

ALLEGATO DI PROCESSO CERTIFICATI QUALIFICATI E DI AUTENTICAZIONE PROCESSO DI SOTTOSCRIZIONE E MODALITÀ DI RICONOSCIMENTO

Parte 1

- 1) Il processo di identificazione e di rilascio di un Certificato di firma può essere attivato dalla RA (Registration Authority) tramite la Piattaforma fornita da InfoCert, in forza dell'Accordo sottoscritto, con la necessaria presenza di un ente emittitore (in seguito "Ente Emittitore") per il rilascio del dispositivo fisico CNS.

Nell'ambito del processo di seguito descritto, si distinguono i seguenti soggetti:

- InfoCert:
 - eroga i Servizi servendosi del riconoscimento posto in essere dalla RA;
 - gestisce il *front end* standard della Piattaforma di erogazione dei Servizi, salvo personalizzazioni che verranno eseguite dalla RA a propria cura e spese, nel rispetto di quanto eventualmente pattuito;
 - fornisce al Titolare gli strumenti standard di autenticazione alla procedura di rilascio dei Certificati, salvo personalizzazioni che verranno eseguite dalla RA a propria cura e spese, nel rispetto di quanto eventualmente pattuito.
- La RA:
 - identifica l'Utente sotto la propria responsabilità;
 - invia a InfoCert l'asserzione d'identità o il verbale di riconoscimento che attesta l'avvenuta identificazione del Titolare;
 - gestisce l'eventuale personalizzazione del *front end* della Piattaforma di erogazione dei Servizi, sulla base delle linee guida fornite da InfoCert;
 - fornisce il dispositivo fisico al Titolare, anche per conto di InfoCert o, nei casi di emissione della Carta Nazionale dei Servizi (CNS), dell'Ente Emittitore, se appositamente delegato

Il processo per il rilascio dei certificati, di cui agli articoli 2A e 2B, varia sulla base della tipologia di Piattaforma fornita da InfoCert.

Qualora la RA fruisca della Piattaforma IPP, si prega di far riferimento anche al processo descritto al seguente link: [Infocert Partner Platform](#)

2A) CERTIFICATI REMOTI

Il processo di identificazione delegato alla RA tramite idonea documentazione contrattuale è finalizzato al rilascio di una delle seguenti tipologie di certificato qualificato definite all'art. 3.2 dell'allegato tecnico:

- **Certificato di Firma Remota**
- **Certificato Long Term**
- **Certificato OneShot**
- **Certificato OneShot di durata.**

In ogni caso, detto processo standard prevede i seguenti step:

1. L'Utente Finale entra in contatto con la RA per richiedere un servizio e fornisce alla RA i propri dati personali.

2. La RA identifica l'Utente sotto la propria responsabilità, in conformità all'Accordo e nel rispetto della normativa vigente, secondo una delle modalità descritte nel paragrafo 3.2.3. del Manuale Operativo ICERT-INDI-MO.
3. La RA invia a InfoCert l'asserzione di identità o il verbale di riconoscimento che attesta l'avvenuta corretta identificazione dell'utente e in base alla quale InfoCert emette il Certificato di firma. L'asserzione di identità o il verbale sono firmati digitalmente attraverso un certificato di firma qualificata con procedura automatica da parte di un soggetto delegato dalla RA. Può accadere che il Certificato venga rilasciato anteriormente al ricevimento delle evidenze della avvenuta identificazione: in tale ipotesi, la validità del Certificato è sospensivamente condizionata al positivo esito del riconoscimento.
4. Qualora venga richiesto un Certificato di Firma Remota, il Titolare deve creare il proprio Profilo Utente inserendo il nome utente e la password necessari per utilizzare il certificato su altre piattaforme.
5. Il Titolare visualizza la documentazione contrattuale di InfoCert relativa al Servizio scelto, accessibile mediante link dalla Piattaforma (il tutto visualizzabile sul sito istituzionale di InfoCert) e, al fine dell'emissione, procede con l'accettazione della stessa.
6. Il Titolare visualizza la documentazione che la RA reputa necessario far firmare con il Servizio InfoCert, accettandone la sottoscrizione.
7. Il Titolare si autentica alla procedura tramite OTP (One Time Password - per i certificati di Firma Remota e *Long Term* viene richiesta la creazione e/o inserimento di un PIN) e procede a sottoscrivere la documentazione.
8. La RA (o InfoCert se espressamente concordato) mette a disposizione del Titolare i contratti firmati (sia quelli di InfoCert, sia quelli eventuali della RA).

2B) CERTIFICATI SU DISPOSITIVO

Il processo di identificazione delegato alla RA tramite idonea documentazione contrattuale è finalizzato al rilascio di un certificato di sottoscrizione e/o un certificato di autenticazione tramite uno dei seguenti dispositivi:

- **Token USB**
- **Token Wireless**
- **Smart Card**

All'interno dei tali Dispositivi, possono essere inseriti uno o più dei seguenti Certificati, definiti all'art. 3.2 dell'allegato tecnico:

- **Certificato di Firma elettronica Qualificata**
- **Certificato di autenticazione**
- **Certificato di autenticazione-CNS**

In ogni caso, il processo standard prevede i seguenti step:

1. Il Titolare entra in contatto con la RA per richiedere un Certificato di sottoscrizione e/o autenticazione su dispositivo e fornisce alla RA i propri dati personali.

2. Il Titolare visualizza la documentazione contrattuale di InfoCert relativa al Servizio scelto (Richiesta di Attivazione, Condizioni Generali di Contratto, Privacy Policy e Allegato/i Tecnico/i), accessibile mediante link dalla Piattaforma di riconoscimento e sul sito istituzionale di InfoCert.
3. La RA identifica il Titolare sotto la propria responsabilità, in conformità all'Accordo e nel rispetto della normativa vigente, secondo una delle modalità descritte nel paragrafo 3.2.3. del Manuale Operativo ICERT-INDI-MO. Infatti, a seconda del tipo di Servizio erogato, l'identità del Titolare deve essere accertata dalla RA prima dell'emissione del Certificato o entro 30 giorni dal momento dell'emissione dello stesso.
4. La RA invia a InfoCert l'asserzione di identità o il verbale di riconoscimento firmati digitalmente, che attesta l'avvenuta corretta identificazione dell'utente e in base alla quale InfoCert emette il Certificato di sottoscrizione e/o di autenticazione.
5. Il Titolare sottoscrive la Richiesta di attivazione di un Certificato di sottoscrizione e/o autenticazione su dispositivo, contenente i dati raccolti e validati.
6. Il Titolare riceve una e-mail all'indirizzo indicato durante il processo all'interno della quale sarà allegata una busta accessibile tramite una *passphrase* o, qualora quest'ultima non sia stata scelta, tramite il Codice fiscale del Titolare.
7. Aperta la busta, il Titolare è dettagliatamente accompagnato al processo di attivazione dei propri certificati. Verrà generata la coppia di chiavi e, dopo le opportune verifiche della RA, verrà emesso il Certificato richiesto all'interno del Dispositivo vergine.
8. Qualora venga richiesta l'emissione di una CNS, per il tramite di un Ente Emittitore, il numero di serie del dispositivo fisico che supporta i Certificati identifica l'Ente Emittitore e deve essere verificato dalla RA.
9. Sulla Carta deve essere presente la scritta "Carta Nazionale dei Servizi" ed il nome dell'Ente Emittitore che l'ha emessa.
10. Conclusasi la fase di registrazione ed emissione del Certificato di sottoscrizione e/o autenticazione il Titolare riceve il dispositivo di firma e/o autenticazione nelle modalità concordate o presso l'Ente Emittitore.

