S.I.P.S.E.

SISTEMA DELLE ISTITUZIONI DEI POPOLI PER LA SOVRANITÀ ECONOMICA

MANUALE TECNICO N. 21/MSP- RMG

REGISTRO MULTILATERALE DELLE GARANZIE (RMG)

Specifiche tecniche, architettura informativa, modello dei dati, identificazione, registrazione, verifica, tracciabilità, interoperabilità e sicurezza del Registro Multilaterale delle Garanzie.

IDENTIFICAZIONE DOCUMENTALE

Campo	Descrizione
Organizzazione	S.I.P.S.E.
Sistema	Mercato Sovrano dei Popoli – MSP
Documento	Manuale tecnico n. 21/MSP
Codice	SIPSE/MSP/MAN/2026/21
Versione	1.0
Data	16 novembre 2026
Sistema interessato	Registro Multilaterale delle Garanzie
Sigla	RMG
Collegamento normativo	Atto n. 18/MSP e Regolamento n. 20/MSP
Integrazioni	CMCRP, RMUM, SMQVM, DSPP, SMRC, LIS-Clear, SIPSE Pay e BNVSM
Stato documentale	Specifica tecnica e organizzativa

Sede istituzionale indicata: Venezia – Palazzo della Zecca.

PREMESSA

Il presente Manuale tecnico definisce il modello informatico, documentale e procedurale del Registro Multilaterale delle Garanzie (RMG), infrastruttura destinata alla raccolta, identificazione, classificazione, verifica, conservazione e consultazione delle informazioni relative alle garanzie dichiarate o documentate dai soggetti partecipanti al Mercato Sovrano dei Popoli.

Il RMG costituisce il punto di riferimento informativo per la gestione delle garanzie e delle coperture connesse alle esposizioni registrate nel sistema MSP.

Il Registro è progettato per consentire:

1. l'identificazione univoca di ogni garanzia;
2. la raccolta della documentazione relativa alla sua costituzione;
3. la verifica documentale e, ove possibile, indipendente;
4. la distinzione tra garanzie dichiarate, documentate, verificate e perfezionate;
5. il monitoraggio del valore prudenziale e della disponibilità;
6. la registrazione delle variazioni e degli eventi;
7. l'interoperabilità con la CMCRP;
8. la produzione di report destinati agli organi competenti;
9. la ricostruzione cronologica delle attività svolte;
10. la prevenzione delle duplicazioni, delle dichiarazioni incongruenti e delle registrazioni non supportate da evidenze.

Il RMG non costituisce, per effetto della sola registrazione, prova definitiva della proprietà di un bene, dell'esistenza di un credito, della validità di una garanzia, della disponibilità di fondi o della sua opponibilità a terzi.

La qualificazione giuridica di ciascuna garanzia resta subordinata alla documentazione, alla legge applicabile, agli accordi sottoscritti, agli eventuali registri pubblici competenti e alle verifiche effettivamente eseguite.

TITOLO I – DISPOSIZIONI GENERALI

Articolo 1 – Oggetto

1. Il presente Manuale disciplina le specifiche tecniche e operative del Registro Multilaterale delle Garanzie.
2. Il Manuale definisce l'architettura logica, il modello dei dati, gli identificativi, i livelli di evidenza, i procedimenti di registrazione e verifica, i profili di accesso e le procedure di sicurezza.
3. Le specifiche costituiscono il riferimento per la progettazione, lo sviluppo, il collaudo e l'eventuale esercizio del sistema informatico RMG.

Articolo 2 – Finalità

Il RMG persegue le seguenti finalità:

a. documentare le garanzie dichiarate dai partecipanti;

b. consentire la verifica della documentazione presentata;

c. associare le garanzie alle esposizioni ammissibili;

d. monitorare il valore prudenziale;

e. identificare le scadenze e gli eventi rilevanti;

f. individuare le situazioni di duplicazione o sovrapposizione;

g. rendere disponibili informazioni coerenti agli altri sistemi MSP;

h. assicurare la tracciabilità delle operazioni;

i. consentire controlli interni e verifiche indipendenti.

Articolo 3 – Natura del Registro

1. Il RMG è concepito come registro informativo, documentale e di controllo.
2. La sua eventuale realizzazione informatica dovrà rispettare le norme applicabili in materia di protezione dei dati, sicurezza informatica, conservazione documentale e trattamento delle informazioni economiche e patrimoniali.
3. L'iscrizione non costituisce automaticamente:
    - certificazione di solvibilità;
    - attestazione di proprietà;
    - riconoscimento di un diritto reale;
    - garanzia di rimborso;
    - attestazione di liquidità;
    - autorizzazione all'esercizio di attività finanziarie;
    - prova di convertibilità monetaria;
    - prova dell'avvenuto pagamento.

Articolo 4 – Ambito di applicazione

Il Registro può contenere informazioni relative a:

a. depositi e disponibilità liquide documentate;

b. crediti e diritti di credito;

c. garanzie bancarie o finanziarie, ove validamente emesse;

d. garanzie personali;

e. garanzie reali;

f. beni mobili e immobili;

g. metalli preziosi e altri beni patrimoniali;

h. titoli e strumenti finanziari;

i. fondi segregati o vincolati, ove giuridicamente documentati;

j. altre forme di garanzia ammissibili secondo il Regolamento n. 20/MSP.

