Allegato 1
(articolo 11, comma 3, del regolamento di attuazione)

Allegato tecnico al regolamento attuativo

Indice dei contenuti

1. Introduzione

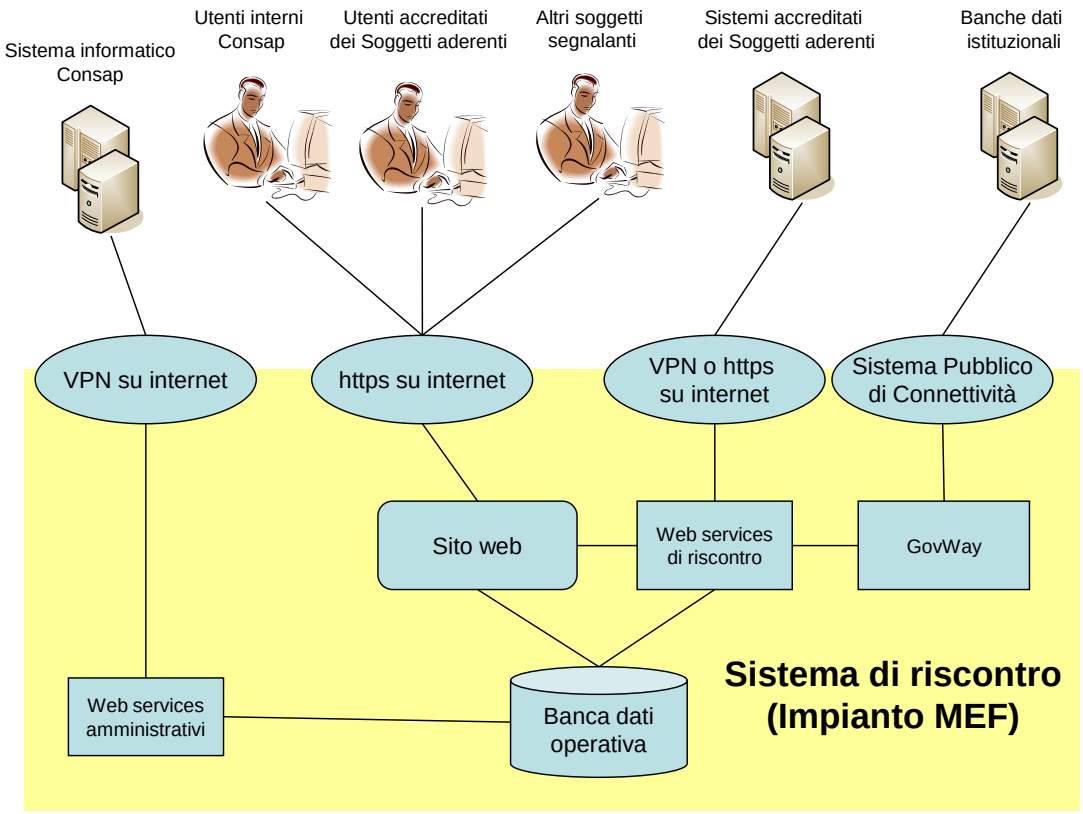
Questo documento descrive in particolare:
- le modalità di collegamento informatico del sistema alle banche dati degli organismi pubblici;
- le modalità di collegamento informatico al sistema da parte degli aderenti diretti, degli aderenti indiretti e dei soggetti autorizzati;
- le procedure di gestione del servizio telefonico e telematico di cui all'articolo 30-*ter*, comma 8, del decreto legislativo n. 141/2010;
- i processi di gestione delle credenziali di accesso al sistema;
- il tracciamento delle operazioni eseguite con il sistema;
- i profili di autorizzazione al riscontro delle diverse tipologie di dati da parte delle diverse tipologie di aderente/soggetto autorizzato.

È previsto che l'Archivio sia costituito da tre moduli funzionali:
- il modulo *Interconnessione di rete*, che riceverà le richieste di verifica provenienti dagli aderenti, le tradurrà in richieste di accesso alle banche dati pubbliche ospitanti i dati autentici da riscontrare e restituirà l'esito, positivo o negativo, della verifica effettuata;
- il modulo *Informatico di allerta*, che raccoglierà le segnalazioni di frodi subite o di rischio di frode provenienti dagli aderenti e le segnalazioni di allerta preventive generate dal sistema;
- il modulo *Informatico centralizzato*, che memorizza, in modo aggregato e anonimo, i casi il cui riscontro ha evidenziato la non autenticità di una o più categorie di dati presenti nelle richieste di verifica inviate dagli aderenti e dai soggetti autorizzati e permette al gruppo di lavoro lo studio del fenomeno delle frodi.

Le modalità d'uso del servizio di riscontro da parte degli aderenti e dei soggetti autorizzati sono diversificate, in quanto si prevede sia uno scenario d'uso allo sportello con il cliente di fronte all'operatore, sia uno scenario d'uso di *back office*, sia uno scenario d'uso che prevede elaborazioni massive di tipo *batch*.

2. L'architettura generale del sistema

La figura seguente mostra l'architettura generale prevista del sistema.



È costituito presso il CED del Ministero dell'economia e delle finanze un sistema informatico altamente scalabile e pienamente ridondato destinato a erogare il servizio operativo di riscontro di dati personali richiesto dai soggetti aderenti e dai soggetti autorizzati interfacciando una molteplicità di banche dati istituzionali (Agenzia delle Entrate, Ministero dell'Interno, Ministero delle Infrastrutture e dei Trasporti, Ministero dell'Economia e delle Finanze, Ministero del Lavoro e delle Politiche Sociali, INPS e INAIL).
Il sistema permetterà inoltre il ricevimento e la registrazione delle segnalazioni dei soggetti che hanno subito frodi configuranti ipotesi di furto di identità.
Il sistema di riscontro dialoga con il sistema informatico Consap, presso la quale è svolta la gestione amministrativa delle convenzioni con gli aderenti e con i soggetti autorizzati, la gestione delle utenze e la gestione del ciclo di calcolo dei consumi, di rendicontazione e di pagamento associato all'attuazione delle convenzioni stesse.

