contratto e disponibile sul sito *www.infocert.it*.
- "**Certificate Practice Statement**", "CPS" o "**Manuale Operativo**": Manuale Operativo per i Certificati di Sottoscrizione di Firma Remota identificati dagli O.I.D. 1.3.76.36.1.1.34 e 1.3.76.36.1.1.64, cod. ICERT-INDI-MO, depositato da InfoCert presso l'Agenzia per l'Italia Digitale ("**AgID**") e reperibile sul sito *www.infocert.it*, sul sito dell'AgID o presso la sede della stessa oppure tramite richiesta da inviarsi per iscritto agli Uffici di Registrazione o al Contatto per gli Utenti Finali, come definito nell'ambito del Manuale Operativo.
- "**Procedura di Identificazione**": procedura eseguita ai fini della verifica dell'identità del Titolare secondo quanto previsto dal Manuale Operativo.
- "**Richiedente**" o "**Ufficio di Registrazione**" o "**Service Provider**" ("**SP**"): Soggetto che richiede l'emissione dei Certificati in favore di uno o più Titolari, incaricato dal TSP a svolgere, in qualità di Ufficio di Registrazione, le attività necessarie al rilascio del Certificato, così come indicato al paragrafo 1.3.5. della *Certificate Practice Statement*.
- "**Richiesta di Attivazione**": è il modulo con cui il Titolare richiede l'attivazione del Servizio FD.
- "**Ruolo**": Titolo e/o Abilitazione professionale in possesso del Titolare, ovvero l'eventuale potere di rappresentare persone fisiche o enti di diritto privato o pubblico, ovvero l'appartenenza a detti enti nonché l'esercizio di funzioni pubbliche.
- "**Servizio di Certificazione**" o semplicemente "**Servizio** ": è l'attività di certificazione, svolta da InfoCert, consistente nella procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo Certificato, in conformità a quanto previsto dal Contratto.
- **"Terzo Interessato":** il soggetto Richiedente che fornisce il consenso all'apposizione del Ruolo nel certificato, ove richiesto.
- **"Titolare"**: il soggetto, ivi compresa l'impresa, identificato in base a quanto riportato nella Richiesta di Attivazione, che richiede l'attivazione del Servizio FD e al quale è rilasciato il Certificato e i cui dati sono valorizzati all'interno dello stesso.

*** *** ***

SEZIONE I - A
DISPOSIZIONI GENERALI

1. Termini e condizioni del Servizio FD.

Le modalità di svolgimento ed i rapporti con il Richiedente e il Titolare sono regolati ai fini del presente Contratto: dal C.A.D., dal D.P.C.M. 22.02.2013, dalle delibere CNIPA (oggi Agenzia per l'Italia Digitale) n. 48/2005, n. 45/2009, dal Manuale Operativo, nonché dalle clausole del Contratto.

Il Richiedente ha assunto tutti gli obblighi previsti dal presente Contratto e, in particolare, l'obbligo di pagamento dei corrispettivi dovuti per il rilascio e la gestione dei Certificati.

Il Richiedente e il Titolare sono tenuti a leggere attentamente ed approvare le previsioni del Manuale Operativo relativo al tipo di Certificato richiesto e le presenti Condizioni Generali. Gli stessi sono altresì tenuti a leggere attentamente i requisiti tecnici sul tipo di certificato richiesto, come dettagliato nel CPS.

I Certificati emessi in base alle presenti Condizioni Generali possono essere utilizzati unicamente nell'ambito (i) del dominio informatico del SP, identificabile con le pagine *web* del sito del SP o ai diversi ed eventuali altri siti che il SP utilizza nei rapporti con la clientela (il "**Dominio SP**") e, eventualmente, (ii) per la sottoscrizione di documenti informatici proposti in favore dei clienti dal SP, il quale potrà agire in nome proprio o in qualità di mandatario, con o senza rappresentanza, di società terze di cui lo stesso colloca prodotti o servizi (di seguito, i "**Soggetti Terzi**"). Anche per questa ragione i Certificati sono efficaci solo qualora il Titolare abbia concluso o concluderà un rapporto contrattuale con il SP relativo ai servizi prestati dallo stesso a suo favore.