3) DURATA

In deroga a quanto disposto dall'Accordo, qualora la RA si dovesse avvalere di un dispositivo fisico emesso dalla Provincia di Padova questo potrà avvenire per tutta la durata della convenzione sottoscritta tra InfoCert e la Provincia medesima, ossia il 31 dicembre 2031, anche se la durata dell'Accordo concluso fosse comunque successiva.

Parte 2

(A) Modalità di identificazione:

A.1 L'identità dell'Utente deve essere accertata dalla RA, secondo le modalità di cui all'art. 3.2.3 del CPS, prima dell'emissione del Certificato di cui al punto 2A e 2B o entro 30 giorni dal momento dell'emissione dello stesso. In tal senso, l'attestazione di avvenuta identificazione deve giungere ai sistemi di InfoCert antecedentemente alla richiesta di certificazione o entro e non oltre il periodo di 30 giorni successivi all'emissione del certificato. In quest'ultimo caso, InfoCert invia alla RA e al Titolare la documentazione sottoscritta solo una volta ricevuta l'attestazione di avvenuto riconoscimento.

(B) Strumenti di autenticazione alla procedura di firma remota:

B.1 La chiave privata del Titolare, contenuta negli HSM (Hardware Security Module) di InfoCert, può essere utilizzata unicamente dal Titolare stesso tramite i seguenti strumenti di autenticazione:

- Autenticazione Interna:
 - Per certificati di Firma Remota e *Long Term*: tramite il codice PIN scelto in autonomia al momento della richiesta del Certificato e una *One Time Password* ("OTP") generata e resa disponibile da InfoCert al numero di telefonia mobile associato al Titolare.
 - Per certificati *One Shot*: tramite una *One Time Password* ("OTP") generata e resa disponibile da InfoCert al numero di telefonia mobile associato al Titolare.
- Autenticazione Esterna: tramite il codice PIN fornito dalla RA o scelto dal Titolare al momento della richiesta del Certificato e una *One Time Password* ("OTP") generata e resa disponibile al Titolare dalla RA stessa.

(C) Customizzazione del Front End: sviluppo e mantenimento

C.1 Qualora il *Front End* attraverso il quale il Titolare verrà guidato nelle fasi di richiesta, registrazione, emissione ed eventuale utilizzo del Certificato, venga customizzato dalla RA, secondo modalità preventivamente condivise con InfoCert, debbono esser osservate le seguenti prescrizioni:

- a) il *Front End* deve assicurare che i dati raccolti sugli applicativi della RA non subiscano alcuna variazione e che siano quindi trasmessi a InfoCert in maniera integrale per i servizi di registrazione e di emissione del Certificato;
- b) il *Front End* sviluppato dalla RA deve esser sottoposto a un *test* di collaudo da parte di InfoCert, a spese della RA, prima dell'avvio in produzione per assicurare che tutti gli elementi indispensabili siano stati implementati, che siano funzionanti e che l'ordine delle chiamate applicative sia stato rispettato. Il collaudo avviene in contraddittorio tra le Parti;
- c) in caso di mancato superamento del *test*, si distinguono due ipotesi. Se esso dipende da errori tecnici o malfunzionamenti dell'applicazione sviluppata dalla RA, l'efficacia degli accordi nell'ambito dei quali è stato eseguito il *test* prosegue regolarmente, salva l'impossibilità di processare richieste di rilascio di Certificati; sarà dunque onere e interesse della RA porre rimedio a sue spese al malfunzionamento del *Front End*. Se, invece, il mancato superamento dipende invece dalla *non compliance* del *Front End* rispetto alla normativa regolamentare e/o tecnica concernente il rilascio dei Certificati, InfoCert ha il diritto di sospendere l'esecuzione dei Servizi a suo carico e l'erogazione dei certificati finché la RA non rende il *Front End* conforme a detta normativa; per il resto, l'efficacia degli accordi tra le parti nell'ambito del quale è stato eseguito il *test* prosegue regolarmente;
- d) nell'ipotesi soprastante, l'accertamento della soluzione del problema (tecnico o di *compliance*) deve essere effettuato mediante un nuovo *test* di collaudo;
- e) la RA si impegna a non modificare in alcun modo il *Front End* implementato dopo il positivo *test* di collaudo, se non previa comunicazione ad InfoCert. In tali ipotesi, la RA, con un preavviso di almeno 60 giorni, deve dare evidenza, in apposito documento tecnico, delle modifiche che si richiedono. Allorché InfoCert nulla eccepisca nei successivi 60 giorni, la RA potrà procedere con le modifiche dichiarate. In ogni caso, qualsivoglia variazione al *Front End* dovrà essere valutata da InfoCert con un nuovo *test* di collaudo, sempre in contraddittorio, trovando applicazione quanto espresso ai punti precedenti.



MANDATO MASTER R.A.O.

tra

InfoCert S.p.A., con sede legale in Roma, Piazzale Flaminio 1/B, CF e P. IVA 07945211006, in persona dell'Amministratore Delegato e legale rapp.te *pro-tempore* dott. Danilo Cattaneo, società soggetta a direzione e coordinamento di Tinexta S.p.A. (di seguito **"InfoCert"**)

e

XXXX, con sede in _____ n. _____, CF e P. IVA _____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, anche **"Ufficio di Registrazione"** o **"R.A."**)

e

XXXX, residente in _____ n. _____, CF _____, (di seguito, **"Master R.A.O."**)

PREMESSO CHE:

- a) L'Ufficio di Registrazione ed InfoCert, in data _____ hanno stipulato apposita convenzione (di seguito **"Convenzione"**), con la quale è stato conferito mandato alla prima di svolgere le funzioni di Ufficio di Registrazione, per il rilascio dei Certificati di firma, secondo quanto previsto dal Manuale Operativo ICERT-INDI-MO (di seguito il **"Manuale Operativo Certificati"**) e/o per il rilascio dello SPID secondo quanto previsto dal Manuale Operativo ICERT-MO-SPID (**"Manuale Operativo SPID"**);
- b) ai sensi della Convenzione, la R.A. ha facoltà di operare anche attraverso propri Master R.A.O., che si impegneranno ad osservare gli obblighi meglio dettagliati nel prosieguo;
- c) con il presente atto, si desidera conferire al Master R.A.O. apposito mandato per l'esecuzione delle attività di sua competenza ai sensi della Convenzione, concernenti le fasi identificazione, autenticazione, revoca e registrazione degli utenti (gli **"Utenti"**), nonché quelle di rilascio ed erogazione dei servizi InfoCert (**"Servizi Trust"**), ai sensi del Manuale Operativo in aggiunta alla gestione operativa e organizzativa delle attività tipiche della piattaforma dedicata, propedeutica al caricamento e alla gestione di tutta la documentazione afferente al ciclo-vita della R.A. (**"Piattaforma"**) e che, pertanto, agirà in nome e per conto della RA stessa;
- d) Il Master R.A.O. si è reso disponibile a svolgere le attività elencate al punto precedente e meglio dettagliate nel presente atto (il **"Mandato"**);
- e) le procedure di registrazione sono analiticamente esposte nel Manuale Operativo di InfoCert sopra citato, pubblicato sul sito Internet "www.infocert.it", e nei provvedimenti legislativi e amministrativi eventualmente ivi richiamati.

TUTTO CIO' PREMESSO, le Parti convengono quanto segue:

1. PREMESSE

1.1. Le premesse, nonché il PDS e il Manuale Operativo Certificati e Manuale Operativo SPID disponibili sul sito InfoCert (<https://www.firma.infocert.it/documentazione/>) formano parte integrante del presente Mandato che sarà espletato secondo le specifiche condizioni ivi previste.