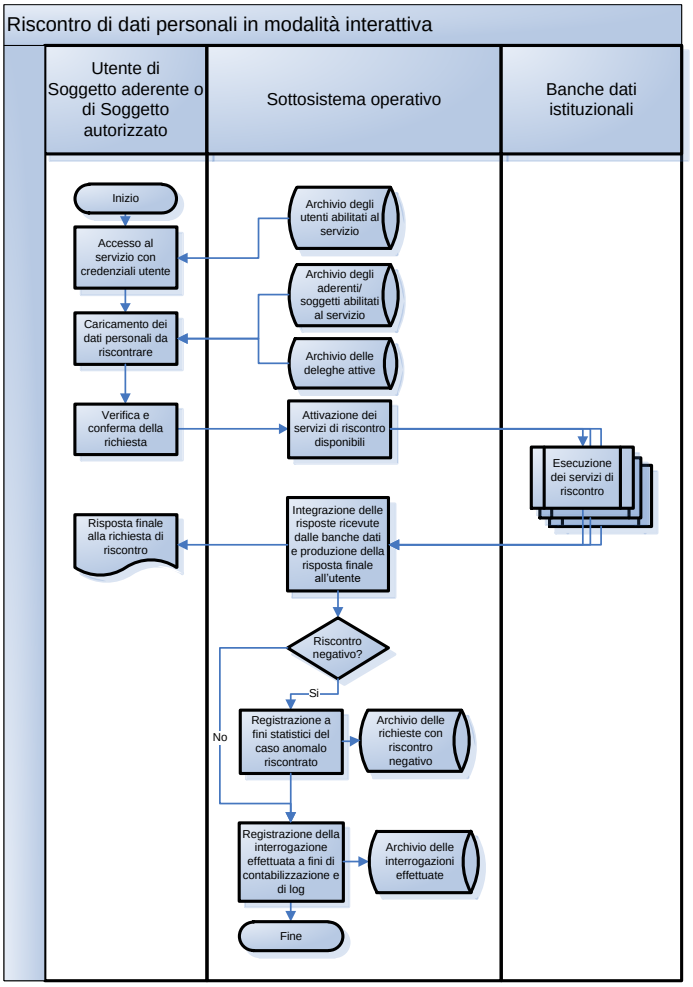
3. Descrizione dei processi operativi di riferimento

Nei paragrafi che seguono sono illustrati i processi operativi per i quali è previsto il supporto da parte del software del sistema di riscontro.

3.1. Riscontro dei dati

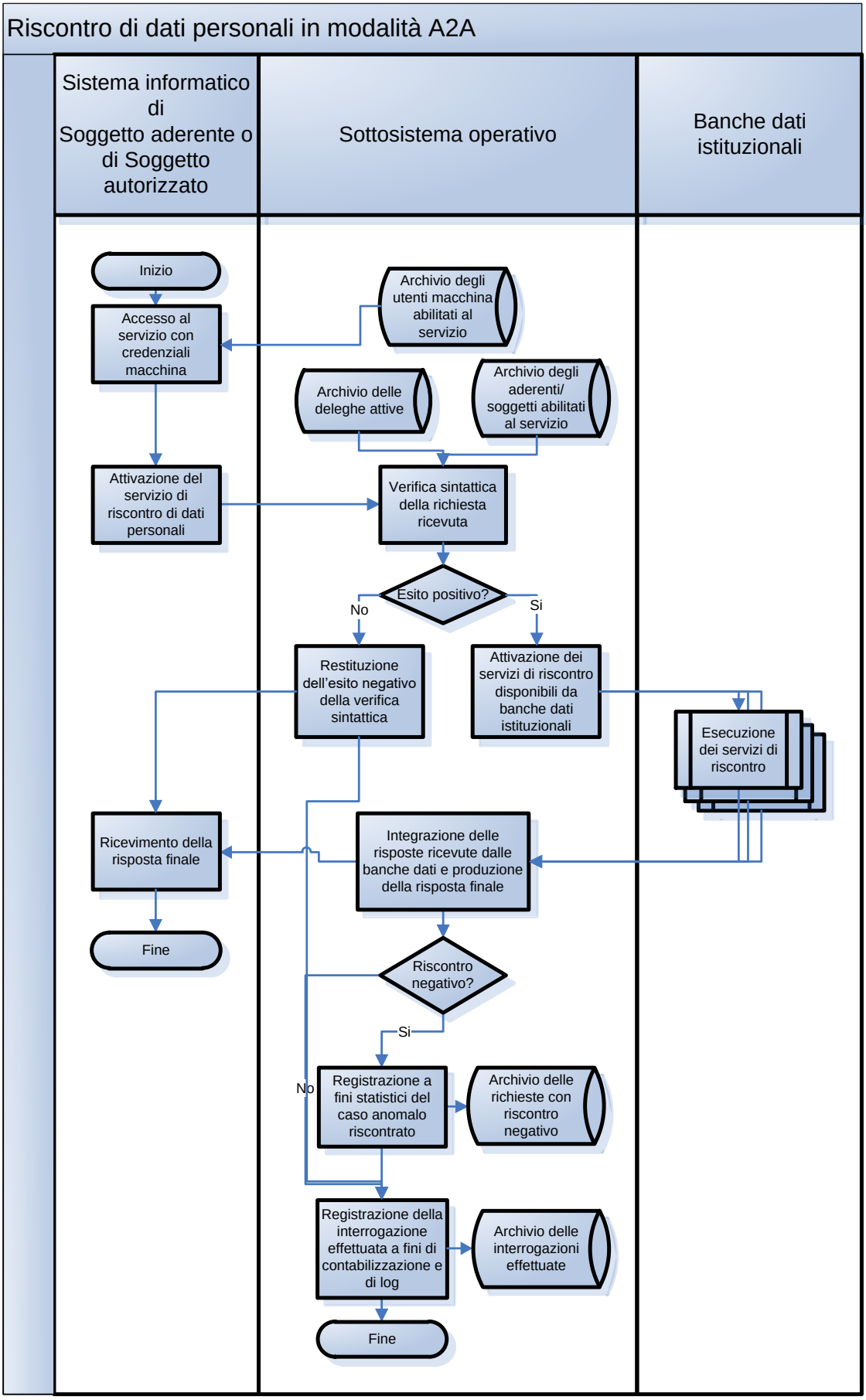
Si evidenzia che la procedura di riscontro, operata secondo le tre modalità descritte nei paragrafi seguenti, è strutturata in maniera tale da non richiedere la registrazione dei dati personali nell'archivio (ad eccezione del codice fiscale della persona fisica oggetto della verifica, che viene conservato in forma cifrata ai soli fini meglio descritti nel par. 6), ma soltanto la loro veicolazione informatica al fine di verificarne l'autenticità.