I contratti e i moduli sottoscritti dal Titolare per mezzo del Certificato (ivi compreso il relativo contenuto) non rientrano nell'oggetto del Servizio di Certificazione. Pertanto, è onere del Titolare verificarne attentamente i contenuti.

2. Informativa e Consenso ai sensi del Regolamento UE n. 679/2016.

InfoCert, titolare del trattamento dei dati forniti dal Titolare mediante la compilazione del modulo di Richiesta di Attivazione o nel corso del rapporto, si impegna a trattare i predetti dati personali, ai sensi e per gli effetti di cui all'art. 13 del Regolamento UE n. 679/2016, con l'ausilio di archivi cartacei e di strumenti informatici e telematici idonei a garantire la massima sicurezza e riservatezza, per le finalità e con le modalità illustrate nell'Informativa sul trattamento dei dati personali che è stata sottoposta al Titolare nel processo di sottoscrizione del presente Contratto e disponibile al seguente link*: https://prd-istituzionale-infocert-cdn.azureedge.net/pdf/infocert/Infomativa%20Privacy_clienti%20che%20acquistano%20da%20sito%20e%20clienti%20finali.pdf?_t=1672935397.*

3. Responsabilità del Titolare.

Il Titolare è responsabile della veridicità dei dati comunicati in fase di identificazione e nel Modulo di Richiesta. Qualora lo stesso, al momento dell'identificazione, abbia, anche attraverso l'utilizzo di documenti personali non veri, celato la propria reale identità o dichiarato falsamente di essere altro soggetto, o, comunque, agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel Certificato, egli sarà considerato responsabile di tutti i danni derivanti al TSP e/o a terzi dall'inesattezza delle informazioni contenute nel Certificato, con obbligo di garantire e manlevare il TSP per eventuali richieste di risarcimento dei danni.

4. Comunicazioni.

Ogni comunicazione scritta dovrà essere inviata dai Titolari al Contatto per gli Utenti Finali.

InfoCert invierà eventuali comunicazioni per iscritto al Richiedente e/o Titolare all'indirizzo di posta elettronica certificata indicato oppure, in mancanza, all'indirizzo di posta elettronica ordinaria indicato nel Modulo di richiesta.

5. Conclusione del Contratto / Clausola sospensiva / Diritto di recesso.

Fermo restando quanto previsto dal precedente art. 3, il Contratto è concluso nel momento in cui InfoCert riceve la Richiesta di Attivazione correttamente compilata in ogni sua parte.

Fermo restando quanto sopra, l'efficacia del Contratto è sospensivamente condizionata all'esito positivo dell'identificazione del Titolare. In caso di esito negativo dell'identificazione, pertanto, il Certificato digitale non sarà emesso dal TSP o, se emesso, si considererà privo di efficacia sin dal momento della sua emissione ed il Contratto si intenderà risolto di diritto.

Il Certificato viene emesso all'esito della corretta identificazione del Titolare. Qualora la Richiesta provenga da un soggetto non autorizzato, non sia integra o manchi delle informazioni richieste, il Contratto non si considera concluso. In caso di esito negativo dell'identificazione, pertanto, il Certificato non sarà emesso dal TSP o, se emesso, si considererà privo di efficacia sin dal momento della sua emissione ed il Contratto si intenderà risolto di diritto.

Il Titolare, se consumatore, ha richiesto l'esecuzione immediata del Servizio con la sottoscrizione della Richiesta di Attivazione, accettando espressamente la perdita del diritto di recesso, a norma dell'art. 59, lett. a), del Codice del Consumo e della presente disposizione. Fermo restando quanto previsto nel successivo art. 16, il Titolare riconosce ed accetta che il presente Contratto si risolverà di diritto, in caso di cessazione per qualsiasi motivo del rapporto tra il medesimo Titolare e il SP, senza che il Titolare abbia nulla a che pretendere nei confronti di InfoCert in conseguenza di tale risoluzione.