2. OGGETTO

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



2.1. InfoCert e la RA conferiscono mandato non esclusivo al Master R.A.O. a svolgere parte dell'attività di cui alla lett. c) delle premesse e, in particolare, a identificare gli Utenti con certezza, esclusivamente attraverso sistemi autorizzati da InfoCert) e secondo le modalità concordate da InfoCert e dalla R.A.

3. OBBLIGHI DELLE PARTI

3.1 La R.A., ferme rimanendo le obbligazioni di cui alla Convenzione, provvederà a:

- a) supervisionare, per conto di InfoCert, l'attività di formazione e/o aggiornamento del Master R.A.O.;
- b) verificare che il Master R.A.O. esegua con la dovuta diligenza le attività a lui assegnate;
- c) monitorare costantemente che il Master R.A.O. mantenga i requisiti di onorabilità, competenza, affidabilità ed esperienza ai sensi dell'art. 24 par. 2 lett b) del Regolamento eIDAS;
- d) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert, qualora cessi il rapporto di dipendenza/collaborazione tra l'Ufficio di Registrazione e il Master R.A.O., ovvero si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del Master R.A.O.), dandone tempestiva comunicazione per iscritto ad InfoCert entro 24 (ventiquattro) ore lavorative.

3.2 Il Master R.A.O. con la diligenza del mandatario ex art. 1710, c.c., dovrà:

- a) conseguire la formazione necessaria per le finalità del presente mandato, partecipando ai corsi di formazione come predisposti dalla R.A. e/o da InfoCert ai sensi dell'art. 3.1 lett. a);
- b) assumere gli obblighi descritti nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere già un'organizzazione di personale e di beni adeguata all'esercizio delle Attività;
- c) conservare debitamente le credenziali della Piattaforma, attraverso cui coordinerà le attività per conto della R.A.;
- d) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust definite da InfoCert;
- e) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert o dalla R.A., qualora cessi il rapporto di dipendenza/collaborazione tra l'Ufficio di Registrazione e il R.A.O., ovvero si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva notizia per iscritto ad InfoCert;
- f) esercitare le Attività nell'interesse di InfoCert e con la diligenza del mandatario, ex art. 1710, c.c.;
- g) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi;
- h) informare entro 8 (otto) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione da parte dei R.A.O.;
- i) consentire alle Autorità di vigilanza, nonché agli incaricati di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
- j) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
- k) sottoporre agli Utenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare preventivamente con quest'ultima qualsiasi documento da rilasciare al Richiedente e/o Utente, relativamente all'attività di registrazione e/o di rilascio dei Servizi Trust;

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00



- l) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla Piattaforma con obbligo di custodia, per un utilizzo da parte di questi ultimi finalizzato all'espletamento delle attività precipue e nel rispetto delle obbligazioni ivi assunte;
- m) obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
- n) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione richiesta da InfoCert (a titolo meramente esemplificativo e non esaustivo: mandati, modulistica dei Servizi Trust), che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta;

3.3. La R.A. e il Master R.A.O. saranno solidalmente responsabili nei confronti di InfoCert per le attività previste nel presente Mandato.

3.4. La violazione di uno qualsiasi degli obblighi di cui al comma 3.1. e 3.2. del presente articolo costituirà giusta causa di revoca del presente Mandato da parte di InfoCert o della R.A., che sarà esercitata a mezzo di apposita comunicazione, fatto salvo il diritto al risarcimento dei danni eventualmente subiti e *subendi*. In caso di revoca, il Master R.A.O. è obbligato a cessare qualsiasi attività posta in essere in base al presente atto ed a restituire i materiali ricevuti al fine dell'espletamento dell'incarico.

4 CORRISPETTIVI E FORNITURA

4.1. La R.A. ed il Master R.A.O. per lo svolgimento dell'attività prevista nel Mandato non potranno pretendere il pagamento di alcun corrispettivo da parte di InfoCert né vantare alcuna esclusiva nei suoi confronti.

4.2. L'esclusione di cui al precedente comma è altresì valida con riferimento ai mezzi necessari per l'esecuzione del Mandato e alle anticipazioni e spese sostenute dal mandatario.

5 DURATA E DECORRENZA

5.1. Il Mandato avrà efficacia per il periodo di un anno dalla data della sua sottoscrizione e si rinnoverà tacitamente per periodi annuali, salvo disdetta di una delle Parti, da comunicarsi per iscritto almeno 3 (tre) mesi prima della scadenza del periodo annuale, a mezzo Posta Elettronica Certificata. Il Mandato perderà automaticamente efficacia, in ogni caso di cessazione della Convenzione in essere tra InfoCert e la R.A.

5.2. Durante il periodo di vigenza del Mandato, InfoCert avrà diritto, senza pagamento di alcun corrispettivo, di recedere da esso in qualsiasi momento, con comunicazione della volontà di esercitare tale diritto a mezzo Posta Elettronica Certificata o raccomandata A/R.

5.3. In caso di recesso e/o revoca, il Master R.A.O. non potrà vantare alcuna richiesta nei confronti della R.A. e/o di InfoCert, neanche per eventuali danni subiti in conseguenza dello stesso.

5.4. Resta salvo tra le Parti che in caso di risoluzione del presente Mandato, la Convenzione rimane valida ed efficace tra InfoCert e la R.A. fino a naturale vigenza della stessa.

6 PRIVACY

6.1. La R.A. e il Master R.A.O. si impegnano alla piena osservanza, per quanto di rispettiva competenza, del dettato del Regolamento (UE) 679/2016 e della normativa italiana compatibile con lo stesso.

6.2. Nell'espletamento del mandato, il Master R.A.O. sarà autorizzato al trattamento dei dati per lo svolgimento delle sole attività oggetto del presente Mandato, sotto la diretta autorità della R.A. e InfoCert attenendosi alle istruzioni impartite da quest'ultima.

6.3. In particolare, il Master R.A.O. metterà in atto le seguenti operazioni di trattamento:

- a) verifica del documento di identità del richiedente, della relativa validità e della corrispondenza al soggetto richiedente;

InfoCert SpA

Piazzale Flaminio 1/B, 00196 – Roma (RM), Italia
T +39 06 836691 F +39 06 833669634
info@infocert.it
infocert.it infocert.digital

Società soggetta alla direzione e coordinamento di Tinexta SpA
P.IVA 07945211006 REA n. 1064345
Cap. Soc. Sottoscritto e versato € 21.099.232,00

- ## 7 LEGGE APPLICABILE E FORO COMPETENTE

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

InfoCert S.p.A.	Ufficio di Registrazione	Master R.A.O.
_____	_____	_____

(Ufficio di Registrazione)

(Master R.A.O.)



MANDATO QUADRILATERALE PER LO SVOLGIMENTO DI ATTIVITA' DA PARTE DEL R.A.O.