3.1.1. Riscontro dei dati in modalità interattiva



- L'utente abilitato del soggetto aderente o del soggetto autorizzato entra nel sistema usando le proprie credenziali, seleziona eventualmente l'aderente delegante (che può coincidere con l'aderente di riferimento dell'utente) per il quale effettuare l'interrogazione, fornisce i dati da riscontrare su maschera *on line*, ne verifica l'esattezza e attiva il servizio di riscontro;
- il sistema, in base alla richiesta ricevuta, attiva i servizi di riscontro messi a disposizione dalle banche dati istituzionali collegate trasmettendo ad esse, ognuna per la propria competenza, i dati forniti dall'utente, raccoglie gli esiti di riscontro – di natura essenzialmente *semaforica* - ricevuti dalle banche dati e li restituisce all'utente;
- il sistema di riscontro registra i dati identificativi dell'interrogazione effettuata (identificativo dell'utente e dell'organizzazione interrogante, momento dell'interrogazione, tipi di campi oggetto del riscontro, esiti semaforici sul riscontro restituiti dalle banche dati interrogate), a fini amministrativi e di tracciamento;
- nei soli casi in cui il riscontro dei dati abbia dato esito negativo, il sistema registra i dati della richiesta di riscontro e gli esiti semaforici corrispondenti nell'archivio delle richieste di riscontro con esito negativo;
- per tutti i casi di riscontro effettuati dagli aderenti, il sistema registra i dati della richiesta di riscontro e gli esiti semaforici corrispondenti nell'archivio delle richieste di riscontro per i 2 giorni lavorativi successivi al riscontro stesso, al fine di consentirne eventualmente la conversione in rischio di frode da parte dell'aderente stesso, dopodiché i dati personali della richiesta di riscontro vengono cancellati.

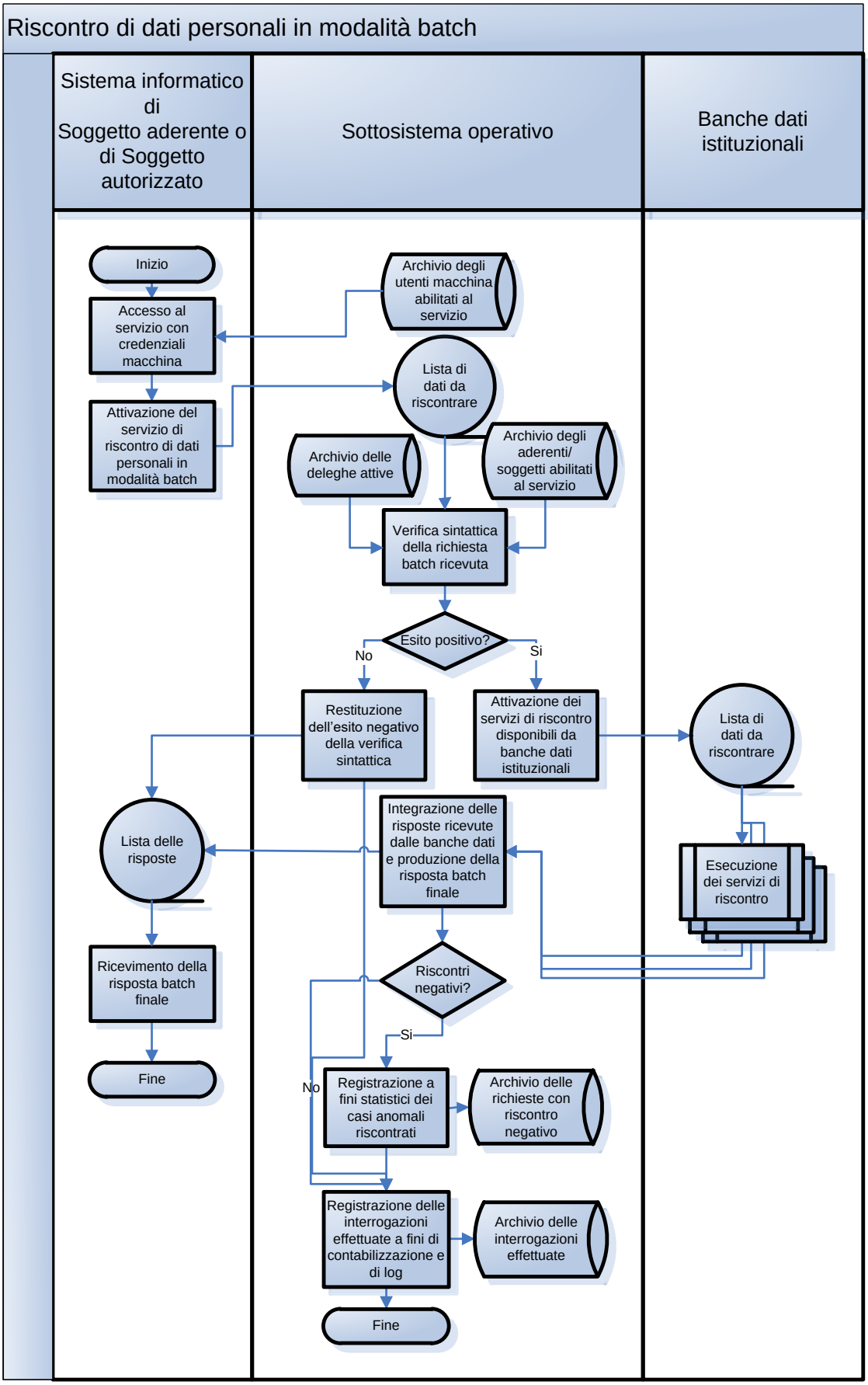
3.1.2. Riscontro dei dati in modalità *application* to *application* - A2A



- Il sistema informatico abilitato del soggetto aderente o del soggetto autorizzato invoca il servizio di riscontro usando le proprie credenziali macchina;

- il sistema verifica la correttezza sintattica della richiesta e dei riferimenti forniti nella richiesta all'aderente diretto, all'aderente indiretto e al soggetto autorizzato, in base alle deleghe registrate come attive nel sistema stesso. Se la verifica sintattica ha esito positivo, attiva i servizi di riscontro messi a disposizione dalle banche dati istituzionali collegate trasmettendo ad esse, ognuna per la propria competenza, i dati forniti dal sistema chiamante, raccoglie gli esiti di riscontro – di natura essenzialmente *semaforica* - ricevuti dalle banche dati, li integra e li restituisce al sistema informatico chiamante; se la verifica sintattica ha invece esito negativo, restituisce al sistema informatico chiamante l'esito negativo con la motivazione;
- il sistema registra i dati identificativi dell'interrogazione effettuata (identificativo dell'utente associato alle credenziali macchina del sistema chiamante e dell'organizzazione interrogante, momento dell'interrogazione, tipi di campi oggetto del riscontro, esiti semaforici sul riscontro restituiti dalle banche dati interrogate), a fini amministrativi e di tracciamento;
- nei soli casi in cui il riscontro dei dati ha dato esito negativo, il sistema registra i dati della richiesta di riscontro e gli esiti semaforici corrispondenti nell'archivio delle richieste di riscontro con esito negativo;
- per tutti i casi di riscontro effettuati dagli aderenti, il sistema registra i dati della richiesta di riscontro e gli esiti semaforici corrispondenti nell'archivio delle richieste di riscontro per i 2 giorni lavorativi successivi al riscontro stesso, al fine di consentirne eventualmente la conversione in rischio di frode da parte dell'aderente stesso, dopodiché i dati personali della richiesta di riscontro vengono cancellati.