6. Disponibilità del Servizio.

La richiesta e/o verifica del Servizio di Certificazione è disponibile dalle 00:00 alle 24:00, 7 giorni su 7. InfoCert si impegna ad assicurare il rispetto del 95% della disponibilità di cui sopra.

7. Legge applicabile.

Il presente Contratto e i rapporti tra le Parti sono regolati dalla legge italiana. Per quanto non espressamente previsto si rinvia alle disposizioni del Codice Civile ed alle normative applicabili in materia.

8. Procedure di reclamo e risoluzione delle controversie.

Si informa che, per eventuali reclami, è possibile prendere contatti direttamente con InfoCert, scrivendo all'indirizzo *reclami@infocert.it* oppure attivando la procedura facilmente accessibile al seguente *link: https://help.infocert.it/reclami/*, dal quale è possibile inviare un reclamo *online*, mediante compilazione di un modulo *standard*.

Ai sensi del Regolamento UE n. 524/2013, per la risoluzione delle controversie relative ai contratti *online* e ai servizi offerti *online*, segnaliamo altresì la possibilità di ricorrere al procedimento di *Online Dispute Resolution* (ODR), raggiungibile al seguente *link: https://webgate.ec.europa.eu/odr/*.

Qualsiasi controversia dovesse insorgere tra le Parti in ordine al presente Contratto, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, sarà devoluta in via esclusiva al Tribunale di Roma, con esclusione di qualsiasi altro foro competente.

Nel caso in cui il Titolare sia un consumatore, ai sensi dell'art. 66 bis del Codice del Consumo, le controversie civili inerenti il Contratto concluso dal consumatore sono devolute alla competenza territoriale inderogabile del giudice del luogo di residenza o di domicilio di questo. Ai sensi dell'art. 141 sexies del Codice del Consumo, seppure InfoCert non si sia impegnata a ricorrere ad alcun organismo di risoluzione alternativa delle controversie, si informa il consumatore che può servirsi, su base volontaria, dei metodi di risoluzione extragiudiziale delle controversie previsti dal Codice del Consumo, dal D.L.vo 28/2010 e dalle altre norme di legge applicabili in materia.

*** *** ***

SEZIONE I - B

CERTIFICATI DI SOTTOSCRIZIONE CON PROCEDURA DI FIRMA REMOTA

9. Oggetto.

In generale, la richiesta di un Certificato ha quale oggetto l'emissione, da parte del TSP, di un certificato qualificato di firma elettronica, da associare alla firma digitale del Titolare, creata tramite un dispositivo sicuro, in conformità a quanto previsto dalle disposizioni normative richiamate dall'art. 1, I c., delle presenti Condizioni Generali.

I Certificati sono utilizzati mediante apposite procedure informatiche tali da garantire il rispetto di quanto previsto all'art. 35, III c., del C.A.D.

Al Titolare che acquista il Servizio FD, il TSP mette a disposizione una procedura informatica, residente sui sistemi di InfoCert o su quelli del Richiedente, mediante la quale il medesimo Titolare può gestire il Certificato di sottoscrizione per procedura di firma remota presente sul modulo HSM (*Hardware Security Module*).

In particolare, il Servizio FD di tipo One Shot consente al Titolare, previa autenticazione dello stesso a mezzo di appositi strumenti, l'utilizzo - in forma remota - del Certificato, nel termine di durata di validità dello stesso pari a 60 (sessanta) minuti ai fini della sottoscrizione dei documenti o dei relativi *hash* provenienti da una specifica procedura informatica indicata dal Richiedente.