SUPPLIER

PER IL RILASCIO DI SERVIZI DI INFOCERT

tra

InfoCert S.p.A., con sede legale in Roma, Piazzale Flaminio 1/B, CF e P. IVA 07945211006, in persona dell'Amministratore Delegato e legale rapp.te *pro-tempore* dott. Danilo Cattaneo, società soggetta a direzione e coordinamento di Tinexta S.p.A. (di seguito "**InfoCert**")

e

XXXX, con sede in _____ n. _____, CF e P. IVA _____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, anche "**Ufficio di Registrazione**" o "**R.A.**")

e

XXXX, con sede in _____ n. _____, CF e P.IVA _____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, "**R.A.O. Supplier**")

e

XXXX, residente in _____ n. _____, CF _____, (di seguito, "**Operatore dell'Ufficio di Registrazione**" o "**R.A.O.**")

PREMESSO CHE:

- a) L'Ufficio di Registrazione ed InfoCert, in data _____ hanno stipulato apposita convenzione (di seguito "**Convenzione**"), con la quale è stato conferito mandato alla prima di svolgere le funzioni di Ufficio di Registrazione, per il rilascio dei Certificati di firma, secondo quanto previsto dal Manuale Operativo ICERT-INDI-MO (di seguito il "**Manuale Operativo Certificati**") e/o per il rilascio dello SPID secondo quanto previsto dal Manuale Operativo ICERT-MO-SPID ("**Manuale Operativo SPID**");
- b) ai sensi della Convenzione, la R.A. ha facoltà di operare anche attraverso propri R.A.O. Supplier, che si impegneranno ad osservare gli obblighi meglio dettagliati nel prosieguo;
- c) con il presente atto, si desidera conferire al R.A.O. Supplier apposito mandato per l'esecuzione delle attività di sua competenza ai sensi della Convenzione, da conferire a sua volta attraverso apposito mandato al R.A.O., nell'ambito dell'identificazione, autenticazione, registrazione e revoca degli utenti (gli "**Utenti**"), nonché quelle di rilascio ed erogazione dei servizi InfoCert ("**Servizi Trust**"), ai sensi del Manuale Operativo;
- d) Il R.A.O. Supplier si è reso disponibile a svolgere le attività elencate al punto precedente e meglio dettagliate nel presente atto per il tramite dei propri Operatori di Registrazione, formalizzando l'apposito documento (il "**Mandato**");
- e) le procedure di registrazione sono analiticamente esposte nel Manuale Operativo di InfoCert sopra citato, pubblicato sul sito Internet "www.infocert.it", e nei provvedimenti legislativi e amministrativi eventualmente ivi richiamati.



TUTTO CIO' PREMESSO, le Parti convengono quanto segue:

1. PREMESSE

1.1. Le premesse, nonché il PDS e il Manuale Operativo Certificati e Manuale Operativo SPID disponibili sul sito InfoCert (<https://www.firma.infocert.it/documentazione/>), formano parte integrante del presente Mandato che sarà espletato secondo le specifiche condizioni ivi previste.

2. OGGETTO

2.1 InfoCert, la R.A. e il R.A.O. Supplier conferiscono mandato non esclusivo al R.A.O. a svolgere parte dell'attività di cui alla lett. c) delle premesse e, in particolare, gli obblighi previsti al successivo art. 3.1, esclusivamente attraverso sistemi autorizzati da InfoCert e secondo le modalità concordate da InfoCert e dalla R.A.

2.2 Per lo svolgimento delle attività previste nel presente Mandato, il R.A.O. Supplier si avvarrà di propri dipendenti e/o collaboratori e, in particolare e non in esclusiva, dell'Operatore di Registrazione che sottoscrive parimenti il presente Mandato.

3. OBBLIGHI DELLE PARTI

3.1. La RA, ferme rimanendo le obbligazioni di cui alla Convenzione, provvederà a:

- a) supervisionare, per conto di InfoCert, l'attività di formazione e/o aggiornamento dei R.A.O. Supplier;
- b) verificare che i destinatari della formazione rispettino i requisiti organizzativi necessari all'esercizio della suddetta attività, come da indicazioni di InfoCert;
- c) fornire i beni ed i materiali da consegnare agli Utenti.

3.2 Il R.A.O. Supplier, con la diligenza del mandatario ex art. 1710, c.c., dovrà:

- a) vigilare sui R.A.O., affinché questi svolgano le attività demandate ai sensi del precedente art. 2, nel rispetto del presente Mandato e della normativa vigente e, in particolare, affinché:
 - i. informino gli Utenti sulle modalità di utilizzo del Servizio, con particolare riferimento alle modalità di revoca, sospensione e rinnovo dello stesso nonché su aspetti normativi e conseguenze giuridiche derivanti dall'utilizzo dello stesso;
 - ii. interrompano l'attività di identificazione, qualora i documenti presentati dall'Utente o altre circostanze oggettive (es. scarsa qualità dell'audio e/o del video, in caso di identificazione a mezzo *webcam*), non consentano di formare il convincimento sull'identità del Richiedente;
- b) far conseguire ai propri R.A.O. la formazione necessaria per le finalità del presente Mandato;
- c) assumere gli obblighi descritti nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere già un'organizzazione di personale e di beni adeguata all'esercizio delle Attività;
- d) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust come prescritte nei Manuali Operativi;
- e) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert, qualora si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva notizia per iscritto ad InfoCert entro 24 (ventiquattro) ore lavorative;
- f) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi Trust;



- g) informare entro 12 (dodici) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione;
- h) consentire alle Autorità di vigilanza, nonché alle R.A. di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
- i) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
- j) sottoporre ai Richiedenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare preventivamente con quest'ultima qualsiasi documento da rilasciare all'Utente, relativamente all'attività di registrazione del Certificato e/o di rilascio dei Servizi Trust;
- k) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla Piattaforma;
- l) obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
- m) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione concordata con InfoCert, che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta;
- n) impedire ai R.A.O. la prosecuzione delle attività e ritirare ogni materiale a tal fine in uso, qualora, per qualsiasi causa, si interrompa il rapporto in essere e darne tempestivamente notizia per iscritto alla R.A. e a InfoCert;
- o) rispettare le istruzioni di cui al successivo art. 6, impartite ai sensi del Reg. (UE) 679/2016;
- p) se prevista la sospensione e/o cessazione del Ruolo, così come definito nel Manuale Operativo ICERT-INDI-MO, inviare ad InfoCert la comunicazione di revoca e/o sospensione del Servizio;

3.3. Il R.A.O. con la diligenza del mandatario ex art. 1710, c.c., dovrà:

- a) assumere gli obblighi descritti nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere già un'organizzazione di personale e di beni adeguata all'esercizio delle Attività;
- b) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust definite da InfoCert;
- c) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniqualvolta venga revocato il Mandato da InfoCert o dalla R.A., qualora si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva notizia per iscritto ad InfoCert;
- d) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi Trust;
- e) informare entro 8 (otto) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione;
- f) consentire alle Autorità di vigilanza, nonché agli incaricati di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
- g) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
- h) sottoporre agli Utenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare preventivamente con quest'ultima qualsiasi documento da rilasciare all'Utente, relativamente all'attività di registrazione e/o di rilascio dei Servizi Trust;



- i) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla piattaforma dedicata, propedeutica al caricamento e alla gestione di tutta la documentazione afferente al ciclo-vita della R.A. ("**Piattaforma**");
- j) obbligersi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
- k) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione richiesta da InfoCert (a titolo meramente esemplificativo e non esaustivo: mandati, modulistica dei Servizi Trust), che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta;
- l) impedire ai R.A.O. la prosecuzione delle attività e ritirare ogni materiale a tal fine in uso, qualora, per qualsiasi causa, si interrompa il rapporto in essere e darne tempestivamente notizia per iscritto alla R.A. e a InfoCert;
- m) rispettare le istruzioni di cui al successivo art. 6, impartite ai sensi del Reg. (UE) 679/2016;
- n) se prevista la sospensione e/o cessazione del Ruolo, così come definito nel Manuale Operativo ICERT-INDI-MO, inviare ad InfoCert la comunicazione di revoca e/o sospensione del Servizio;

3.4 La R.A., il R.A.O. Supplier e il R.A.O. saranno solidalmente responsabili nei confronti di InfoCert per le attività previste nel presente Mandato, anche per eventuali danni patiti dagli Utenti e/o da terzi, direttamente conseguenti a propri comportamenti e/o omissioni colpevoli nonché per i comportamenti e/o le omissioni colpevoli dei propri R.A.O., nell'espletamento degli obblighi nascenti dal presente Mandato e dalla normativa vigente, senza possibilità di esonero neanche parziale e anche in deroga all'art. 1717, c. 2, c.c.