3.1.3. Riscontro dei dati in modalità batch

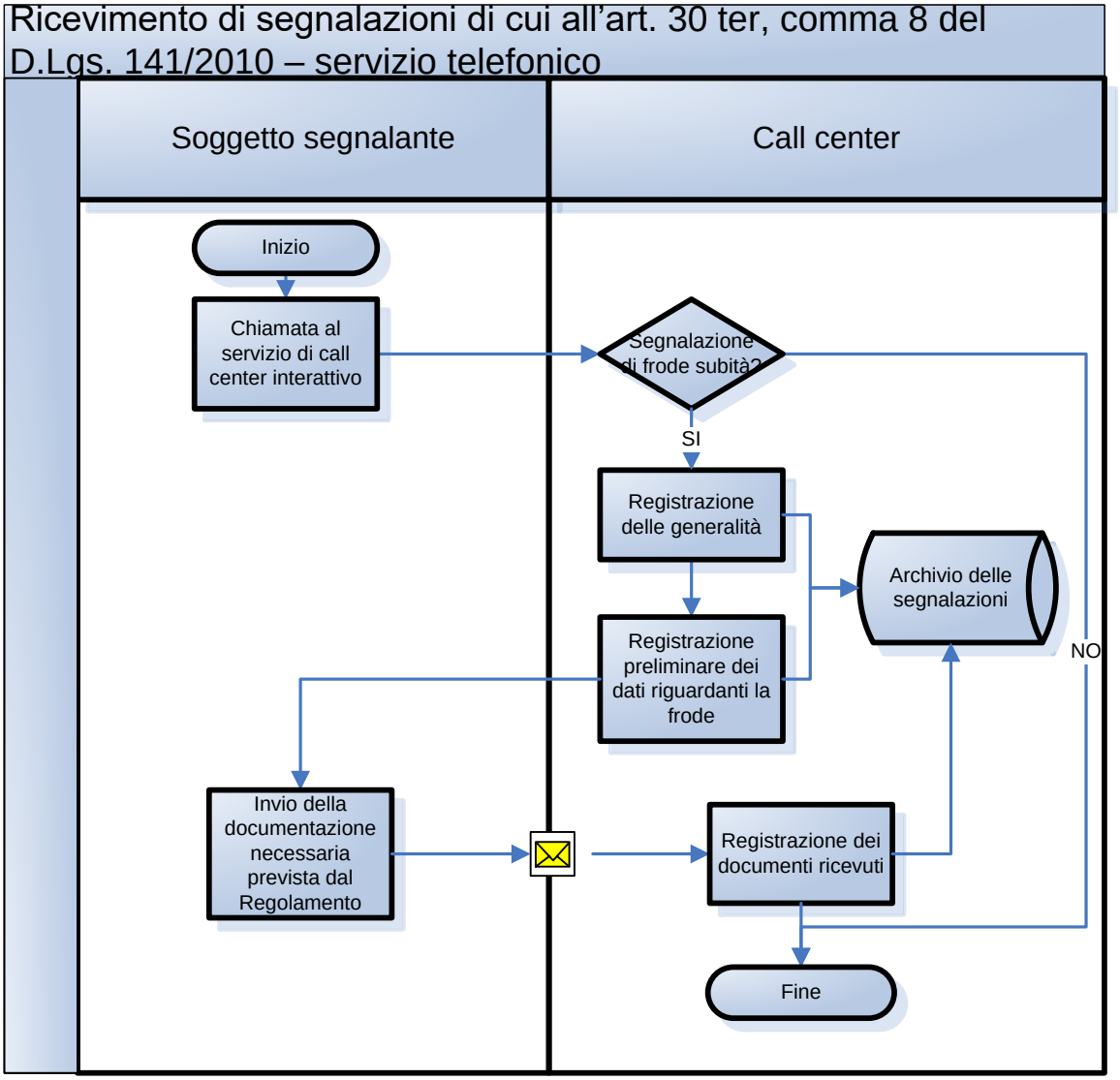


Il processo previsto differisce da quello precedente in quanto permette l'elaborazione massiva di più richieste di riscontro provenienti dal sistema informatico di un soggetto aderente o di un soggetto autorizzato. Il processo è il seguente:

- il sistema informatico abilitato del soggetto aderente o del soggetto autorizzato prepara la lista delle richieste di riscontro e invoca il servizio di riscontro massivo usando le proprie credenziali macchina;
- il sistema verifica la correttezza sintattica della lista di richieste ricevute e dei riferimenti forniti nella richiesta all'aderente diretto, all'aderente indiretto e al soggetto autorizzato, in base alle deleghe registrate come attive nel sistema al momento in cui la richiesta è stata inoltrata dall'aderente. Per ogni richiesta sintatticamente corretta, attiva i servizi di riscontro messi a disposizione dalle banche dati istituzionali collegate trasmettendo ad esse, ognuna per la propria competenza, i dati forniti dal sistema chiamante, raccoglie gli esiti di riscontro – di natura essenzialmente *semaforica* - ricevuti dalle banche dati, li integra, confeziona la risposta finale da restituire al sistema informatico chiamante; per ogni richiesta sintatticamente non corretta, confeziona un esito negativo con la motivazione;
- il sistema di riscontro restituisce al sistema informatico chiamante la lista degli esiti delle verifiche effettuate;
- il sistema di riscontro registra i dati identificativi dell'interrogazione effettuata (identificativo dell'utente associato alle credenziali macchina del sistema chiamante e dell'organizzazione interrogante, momento dell'interrogazione, tipi di campi oggetto del riscontro, esiti semaforici sul riscontro restituiti dalle banche dati interrogate), a fini amministrativi e di tracciamento;
- nei soli casi in cui il riscontro dei dati ha dato esito negativo, il sistema registra i dati della richiesta e gli esiti semaforici corrispondenti nell'archivio delle richieste di riscontro con esito negativo;
- per tutti i casi di riscontro effettuati dagli aderenti, il sistema registra i dati della richiesta di riscontro e gli esiti semaforici corrispondenti nell'archivio delle richieste di riscontro per i 2 giorni lavorativi successivi al riscontro stesso, al fine di consentirne eventualmente la conversione in rischio di frode da parte dell'aderente stesso, dopodiché i dati personali della richiesta di riscontro vengono cancellati.