10. Modulo di Richiesta dei Servizi di Firma Digitale.

Il Richiedente, ai sensi di quanto previsto nel PDS e nel Manuale Operativo pubblicato nel sito del TSP, ha assunto l'impegno di pagare i corrispettivi del Servizio FD e di indicare, attraverso specifici atti e procedure, i soggetti a cui i Certificati dovranno essere rilasciati.
Il Titolare deve richiedere al TSP la registrazione e l'emissione del Certificato con le modalità stabilite nel PDS e dettagliate nel Manuale Operativo, utilizzando l'apposito Modulo di Richiesta messo a sua disposizione in modalità telematica. In caso di esito positivo delle verifiche necessarie al rilascio del Certificato, lo stesso è emesso, pubblicato nell'apposito registro e rilasciato al Titolare ai sensi del Manuale Operativo.
I Certificati sono efficaci solo qualora il Titolare abbia concluso o concluderà un rapporto contrattuale con il SP relativo ai servizi prestati dallo stesso a suo favore ovvero dallo stesso proposti.
Il Titolare presta fin da ora il proprio consenso affinché il TSP registri e mantenga per 20 (venti) anni le informazioni raccolte con la registrazione, quelle concernenti gli strumenti forniti, le revoche, l'identità e gli attributi inseriti nel Certificato e altresì acconsentono al trasferimento di tali informazioni a terze parti alle stesse condizioni se il TSP terminerà la propria attività, così come indicato al par. 5.8. del Manuale Operativo.

11. Attivazione e gestione del Servizio FD.

Il Servizio FD è attivato in seguito all'individuazione e comunicazione al TSP da parte del Richiedente della procedura informatica a mezzo della quale saranno inviati i documenti da sottoporre alla procedura di firma remota ed all'attivazione delle chiavi di firma da parte del Titolare.
Qualora il Richiedente richieda, ai sensi dell'art. 28, c. 3, del C.A.D. e della determinazione AgID 121/2019 e ss.mm.ii., l'inserimento del Ruolo nel Certificato, questo avviene secondo quanto stabilito dal Manuale Operativo di riferimento, prevedendo altresì anche il consenso del Terzo Interessato.

12. Obblighi del Titolare.

Il Titolare deve indicare, assumendo ogni responsabilità in merito, la tipologia di sistema di autenticazione prescelta al fine di attivare la procedura di firma remota.
Gli obblighi del Titolare sono quelli indicati dalla normativa vigente, dal PDS e dal Manuale Operativo. Ai sensi dell'art. 32 del C.A.D., il Titolare è obbligato ad adottare tutte le misure idonee ad evitare che dall'utilizzo della firma digitale derivi danno ad altri.
In considerazione della circostanza che l'utilizzo di una firma digitale comporta la possibilità di sottoscrivere atti e documenti rilevanti a tutti gli effetti della legge italiana e riconducibili unicamente alla sua persona, il Titolare è obbligato ad osservare la massima diligenza nell'indicazione, utilizzo, conservazione e protezione degli strumenti di autenticazione messi a disposizione dal TSP o dall'Ufficio di Registrazione. Gli strumenti di autenticazione per l'attivazione della procedura di firma remota sono strettamente personali. Pertanto, il Titolare è tenuto a proteggere la segretezza di detti strumenti non comunicandoli o divulgandoli a terzi, neanche in parte, e conservandoli in un luogo sicuro. Il Titolare è, inoltre, tenuto a provvedere all'adeguamento dei suoi sistemi *hardware* e *software* alle misure di sicurezza previste dalla legislazione vigente.
È responsabilità del Titolare verificare attentamente il contenuto dei documenti che il medesimo intende sottoscrivere con la procedura di firma remota, impegnandosi ad astenersi dall'attivare la procedura di firma qualora detto contenuto non sia conforme alla volontà che egli intende esprimere.