3.5. La violazione di uno qualsiasi degli obblighi di cui al comma 3.2. del presente articolo costituirà giusta causa di revoca del presente Mandato da parte di InfoCert o della R.A., che sarà esercitata a mezzo di apposita comunicazione, fatto salvo il diritto al risarcimento dei danni eventualmente subiti e *subendi*. In caso di revoca, il R.A.O. Supplier è obbligato a cessare qualsiasi attività posta in essere in base al presente atto ed a restituire i materiali ricevuti al fine dell'espletamento dell'incarico.

4. CORRISPETTIVI E FORNITURA

4.1. Il R.A.O. Supplier ed il R.A.O. per lo svolgimento dell'attività prevista nel Mandato non potranno pretendere il pagamento di alcun corrispettivo da parte di InfoCert né vantare alcuna esclusiva nei suoi confronti.

4.2. L'esclusione di cui al precedente comma è altresì valida con riferimento ai mezzi necessari per l'esecuzione del Mandato e alle anticipazioni e spese sostenute dal mandatario.

5. DURATA E DECORRENZA

5.1. Il Mandato avrà efficacia per il periodo di un anno dalla data della sua sottoscrizione e si rinnoverà tacitamente per periodi annuali, salvo disdetta di una delle Parti, da comunicarsi per iscritto almeno 3 (tre) mesi prima della scadenza del periodo annuale, a mezzo Posta Elettronica Certificata o lettera raccomandata A/R. Il Mandato perderà automaticamente efficacia, in ogni caso di cessazione della Convenzione in essere tra InfoCert e l'R.A..

5.2. Durante il periodo di vigenza del Mandato, InfoCert avrà diritto, senza pagamento di alcun corrispettivo, di recedere da esso in qualsiasi momento, con comunicazione della volontà di esercitare tale diritto a mezzo Posta Elettronica Certificata o raccomandata A/R.

5.3. In caso di recesso e/o revoca, il R.A.O. Supplier ed il R.A.O. non potranno vantare alcuna richiesta nei confronti della R.A. e/o di InfoCert, neanche per eventuali danni subiti in conseguenza dello stesso.

5.4. Resta salvo tra le Parti che in caso di risoluzione del presente Mandato, la Convenzione rimane valida ed efficace tra InfoCert e la R.A. fino a naturale vigenza della stessa.



6. PRIVACY

6.1. La R.A. e il R.A.O. Supplier e il R.A.O. si impegnano alla piena osservanza, per quanto di rispettiva competenza, del dettato del Regolamento (UE) 679/2016 e della normativa italiana compatibile con lo stesso.

6.2. Nell'espletamento del mandato, il R.A.O. Supplier e il R.A.O. saranno autorizzati al trattamento dei dati per lo svolgimento delle sole attività oggetto del presente Mandato, sotto la diretta autorità della R.A. e InfoCert attenendosi alle istruzioni impartite da quest'ultima.

6.3. In particolare, il R.A.O. Supplier e il R.A.O. metteranno in atto le seguenti operazioni di trattamento:

- a) verifica del documento di identità dell'Utente, della relativa validità e della corrispondenza al soggetto richiedente;
- b) trascrizione o verifica (in base alle indicazioni fornite in sede di formazione) delle informazioni inerenti alla persona fisica dell'Utente;
- c) produzione della documentazione che attesta l'avvenuto riconoscimento dell'Utente;
- d) raccolta dei documenti firmati, se applicabile sulla base della procedura di identificazione messa in atto.

7. LEGGE APPLICABILE E FORO COMPETENTE

7.1. Il presente Mandato è soggetto alla legge italiana.

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

Luogo _____, data _____

InfoCert S.p.A.	Ufficio di Registrazione	R.A.O. Supplier	R.A.O.

Si intendono espressamente approvati ai sensi e per gli effetti degli artt. 1341 e 1342, c.c., i seguenti articoli: 3.2, 3.3. e 3.4. (obblighi e responsabilità delle Parti); 4 (Corrispettivi e fornitura); 5 (Durata e decorrenza).

(Ufficio di Registrazione)

(R.A.O. Supplier)

(R.A.O.)



**MANDATO TRILATERALE PER LO SVOLGIMENTO DI ATTIVITA' DA PARTE DEL R.A.O.
PER IL RILASCIO DI SERVIZI TRUST DI INFOCERT**

Tra

InfoCert S.p.A., con sede legale in Roma, Piazzale Flaminio 1/B, CF e P. IVA 07945211006, in persona dell'Amministratore Delegato e legale rapp.te *pro-tempore* dott. Danilo Cattaneo, società soggetta a direzione e coordinamento di Tinexta S.p.A. (di seguito "**InfoCert**")

e

XXXX, con sede in _____ n. _____, CF e P. IVA _____, in persona del legale rappresentante *pro tempore* _____ munito dei necessari poteri, come dichiara e garantisce (di seguito, anche "**Ufficio di Registrazione**" o "**R.A.**")

e

XXXX, residente in _____ n. _____, CF _____, (di seguito, "**Operatore dell'Ufficio di Registrazione**" o "**R.A.O.**")

PREMESSO CHE:

- a) L'Ufficio di Registrazione ed InfoCert, in data _____ hanno stipulato apposita convenzione (di seguito "**Convenzione**"), con la quale è stato conferito mandato alla prima di svolgere le funzioni di Ufficio di Registrazione, per il rilascio dei Certificati di firma, secondo quanto previsto dal Manuale Operativo ICERT-INDI-MO (di seguito il "**Manuale Operativo Certificati**") e/o per il rilascio dello SPID secondo quanto previsto dal Manuale Operativo ICERT-MO-SPID ("**Manuale Operativo SPID**");
- b) ai sensi della Convenzione, la R.A. ha facoltà di operare anche attraverso propri Operatori dell'Ufficio di Registrazione, che si impegneranno ad osservare gli obblighi meglio dettagliati nel prosieguo;
- c) con il presente atto, si desidera conferire all'Operatore dell'Ufficio di Registrazione apposito mandato per l'esecuzione delle attività di sua competenza ai sensi della Convenzione, concernenti le fasi identificazione, autenticazione, registrazione e revoca degli utenti (gli "**Utenti**"), nonché quelle di emissione, revoca e sospensione dei certificati e consegna del dispositivo ("**Servizi Trust**"), ai sensi del Manuale Operativo;
- d) l'Operatore dell'Ufficio di Registrazione si è reso disponibile a svolgere le attività elencate al punto precedente e meglio dettagliate nel presente atto (il "**Mandato**");
- e) le procedure di registrazione sono analiticamente esposte nel Manuale Operativo di InfoCert sopra citato, pubblicato sul sito Internet "www.infocert.it", e nei provvedimenti legislativi e amministrativi eventualmente ivi richiamati.

TUTTO CIO' PREMESSO, e Parti convengono quanto segue:

1. PREMESSE



1.1. Le premesse, nonché il PDS e il Manuale Operativo Certificati e Manuale Operativo SPID disponibili sul sito InfoCert (<https://www.firma.infocert.it/documentazione/>) formano parte integrante del presente Mandato che sarà espletato secondo le specifiche condizioni ivi previste.