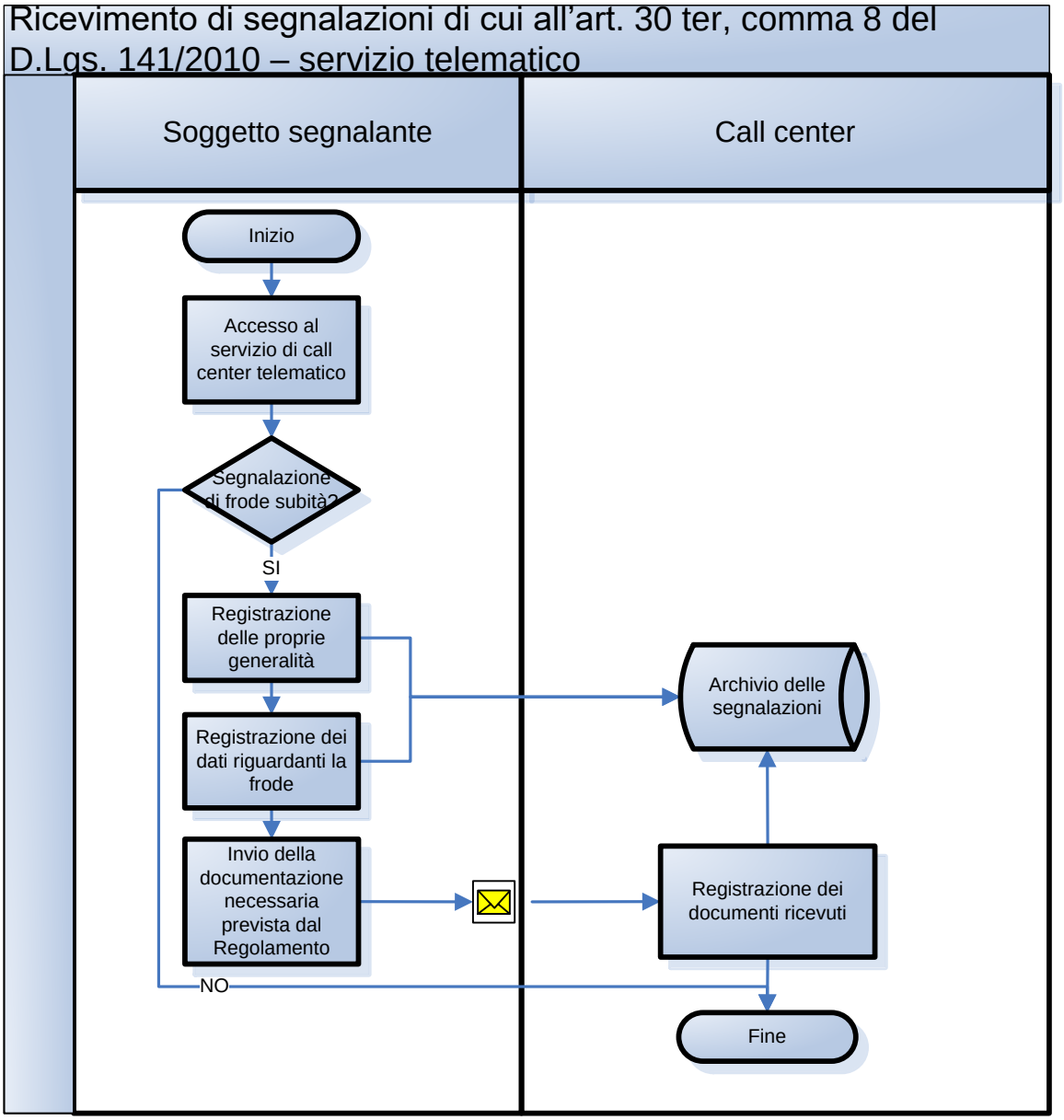
3.2. Servizi telefonici e telematici

3.2.1. Servizio telefonico



- Il soggetto segnalante chiama il call center telefonico dedicato al servizio di ricevimento di segnalazioni di cui all'art. 30 ter, comma 8, del D.lgs. n. 141/2010;
- Il servizio di call center, interagendo con il soggetto segnalante, individua se trattasi di frode subita o di rischio di frode;
- Nel caso di segnalazione di frode subita, il servizio di call center raccoglie le generalità del segnalante e i dati relativi alla frode subita, chiedendo di inviare copia dei documenti previsti dall'articolo 22, comma 22, del regolamento di attuazione per la successiva registrazione nell'archivio;
- Nel caso di segnalazione di rischio di frode, la stessa non viene registrata nell'archivio.