13. Obblighi del TSP.

Gli obblighi del TSP sono quelli indicati dalla normativa vigente, dal PDS e dal Manuale Operativo al punto 1.3.1. e dalle presenti Condizioni Generali.
La procedura di riconoscimento del Titolare, con particolare riguardo all'identificazione dello stesso, può essere effettuata in via alternativa secondo una delle modalità previste nel Manuale Operativo e concordate tra InfoCert e il Richiedente.
Il TSP non assume altri obblighi ulteriori rispetto a quelli previsti dalle presenti Condizioni Generali, dal PDS, dal Manuale Operativo e dalle leggi vigenti in materia di attività di certificazione.
In particolare, il TSP si obbliga a:

- Conservare in un apposito archivio digitale non modificabile per 20 (venti) anni tutti i Certificati emessi nelle modalità previste dal PDS e dal Manuale Operativo;
- Garantire la conservazione digitale nelle modalità di cui sopra anche dei *logs* del Servizio.

Il TSP non presta alcuna garanzia (i) sul corretto funzionamento e sulla sicurezza dei macchinari *hardware* e dei *software* utilizzati dal Titolare, (ii) su usi del Certificato diversi rispetto a quelli previsti dalle norme italiane vigenti, dal PDS e dal Manuale Operativo, (iii) sul regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali, (iv) sulla validità e rilevanza, anche probatoria, del Certificato o di qualsiasi messaggio, atto o documento ad esso associato o confezionato tramite le chiavi a cui il Certificato è riferito, in relazione ad atti e documenti sottoposti a legislazioni differenti da quella italiana nonché sulla loro segretezza e/o integrità (nel senso che eventuali violazioni di quest'ultima sono, di norma, rilevabili da Titolare o dal destinatario attraverso l'apposita procedura di verifica).
Il TSP garantisce unicamente il funzionamento della procedura di firma remota secondo i livelli di servizio indicati al Richiedente e al Titolare.
In considerazione di quanto stabilito al precedente art. 12, ult. c., il TSP non assume alcun obbligo di sorveglianza in merito al contenuto, alla tipologia o al formato elettronico dei documenti e degli *hash* trasmessi dalla procedura informatica indicata dal Richiedente o dal Titolare, non assumendo alcuna responsabilità, salvo il caso di dolo o colpa grave, in merito alla validità degli stessi ed alla riconducibilità dei medesimi alla effettiva volontà del Titolare.

14. Durata del contratto e validità del Certificato.

L'efficacia delle presenti Condizioni Generali decorrerà dalla data in cui il TSP emetterà il Certificato e avrà durata pari a quella indicata nel campo "validità (*validity*)" dello stesso.

15. Corrispettivi.

I corrispettivi per l'erogazione del Servizio FD sono versati ad InfoCert nell'ambito degli accordi intercorsi tra questa e il SP.

16. Revoca, sospensione e ripristino del Certificato.

Essendo la durata del certificato minore o uguale del tempo minimo (60 minuti) previsto per rendere pubblica l'informazione sulla subentrata invalidità dello stesso, per i Certificati oggetto delle presenti Condizioni Generali di Contratto non è prevista la possibilità di revoca e sospensione.

17. Responsabilità del TSP.

Fermo restando quanto previsto all'art. 13 delle presenti Condizioni Generali, la responsabilità del TSP per il Servizio FD è regolata dal Manuale Operativo (pubblicato nel sito del TSP) al punto 4.1.2, dalle presenti Condizioni Generali e dalla normativa vigente.
Il TSP, inoltre, fin dalla fase di formazione del Contratto, e anche nel corso dell'esecuzione, non risponde per eventuali danni e/o ritardi dovuti a malfunzionamento o blocco del sistema informatico.

18. Risoluzione del rapporto.

Il TSP ha facoltà, ai sensi dell'art. 1456, c.c., di risolvere il presente Contratto, qualora il Titolare si sia reso inadempiente ad una delle obbligazioni previste a suo carico dalle presenti Condizioni Generali nonché in caso di mancato pagamento da parte del Richiedente del corrispettivo dei servizi o nelle altre ipotesi previste dalle presenti Condizioni.

Dei provvedimenti stabiliti nel presente articolo verrà data comunicazione al Richiedente e al Titolare con le forme di cui al precedente art. 4.
In tutti i casi di risoluzione non dipendenti dal TSP, lo stesso avrà diritto a trattenere l'importo corrisposto ai sensi del precedente art. 15 dal Richiedente.