2. OGGETTO

2.1. InfoCert e la R.A. conferiscono mandato non esclusivo all'Operatore dell'Ufficio di Registrazione a svolgere parte dell'attività di cui alla lett. c) delle premesse e, in particolare, a identificare gli Utenti con certezza, esclusivamente attraverso sistemi autorizzati da InfoCert e secondo le modalità concordate da InfoCert e dalla R.A.

3. OBBLIGHI DELLE PARTI

3.1. La R.A., ferme rimanendo le obbligazioni di cui alla Convenzione, provvederà a:

- a) supervisionare, per conto di InfoCert, l'attività di formazione e/o aggiornamento dei R.A.O.;
- b) verificare che gli Operatori dell'Ufficio di Registrazione eseguano con la dovuta diligenza le attività a loro assegnate;
- c) monitorare costantemente che gli Operatori dell'Ufficio di Registrazione mantengano i requisiti di competenza, affidabilità, onorabilità ed esperienza ai sensi dell'art. 24 par. 2 lett. b) del Regolamento eIDAS;
- d) assicurarsi che venga inibita la possibilità di utilizzo di ogni mezzo necessario per la prosecuzione delle Attività, ogniquale volta venga revocato il Mandato da InfoCert o dalla R.A., qualora cessi il rapporto di dipendenza/collaborazione tra l'Ufficio di Registrazione e il R.A.O., ovvero si manifesti il venir meno dei requisiti necessari per dar seguito ai Mandati (a titolo esemplificativo, venga revocato o compromesso il certificato del R.A.O.), dandone tempestiva comunicazione per iscritto ad InfoCert entro 24 (ventiquattro) ore lavorative;
- e) fornire i beni ed i materiali ai R.A.O. da consegnare agli Utenti.

3.2 L'Operatore dell'Ufficio di Registrazione, con la diligenza del mandatario ex art. 1710, c.c., dovrà:

- a) conseguire la formazione necessaria per le finalità del presente mandato, partecipando ai corsi di formazione come predisposti dal R.A. ai sensi dell'art. 3.1 lett. a);
- b) prendere visione delle istruzioni contenute nei Manuali Operativi, nell'ultima versione tempo per tempo disponibile online sul sito di InfoCert, e garantire di possedere e mantenere in essere requisiti di onorabilità e professionalità necessari all'esercizio delle Attività;
- c) rispettare le procedure operative di rinnovo, revoca o sospensione dei Servizi Trust definite da InfoCert;
- d) esercitare le Attività nell'interesse di InfoCert e con la diligenza del mandatario, ex art. 1710, c.c.;
- e) svolgere le Attività nel rispetto della normativa vigente, dei Manuali Operativi e delle istruzioni ricevute da InfoCert, con particolare riferimento all'identificazione personale certa degli Utenti che richiedono l'emissione dei Servizi Trust;
- f) informare entro 12 (dodici) ore InfoCert di eventuali vizi, difetti, interruzioni o malfunzionamenti del sistema e/o di errori nello svolgimento delle attività di identificazione e registrazione;
- g) consentire alle Autorità di vigilanza, nonché alle R.A. di InfoCert, di accedere nei propri locali per verificare il corretto espletamento delle Attività ed il rispetto delle procedure per lo svolgimento delle stesse;
- h) fornire evidenza, entro e non oltre 3 (tre) giorni dalla richiesta da parte di InfoCert, di tutta la documentazione relativa alle Attività, qualora la richiesta derivi dall'Autorità di vigilanza;
- i) sottoporre agli Utenti, siano esse persone fisiche o giuridiche che richiedono l'emissione dei Servizi Trust per conto dell'Utente, la documentazione contrattuale messa a disposizione da InfoCert, nonché concordare



preventivamente con quest'ultima qualsiasi documento da rilasciare al Richiedente e/o Utente, relativamente all'attività di registrazione del Certificato e/o di rilascio dei Servizi Trust;

- j) mantenere strettamente riservate le credenziali ricevute da InfoCert per l'accesso alla piattaforma dedicata, propedeutica al caricamento e alla gestione di tutta la documentazione afferente al ciclo-vita della R.A. ("**Piattaforma**");
- k) obbligarsi ad un corretto utilizzo della Piattaforma, nelle modalità indicate da InfoCert;
- l) provvedere ad un regolare caricamento/aggiornamento sulla Piattaforma di tutta la documentazione richiesta da InfoCert (a titolo meramente esemplificativo e non esaustivo: mandati, modulistica dei Servizi Trust), che dovrà essere fornita a quest'ultima entro i termini con essa convenuti, e in ogni caso qualora InfoCert ne faccia espressa richiesta.

3.3. L' Operatore dell'Ufficio di Registrazione e la R.A. saranno solidalmente responsabili nei confronti di InfoCert per le attività previste nel presente Mandato.

3.4. La violazione di uno qualsiasi degli obblighi di cui al comma 3.2. e 3.3 del presente articolo costituirà giusta causa di revoca del presente Mandato da parte di InfoCert o della R.A., che sarà esercitata a mezzo di apposita comunicazione, fatto salvo il diritto al risarcimento dei danni eventualmente subiti e *subendi*. In caso di revoca, l'Operatore dell'Ufficio di Registrazione è obbligato a cessare qualsiasi attività posta in essere in base al presente atto ed a restituire i materiali ricevuti al fine dell'espletamento dell'incarico.

4. CORRISPETTIVI E FORNITURA

4.1. L' Operatore dell'Ufficio di Registrazione e la R.A. per lo svolgimento dell'attività prevista nel Mandato non potranno pretendere il pagamento di alcun corrispettivo da parte di InfoCert né vantare alcuna esclusiva nei suoi confronti.

4.2. L'esclusione di cui al precedente comma è altresì valida con riferimento ai mezzi necessari per l'esecuzione del Mandato e alle anticipazioni e spese sostenute dal mandatario.

5. DURATA E DECORRENZA

5.1. Il Mandato avrà efficacia per il periodo di un anno dalla data della sua sottoscrizione e si rinnoverà tacitamente per periodi annuali, salvo disdetta di una delle Parti, da comunicarsi per iscritto almeno 3 (tre) mesi prima della scadenza del periodo annuale, a mezzo Posta Elettronica Certificata o lettera raccomandata A/R. Il Mandato perderà automaticamente efficacia, in ogni caso di cessazione della Convenzione in essere tra InfoCert e la R.A..

5.2. Durante il periodo di vigenza del Mandato, InfoCert avrà diritto, senza pagamento di alcun corrispettivo, di recedere da esso in qualsiasi momento, con comunicazione della volontà di esercitare tale diritto a mezzo Posta Elettronica Certificata o raccomandata A/R.

5.3. In caso di recesso e/o revoca, l'Operatore dell'Ufficio di Registrazione non potrà vantare alcuna richiesta nei confronti della R.A. e/o di InfoCert, neanche per eventuali danni subiti in conseguenza dello stesso.

5.4. Resta salvo tra le Parti che in caso di risoluzione del presente Mandato, la Convenzione rimane valida ed efficace tra InfoCert e la R.A. fino a naturale vigenza della stessa.

6. PRIVACY

6.1. La R.A. e l'Operatore dell'Ufficio di Registrazione si impegnano alla piena osservanza, per quanto di rispettiva competenza, del dettato del Regolamento (UE) 679/2016 e della normativa italiana compatibile con lo stesso.



6.2. Nell'espletamento del mandato, l'Operatore dell'Ufficio di Registrazione sarà autorizzato al trattamento dei dati per lo svolgimento delle sole attività oggetto del presente Mandato, sotto la diretta autorità della R.A. e InfoCert attenendosi alle istruzioni impartite da quest'ultima.