3.2.2. Servizio telematico



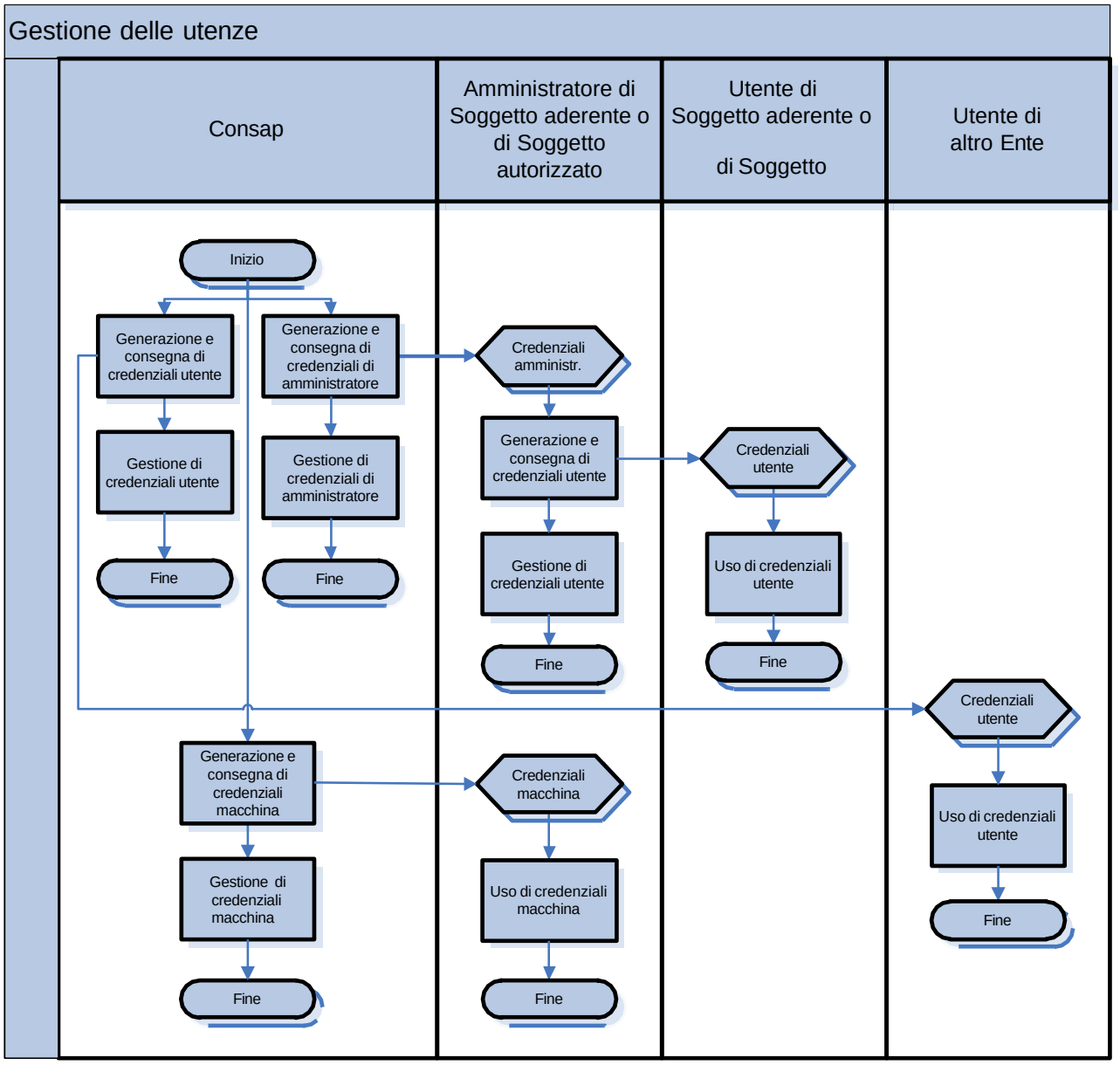
- Il soggetto segnalante accede a un apposito servizio sulla home page pubblica del sito web;
- Nel caso di segnalazione di frode subita, il soggetto segnalante compila una scheda di segnalazione fornendo le proprie generalità e i dati relativi alla frode subita, che vengono registrati nell'archivio delle segnalazioni pervenute dai soggetti segnalanti; invia inoltre al call center copia dei documenti previsti dall'art. 22, comma 2, del regolamento di attuazione per la successiva registrazione nell'archivio;
- Nel caso di segnalazione di rischio di frode, il sito web invece non prevede alcuna registrazione di dati.

4. Modalità di collegamento informatico del sistema

Il sistema opera su un'apposita piattaforma tecnologica dedicata del MEF. Tale piattaforma è logicamente separata dal resto dell'impianto MEF - consentendone quindi l'esercizio anche in un eventuale cloud del MEF - ed è possibile il suo accesso, la sua gestione e la sua manutenzione al solo personale Consap e MEF autorizzato a tale attività.
Il sistema di riscontro comunica con i diversi interlocutori e sistemi cooperanti mediante meccanismi atti ad assicurare la riservatezza, l'integrità e l'autenticità delle comunicazioni.

5. Produzione, distribuzione e gestione delle credenziali di accesso al sistema

La figura seguente illustra il processo di gestione delle credenziali per l'accesso al sistema.



In particolare, è prevista la generazione e la gestione di tre tipi di credenziali di accesso ai servizi del sistema:

- credenziali di amministratore, generate da Consap con il sistema di gestione amministrativa delle convenzioni e consegnate agli utenti amministratori di ogni soggetto aderente che ne faccia domanda. Con tali credenziali, il soggetto aderente ha la possibilità di generare e di gestire credenziali utente per i propri utenti interni che saranno abilitati all'uso del sistema di riscontro;
- credenziali utente, generate da Consap o, per i propri utenti interni, dagli utenti amministratore dei soggetti aderenti o dei soggetti autorizzati. Queste credenziali permettono ai titolari di usare i servizi utente del sistema di riscontro;
- credenziali macchina, generate da Consap con il sistema di gestione amministrativa delle convenzioni per permettere ai sistemi informatici dei soggetti aderenti e dei soggetti autorizzati

di accreditarsi per ottenere servizi dal sistema informatico in modalità A2A - Application to Application.

L'autenticazione ai servizi SCIPAFI, sia in modalità interattiva (web based) che application-to-application (A2A), è assicurata attraverso l'implementazione di metodi d'accesso multifattore (c.d. Multi Factor Authentication) al fine di ridurre significativamente il rischio di accessi non autorizzati. In particolare, per la classe di utenti interattivi le credenziali di accesso sono costituite da nome utente (login), da una coppia di password e da un token di sicurezza, generato in modo random ad ogni accesso, che l'utente può ricevere attraverso e-mail o SMS. Per la classe di utenti macchina è invece previsto un metodo di autenticazione tra gli "end-point applicativi A2A" basato su mutua autenticazione attraverso certificati digitali TLS x509 emessi da una Certification Autority (CA) privata di CONSAP. Ciascun aderente ha la facoltà di richiedere a CONSAP un certificato digitale da associare ad uno specifico "utente macchina" per l'autenticazione applicativa.

L'utenza di tipo interattivo accede al sistema di riscontro via internet usando credenziali nominative (credenziali utente) costituite da una login, una prima password (password1) e una seconda password (password2). Le credenziali hanno le seguenti caratteristiche:

- sono generate mediante il sistema di gestione amministrativa dall'amministratore di sistema Consap o dagli utenti dell'aderente aventi ruolo di amministratore;
- la login individua univocamente l'utente;
- la prima password è fornita automaticamente al solo utente titolare, mediante email inviata alla casella di posta elettronica del titolare;
- la seconda password è fornita automaticamente all'organizzazione di appartenenza dell'utente titolare mediante messaggio PEC inviato alla casella di posta elettronica certificata dell'organizzazione di appartenenza dell'utente titolare che la dovrà inoltrare all'utente stesso;
- la procedura tecnica di autenticazione prevede, a valle dell'inserimento di login e delle due password, l'invio di un token quale ulteriore fattore di autenticazione;
- al primo accesso il sistema chiede all'utente di cambiare la prima password;
- il sistema chiede all'utente di cambiare la prima password se sono trascorsi più di sei mesi dall'ultima modifica;
- l'amministratore di sistema Consap o l'utente col ruolo di amministratore del soggetto aderente possono abilitare/disabilitare gli utenti all'uso dei servizi SCIPAFI e cambiarne il ruolo, ovvero l'insieme delle funzioni applicative ad essi abilitate;
- un'apposita funzione applicativa elabora con periodicità semestrale un report degli utenti configurati a sistema e la relativa data di ultimo accesso. Il report viene analizzato sistematicamente dal personale di Consap che, a valle delle necessarie verifiche, può decidere di disabilitare le utenze non più attive.

Attraverso il portale amministrativo è possibile gestire anche le utenze della c.d. classe macchina, ovvero le utenze a cui saranno associati i certificati digitali utilizzati per la muta autenticazioni in modalità application-to-application. In particolare, attraverso apposite funzioni applicative, l'amministratore di CONSAP o l'utente amministratore dell'aderente potranno richiedere la creazione di un utente specifico di "classe macchina" e la contestuale generazione di un certificato digitale ad esso associato. Il certificato digitale verrà quindi emesso da CONSAP attraverso una CA privata e reso disponibile al richiedente all'interno del portale amministrativo. L'aderente potrà così scaricare il certificato client ed installarlo sull'end-point applicativo che comunica col sistema di riscontro in modalità A2A.

Al momento dell'invocazione dell'end-point di riscontro si attiva una procedura automatica di mutua autenticazione tra il certificato dell'aderente e quello già presente sul sistema di riscontro.

5.1. Gestione dei ruoli e profili autorizzativi

Il sistema SCIPAFI prevede differenti tipologie di aderenti. Ciascuna tipologia ha un profilo di visibilità, ovvero un set di dati riscontrabili presso le relative Banche Dati.

La tabella seguente riporta in colonna le tipologie di aderente ed in riga il set di dati riscontrabili. Ad esempio, si evince che la tipologia "**c-bis Imprese di assicurazione**" non possono riscontrare la dichiarazione dei redditi presso la BD AdE.

Sezione / Banca Dati di riferimento	a) banche e intermediari finanziari ex art. 106 del TUB	a) intermediari finanziari ex art. 114-quater del TUB (IMEL)	a) intermediari finanziari ex art. 114-septies del TUB (IP)	b) Fornitori di comunicazion e elettronica	b-bis) Gestori di identità digitale / b-bis) Fornitori di servizi fiduciari qualificati e gestori di posta elettronica certificata	b-ter) soggetti autorizzati distributori di energia	c) Fornitori di servizi interattivi associati o di servizi di accesso condizionato	c-bis) Imprese di assicurazion e	d) Gestori sistemi informazione credit. e imprese che offrono servizi assimilabili
Dati identificativi (ADE)	si	si	si	si	si	si	si	si	si
Domicilio fiscale (ADE)	si	si	si	si	no	si	si	si	in base al delegante
Patente di guida (MIT)	si	si	si	si	si	si	si	si	si
Passaporto (CEN)	si	si	si	si	si	si	si	si	si
Permesso di soggiorno (CEN)	si	si	si	si	si	si	si	si	si
Altro documento (CED Interforze)	si	si	si	si	si	si	si	si	si
Tessera sanitaria (RGS)	si	si	si	si	si	si	si	si	si
Dichiarazione dei redditi (ADE)	si	si	si	no	no	no	no	no	in base al delegante
Busta paga dip. Privati (INPS)	si	si	si	no	no	no	no	no	in base al delegante
Busta paga dip. Pubblici (Ex-Inpdap)	si	si	si	no	no	no	no	no	in base al delegante
Dati identificativi - Partita iva (ADE)	si	si	si	no	no	no	no	no	in base al delegante
Posizione INAIL (INAIL)	si	si	si	no	no	no	no	no	in base al delegante
Carta di Identità	si	si	si	si	si	si	si	si	si
Pratica (ANPR)	si	si	si	si	si	si	si	si	si

Inoltre, a livello utente il sistema SCIPAFI prevede i seguenti ruoli autorizzativi:

- Amministratore di sistema Consap: soggetto incaricato alla configurazione del portale amministrativo Scipafi. Inserisce i dati della società e del Riferimento operativo/organizzativo (presente sul formulario) che si occuperà dell'iter convenzionale;

- Riferimento operativo/organizzativo autorizzato tramite formulario: previa richiesta, Consap assegna le credenziali di accesso al solo portale amministrativo con accesso condizionato ad alcune funzioni (a titolo di esempio, per la gestione amministrativa della convenzione);

- Riferimento di sicurezza individuato e autorizzato tramite formulario: previa richiesta, Consap assegna le credenziali di accesso al portale amministrativo. Con tali credenziali, il Riferimento di sicurezza ha la facoltà di generare e di gestire direttamente le credenziali degli utenti per l'accesso e l'utilizzo del sistema di riscontro e di quello amministrativo per tutti i soggetti appartenenti all'organizzazione dell'aderente;

- Riferimento amministrativo individuato e autorizzato tramite formulario: previa richiesta, Consap assegna le credenziali di accesso al solo portale amministrativo con accesso condizionato ad alcune funzioni (a titolo di esempio, per la gestione dei pagamenti/fatture/consumi);

- Riferimento informatico individuato e autorizzato tramite formulario: previa richiesta, Consap assegna le credenziali di accesso al portale amministrativo e di riscontro con accesso condizionato ad alcune funzioni (a titolo di esempio, per conferire obbligatorietà ad alcuni campi non necessariamente obbligatori per il sistema di riscontro);

- Utente di riscontro individuato dal Referente di sicurezza: accede al sistema di riscontro e al sistema amministrativo per la sola gestione dell'utenza;

- Utenti delle Amministrazioni (Mef/Consap): queste credenziali, assegnate da Consap, permettono ai titolari di usare i servizi utente del sistema amministrativo e di riscontro.

Il sistema amministrativo prevede dei programmi di tipo batch che periodicamente verificano l'utilizzo delle utenze (ultimo login a sistema). Dopo un periodo di inattività (configurato a 180g) viene inviata una email automatica all'aderente informandolo che dopo ulteriori 30gg l'utenza verrà disabilitata.