6.3. In particolare, l'Operatore dell'Ufficio di Registrazione metterà in atto le seguenti operazioni di trattamento:

- a) verifica del documento di identità del richiedente, della relativa validità e della corrispondenza al soggetto richiedente;
- b) trascrizione o verifica (in base alle indicazioni fornite in sede di formazione) delle informazioni inerenti alla persona fisica del richiedente;
- c) produzione della documentazione che attesta l'avvenuto riconoscimento dell'Utente;
- d) raccolta dei documenti firmati, se applicabile sulla base della procedura di identificazione messa in atto.

7. LEGGE APPLICABILE E FORO COMPETENTE

7.1. Il presente Mandato è soggetto alla legge italiana.

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

Luogo _____, data _____

InfoCert S.p.A.	Ufficio di Registrazione	Operatore dell'Ufficio di Registrazione
_____	_____	_____

Si intendono espressamente approvati ai sensi e per gli effetti degli artt. 1341 e 1342, c.c., i seguenti articoli: 3 (Obblighi delle Parti); 4 (Corrispettivi e fornitura); 5 (Durata e decorrenza).

(Ufficio di Registrazione)

(Operatore dell'Ufficio di Registrazione)

tinexta
infocert

Requisiti di compliance

Registration Authority

1 INTRODUZIONE

SCOPO

I Clienti che svolgono l'attività di Registration Authority per conto di InfoCert, eventualmente anche integrando i loro servizi con componenti applicative, devono rispettare, nell'erogazione del servizio oggetto dell'Accordo, i seguenti principi e criteri, necessari a garantire una adeguata compliance alla normativa relativa ai servizi fiduciari:

- sicurezza informatica;
- erogazione dei servizi IT;
- qualità del servizio;
- requisiti ambientali;
- requisiti per la fornitura.

RIFERIMENTI

- ISO/IEC 27001 - Sistema di gestione sulla Sicurezza delle informazioni
- ISO 20000-1 - Requisiti sistema di gestione dei servizi IT
- ISO 9001 - Sistemi di gestione qualità
- ISO 14001 - Sistemi di gestione ambientale
- ETSI EN 319 401 – Policy di requisiti generali per i Fornitori di servizi fiduciari

2 REQUISITI

Sono qui di seguito delineati i **Requisiti** ai quali la Registration Authority deve garantire di essere conforme, al fine di rispettare i principi e criteri di compliance di cui alla normativa dei servizi fiduciari.

MISURE ORGANIZZATIVE

La Registration Authority deve:

- garantire, nell'erogazione del servizio contrattualizzato, personale, adeguatamente informato e formato sui requisiti minimi in ambito di information security. La Registration Authority deve anche conservare appropriate informazioni documentate quale evidenza delle competenze e della formazione effettuate sui temi di cui sopra;
- garantire che le figure degli Operatori dell'Ufficio di Registrazione (RAO) ovvero dei Master RAO abbiano compreso loro mansioni e responsabilità, siano costantemente aggiornati sulle stesse e che abbiano frequentato e concluso un corso adeguato nei processi di erogazione dei servizi fiduciari che li riguardano;
- definire e rispettare una procedura per la gestione, la protezione ed il monitoraggio degli accessi fisici agli spazi aziendali della Registration Authority, che consideri anche i locali adibiti alla conservazione delle informazioni correlate al servizio erogato (archivi cartacei, etc);
- definire le responsabilità in merito alla protezione dei dati personali all'interno dell'azienda, in coerenza con quanto sottoscritto in termini di Accordo e/o mandato con InfoCert;
- garantire conformità ai requisiti legislativi applicabili per la tutela della privacy: informative, trattamenti, cancellazione dati, gestione data breach, valutazione d'impatto, protezione dei dati memorizzati, protezione dei dati trasmessi, cancellazione sicura dei dati e modalità di conservazione dei dati personali, ecc;
- definire le proprie politiche/regolamenti relativi alla sicurezza informatica, garantendo che siano applicate all'interno di tutta l'Azienda;
- prevedere l'inserimento di analoghi requisiti di sicurezza, riservatezza, privacy nei contratti con gli eventuali sub-fornitori, qualora preventivamente autorizzati da InfoCert;
- garantire il monitoraggio della sicurezza informatica degli eventuali sub- fornitori con potenziale impatto sui servizi oggetto dell'Accordo e che possano pertanto pregiudicare gli SLA concordati;
- verificare le misure di sicurezza delle informazioni adottate da eventuali terze parti fornitrici di servizi cloud computing coinvolte nelle attività contrattualizzate e comunicarle ad InfoCert;
- comunicare un processo di gestione degli incidenti di sicurezza delle informazioni e, in caso di incidente significativo, garantirne la comunicazione ad InfoCert entro 8 ore

dall'avvenuta conoscenza dell'evento (si veda capitolo specifico "Comunicazione incidente di sicurezza informatica significativo");

- garantire la disponibilità alle attività di monitoraggio, annuale o ad evento significativo, dei requisiti suddetti da parte del Committente attraverso la somministrazione di questionari;
- garantire un processo di gestione delle emergenze per la sicurezza nei luoghi di lavoro;
- rispettare le normative vigenti in ambito ambientale applicabili all'oggetto della fornitura.

MISURE TECNOLOGICHE

La Registration Authority deve:

- definire e descrivere una modalità di utilizzo delle risorse informatiche aziendali condivisa all'interno dell'organizzazione sia per i dipendenti che per i collaboratori e che comprenda almeno:
 - una policy di generazione ed utilizzo delle password di dominio;
 - modalità di protezione degli endpoint aziendali (password del BIOS, cifratura disco, piattaforma MDM, etc);
 - l'utilizzo in tutte le postazioni di software antivirus/anti malware;
 - obblighi e limitazioni d'uso dei dispositivi informatici;
 - una procedura di gestione degli aggiornamenti software;
 - le tecniche di sicurezza implementate nei casi di utilizzo di reti wireless;
 - misure di sicurezza adottate nei casi di lavoro da remoto (es.VPN, crittografia delle comunicazioni, etc);
- garantire che le password di accesso ai sistemi e alle applicazioni utilizzate nell'erogazione della fornitura, siano univoche, personali, "forti" e non memorizzate su supporti logici/fisici.

Di seguito alcuni esempi di buone pratiche nella creazione di password:

- Almeno 1 lettera minuscola
- Almeno 1 lettera maiuscola
- Almeno 1 numero
- Almeno 1 carattere speciale
- Non deve contenere uno dei seguenti pattern = qwerty, asdf , 1234
- Lunghezza di almeno 8 caratteri
- Non è una parola di una qualunque lingua, dialetto o linguaggio specialistico
- Non si basa su informazioni personali.

Tali password dovranno essere gestite utilizzando esclusivamente un sistema di password manager;

- garantire di aver definito ed attuato un processo per l'assegnazione e la revoca dei diritti di accesso e delle abilitazioni degli operatori preposti. Deve essere verificato che l'accesso alle workstation da parte degli operatori preposti avvenga esclusivamente

tramite le credenziali personali;

- garantire che eventuali sistemi informativi coinvolti nei processi oggetto dell'Accordo siano stati periodicamente analizzati e scansionati al fine di individuare e risolvere eventuali vulnerabilità tecniche (almeno annualmente).

Le attività di remediation devono rispettare le seguenti tempistiche: Oday/Early Warning 5gg, Critical/High 30 gg, Medium 90 gg, Low 120 gg, considerando come riferimento il risk score CVSS (Common Vulnerability Scoring System). Queste tempistiche devono essere rispettate anche nei casi di remediation chieste da InfoCert;

- garantire un flusso autorizzativo degli accessi logici ai sistemi ed alle applicazioni per gli utenti. Inoltre, la Registration Authority deve garantire un processo di gestione e monitoraggio degli amministratori di sistema;
- definire le misure di sicurezza informatica adottate per proteggere la rete (DMZ, firewall, etc.);
- garantire che le connessioni di rete siano sicure e protette con adeguate tecnologie di crittografia;
- assicurare che le informazioni ed i sistemi informativi siano protetti contro malware/antispam;
- garantire, nei casi di utilizzo di dispositivi fisici (smart card o business key) per il rilascio di certificati di firma, un processo di:
 - ✓ conservazione sicura di tali dispositivi (es. magazzino con protezioni antiallagamento, anti-danneggiamento, antincendio, etc);
 - ✓ gestione di un inventario di tali asset;
 - ✓ definizione di una lista di utenti autorizzati all'utilizzo e gestione di tali asset;
 - ✓ consegna ai clienti finali di tali asset;
 - ✓ gestione e smaltimento dei dispositivi obsoleti, che comprenda la definizione delle attività di utilizzo, conservazione e gestione dell'obsolescenza.

Inoltre, nei casi in cui la Registration Authority (RA), per la sua attività nel processo di erogazione di servizi fiduciari, utilizzi software o parti di esso sviluppati internamente, si aggiungono i seguenti requisiti:

- se sono presenti servizi di web running gestiti dalla RA, devono essere garantite misure di ridondanza dell'impianto di alimentazione elettrica (eventuali UPS, sistemi generazioni di emergenza, etc) e di sistemi di sicurezza fisica ove siano gestiti i dati (sistemi antincendio, sistemi videosorveglianza, etc);
- definire un processo di gestione delle richieste di change, incluse le proposte per aggiungere, rimuovere o trasferire servizi, che ne preveda la registrazione e la classificazione, l'approvazione formale, la verifica ed i test preliminari al rilascio della change stessa.

Nei casi di change richieste da InfoCert, la Registration Authority deve garantire l'applicazione delle stesse nei tempi richiesti dalla Committente.

Inoltre, prevedere una tempestiva comunicazione ad InfoCert nei casi di modifiche che

impattano la sicurezza dei sistemi applicativi utilizzati nell'erogazione del servizio contrattualizzato;

- definire e rispettare un processo di sviluppo sicuro del software che preveda dei test periodici di sicurezza e la formazione degli sviluppatori coinvolti;
- garantire che gli ambienti di sviluppo, collaudo e produzione siano segregati logicamente;
- gestire le fasi di release e deploy nel rispetto dei principi dello sviluppo sicuro che garantisca ad esempio:
 - ✓ la definizione dei requisiti di sicurezza in fase progettuale,
 - ✓ i requisiti di sicurezza devono garantire l'integrità, la riservatezza e la disponibilità dei dati gestiti dall'applicazione, tramite l'applicazione dei criteri di Software Development Life Cycle (SDLC),
 - ✓ la valutazione dei rischi emergente dalla combinazione tra la classificazione dei dati, trattati, gli eventuali impatti in tema di Data Protection e l'ambito di utilizzo,
 - ✓ l'assicurazione dell'integrità dei dati "at rest", "in transit" ed "end-to-end",
 - ✓ gli ambienti di sviluppo, test e produzione devono essere separati,
 - ✓ scansioni statiche del codice,
 - ✓ devono essere definite e documentate le modalità per tenere traccia del ciclo di vita dei dati personali (dalla raccolta alla conservazione, fino alla distruzione),
 - ✓ i cambiamenti ai sistemi all'interno del ciclo di vita devono essere tenuti sotto controllo attraverso l'utilizzo di procedure formali di controllo dei cambiamenti,
 - ✓ il prodotto/servizio non deve contenere vulnerabilità note
 - ✓ durante lo sviluppo devono essere effettuati test relativi alle funzionalità di sicurezza del prodotto/servizio.
- definire e rispettare una procedura per la gestione della configurazione;
- definire e rispettare un processo di gestione delle vulnerabilità infrastrutturali e delle applicazioni (coinvolte nell'oggetto della fornitura) che preveda sia delle scansioni periodiche, almeno annuali, che delle attività di remediation a valle di vulnerabilità riscontrate o degli aggiornamenti software.

Le attività di remediation devono rispettare le seguenti tempistiche: Oday/Early Warning 5gg, Critical/High 30 gg, Medium 90 gg, Low 120 gg, considerando come riferimento il risk score CVSS (Common Vulnerability Scoring System). Queste tempistiche devono essere rispettate anche nei casi di remediation chieste da InfoCert;
- definire ed attuare un processo di risk management relativo alla sicurezza delle informazioni aziendali;
- definire e rispettare un processo di backup delle informazioni, che descriva metodi, retention, strumenti;
- monitorare il livello di conformità alla gestione della sicurezza delle informazioni.

COMUNICAZIONE INCIDENTE DI SICUREZZA INFORMATICA SIGNIFICATIVO

Gli incidenti di sicurezza, per tali intendendo qualsivoglia evento o insieme di eventi che sottintendono una violazione o anche solo la minaccia di violazione delle politiche di sicurezza ICT e per la quale si renda necessaria l'applicazione di misure di contrasto e/o contenimento da parte delle strutture preposte, possono essere di varia natura e con vari livelli di criticità associati.

Secondo la definizione della Direttiva (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022 (NIS2) un incidente è considerato significativo se:

- ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
- si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

L'identificazione di quali di essi possano essere identificati come significativi è lasciata alla discrezionalità del caso specifico, ma di seguito viene fornita una lista, non esaustiva, dei casi in cui un incidente è da ritenersi significativo e pertanto soggetto alla gestione descritta nel presente paragrafo:

- eventi che impattano negativamente sulle risorse infrastrutturali critiche o sui dati in esse contenuti;
- incidenti che impattano un elevato numero di clienti;
- incidenti che coinvolgono dati personali e/o sensibili e che potrebbero richiedere la notifica verso il garante e/o il cliente, come previsto dal GDPR;
- incidenti che diventano di pubblico dominio attraverso i media;
- incidenti che violino le normative e/o le leggi che regolano i servizi forniti da InfoCert;
- incidenti che potrebbero avere un impatto negativo sulla reputazione di InfoCert;
- tipologie di incidenti comprese negli adempimenti normativi InfoCert.

In caso di incidente di sicurezza significativo relativo al servizio contrattualizzato, la Registration Authority dovrà seguire la seguente procedura:

- Prima comunicazione ad InfoCert alla casella di posta cyber.security@infocert.it
 - ✓ SLA: in mancanza di specifica contrattuale, entro 8 ore dalla verifica dell'incidente
 - ✓ Oggetto della comunicazione: Segnalazione Incidente di Sicurezza
 - ✓ Corpo della comunicazione: Descrizione dell'evento
- Report Incident da inviare ad InfoCert contenente
 - ✓ SLA: in mancanza di specifica contrattuale, entro 5 giorni lavorativi dalla verifica dell'incidente
 - ✓ Oggetto della comunicazione: Report Incident di Sicurezza
 - ✓ Allegato della comunicazione: Report Incident con il contenuto relativo al seguente sommario:
 - Template Verbale Incident di sicurezza
 - 1.1 Novità introdotte rispetto alla precedente emissione

- 1.2 Scopo e campo di applicazione del documento
- 1.3 Termini e definizioni
- 2 Servizi cui il verbale si riferisce
- 3 Descrizione dell'incidente
- 4 Analisi delle cause dell'evento
- 5 Azioni completate/in corso per ridurre la probabilità del ripetersi dell'evento e mitigare gli impatti
- 6 Appendice – Estrazione log.