6. Tracciamento delle operazioni

Tutte le operazioni di accesso (lato *client*) ai servizi del sistema di riscontro, comprese quelle per l'accesso e l'utilizzo delle informazioni presenti nell'archivio delle frodi subite, e tutte le richieste di servizio del sistema di riscontro alle banche dati istituzionali (lato *server*) sono registrate in log applicativi, nei quali viene associato ad ogni operazione l'identificativo dell'utente richiedente l'operazione stessa. Più in particolare:

- per ogni operazione eseguita con il sistema di riscontro, il sistema stesso registra l'utente che ha eseguito l'operazione, il momento e il tipo di operazione eseguita;
- per ogni richiesta di riscontro e per ogni richiesta di accesso all'archivio delle frodi subite sono registrate nella base di dati di sistema l'identificativo dell'utente richiedente, l'identificativo dell'aderente/soggetto autorizzato di appartenenza e dell'eventuale aderente delegante, l'identificativo univoco della richiesta, la data e ora (*timestamp*) della richiesta pervenuta dall'aderente/soggetto autorizzato e la data e ora (*timestamp*) della risposta fornita all'aderente/soggetto autorizzato, l'elenco dei campi oggetto di riscontro/accesso all'archivio delle frodi subite e il codice fiscale della persona fisica oggetto di riscontro: questa ultima informazione è memorizzata - in forma criptata - in modo che possa essere verificata, attraverso una specifica funzione applicativa messa a disposizione del solo personale Consap appositamente incaricato, nell'ambito di possibili controlli sulla liceità dell'uso del sistema da parte dell'utenza in specifici casi. Nel caso di richieste di riscontro, sono inoltre registrati nella base di dati di sistema l'elenco degli esiti semaforici restituiti dalle banche dati a fronte di ognuno dei campi oggetto di riscontro, l'elenco delle banche dati interpellate e l'esito tecnico complessivo dell'esecuzione della richiesta (in termini di esecuzione terminata correttamente oppure no);
- per ogni richiesta di riscontro attivata dal sistema di riscontro nei confronti di ogni banca dati, sono registrate inoltre nella base di dati di sistema l'identificativo univoco della richiesta dell'aderente/soggetto autorizzato originante tale attivazione di servizio, l'identificativo della banca dati chiamata e del servizio invocato, la data e ora (*timestamp*) della richiesta effettuata dal sistema di riscontro e la data e ora (*timestamp*) della risposta fornita dalla banca dati, l'elenco dei campi (ma non i corrispondenti valori) oggetto di riscontro, l'elenco dei corrispondenti esiti semaforici restituiti dalla banca dati e l'esito tecnico complessivo dell'invocazione del servizio fornito dalla banca dati (in termini di esecuzione terminata correttamente oppure no).

7. Profili di autorizzazione

Il sistema consente all'utenza di riscontrare insiemi diversi di dati in funzione della singola tipologia di aderente/soggetto autorizzato.

La tabella seguente mostra i profili di autorizzazione previsti per le singole tipologie di aderenti/soggetti autorizzati, in rapporto ai riscontri sui diversi tipi di dati previsti dall'art. 12 del regolamento attuativo.

	Dati oggetto di riscontro	**Aderenti ex art. 30-ter, comma 5, lettera a)**	**Aderenti ex art. 30-ter, comma 5, lettera b)**	**Aderenti ex art. 30-ter, comma 5, lettera b-bis)**	**Aderenti ex art. 30-ter, comma 5, lettera b-ter)**	**Aderenti ex art. 30-ter, comma 5, lettera c)**	**Aderenti ex art. 30-ter, comma 5, lettera c-bis)**	**Aderenti ex art. 30-ter, comma 5, lettera d)**	**Soggetti autorizzati ex art. 30-ter, commi 5-bis e 6**
Elementi identificativi del richiedente (articolo 12, comma 1, lettere a) e b)	Nome e cognome Data e luogo di nascita Sesso Cittadinanza Domicilio fiscale* Provincia Codice avviamento postale Residenza* Provincia Codice avviamento postale Riscontro dell'esistenza in vita Identificativo unico ANPR	Si	Si	Si	Si	Si	Si	Si	Si
Elementi identificativi dei documenti di identità (articolo 12, comma 1, lettera c)	Tipologia di documento Numero del documento Data di rilascio del documento Data di scadenza del documento Ente che ha rilasciato il documento Provincia del comune che ha rilasciato il documento Numero di serie del supporto plastico Riscontro della presenza del documento nell'archivio dei documenti smarriti o rubati	Si	Si	Si	Si	Si	Si	Si	Si

	Dati oggetto di riscontro	Aderenti ex art. 30-ter, comma 5, lettera a)	Aderenti ex art. 30-ter, comma 5, lettera b)	Aderenti ex art. 30-ter, comma 5, lettera b-bis)	Aderenti ex art. 30-ter, comma 5, lettera b-ter)	Aderenti ex art. 30-ter, comma 5, lettera c)	Aderenti ex art. 30-ter, comma 5, lettera c-bis)	Aderenti ex art. 30-ter, comma 5, lettera d)	Soggetti autorizzati ex art. 30-ter, commi 5-bis e 6
Dati relativi alle tessere sanitarie, ai codici fiscali, alle partite IVA e ai documenti che attestano il reddito (articolo 12, comma 2)	Numero della tessera sanitaria Data di scadenza della tessera sanitaria Riscontro della presenza della tessera sanitaria nell'archivio dei documenti smarriti o rubati Numero del codice fiscale Numero della partita IVA Data di attribuzione della partita IVA	Si	Si	Si	Si	Si	Si	Si	Si
	Anno dell'ultima presentazione della dichiarazione dei redditi Riscontro della fascia di reddito entro la quale la persona fisica è collocata	Si	No	No	No	No	No	Autorizzazione in funzione della tipologia di aderente/ soggetto autorizzato delegante	Si
Dati relativi alle posizioni contributive, previdenziali e assistenziali (articolo 12, comma 3)	Data di inizio del rapporto di lavoro Tipologia del rapporto di lavoro Qualifica Periodo di competenza del prospetto di paga Imponibile previdenziale del prospetto di paga Numero posizione contributiva previdenziale del datore di lavoro Numero posizione assicurativa del datore di lavoro Nominativo del datore di lavoro o del rappresentante legale Numero del codice fiscale del datore di lavoro Numero della partita IVA del datore di lavoro	Si	No	No	No	No	No	Autorizzazione in funzione della tipologia di aderente/ soggetto autorizzato delegante	Si

* Tale dato viene restituito in chiaro a causa dell'impossibilità tecnica di utilizzare campi "normalizzati".