Articolo 5 – Principi di funzionamento

Il RMG opera secondo i seguenti principi:

1. identificazione univoca;
2. verificabilità;
3. completezza documentale;
4. separazione tra dichiarazione e accertamento;
5. tracciabilità;
6. riservatezza;
7. integrità;
8. aggiornamento;
9. proporzionalità dei controlli;
10. responsabilità del soggetto dichiarante;
11. separazione delle funzioni;
12. interoperabilità controllata.

Articolo 6 – Definizioni

Ai fini del presente Manuale:

- **RMG:** Registro Multilaterale delle Garanzie.
- **Garanzia:** bene, diritto, impegno o strumento destinato a coprire un'obbligazione.
- **Dichiarante:** soggetto che presenta la richiesta di registrazione.
- **Beneficiario:** soggetto a favore del quale la garanzia è costituita.
- **Garante:** soggetto che presta o costituisce la garanzia.
- **Custode:** soggetto che detiene materialmente o amministrativamente il bene, ove applicabile.
- **Valore dichiarato:** valore comunicato dal dichiarante.
- **Valore documentato:** valore supportato da documentazione acquisita.
- **Valore verificato:** valore sottoposto a controllo documentale o specialistico.
- **Valore prudenziale:** valore risultante dall'applicazione dei criteri prudenziali.
- **Perfezionamento:** completamento degli adempimenti richiesti dalla disciplina applicabile.
- **RMG-ID:** identificativo univoco della registrazione.
- **Evidenza:** documento, attestazione o riscontro utilizzato nel procedimento.

TITOLO II – ARCHITETTURA TECNICA DEL SISTEMA

Articolo 7 – Architettura generale

Il sistema RMG è progettato secondo un'architettura modulare composta dai seguenti componenti:

1. modulo di autenticazione;
2. modulo di gestione dei partecipanti;
3. modulo di acquisizione delle domande;
4. modulo di gestione documentale;

5. modulo di identificazione delle garanzie;
6. modulo di classificazione;
7. modulo di istruttoria;
8. modulo di valutazione prudenziale;
9. modulo di gestione delle esposizioni;
10. modulo di monitoraggio;
11. modulo di interoperabilità;
12. modulo di audit;
13. modulo di reportistica;
14. modulo di sicurezza e amministrazione.

Articolo 8 – Moduli applicativi

8.1 Modulo partecipanti

Gestisce:

- anagrafica dei partecipanti;
- codici identificativi;
- rappresentanti autorizzati;
- poteri di firma;
- stato di adesione;
- profili di accesso;
- storico delle modifiche.

8.2 Modulo delle garanzie

Gestisce:

- identificativo della garanzia;
- categoria;
- tipologia;
- soggetto garante;
- beneficiario;
- importo;
- valuta o unità di riferimento;
- durata;
- scadenza;
- condizioni;
- eventuali vincoli;
- stato della registrazione.

8.3 Modulo documentale

Consente:

- caricamento dei documenti;
- classificazione;
- indicizzazione;
- associazione alla garanzia;

- verifica di integrità;
- registrazione delle versioni;
- conservazione secondo la politica documentale applicabile.

8.4 Modulo di verifica

Gestisce le attività istruttorie e registra:

- soggetto verificatore;
- data;
- oggetto del controllo;
- metodologia;
- documenti esaminati;
- risultato;
- eventuali limitazioni;
- motivazione dell'esito.

8.5 Modulo di valorizzazione

Acquisisce i valori documentati e verificati e applica i criteri prudenziali previsti dal Regolamento n. 20/MSP.

8.6 Modulo di interoperabilità

Consente lo scambio controllato di informazioni con i sistemi MSP, senza attribuire automaticamente effetti dispositivi alle comunicazioni ricevute.

Articolo 9 – Separazione architetturale

1. I moduli di acquisizione, verifica, approvazione e amministrazione devono essere logicamente separati.
2. Il soggetto che inserisce una garanzia non può approvarne autonomamente il livello di verifica.
3. Le operazioni sensibili devono prevedere autorizzazioni distinte.
4. Le modifiche successive all'approvazione devono generare una nuova versione o un nuovo evento tracciato.

Articolo 10 – Ambienti informatici

Il sistema prevede tre ambienti distinti.

Ambiente	Funzione
SIM	Simulazione e sviluppo dei processi
UAT	Collaudo e accettazione degli utenti
PROD	Eventuale esercizio operativo

1. L'ambiente SIM utilizza dati sintetici o opportunamente anonimizzati.
2. L'ambiente UAT verifica la conformità funzionale e tecnica.

3. L'ambiente PROD può essere attivato soltanto dopo le verifiche organizzative, tecniche, legali e di sicurezza.
4. Nessuna attività SIM o UAT costituisce registrazione operativa di una garanzia reale.

TITOLO III – IDENTIFICAZIONE E CODIFICAZIONE

Articolo 11 – Identificativo univoco

Ogni garanzia registrata riceve un identificativo RMG-ID.

Formato proposto:

```
SIPSE-RMG-[AREA]-[CODICE-POPOLO]-[TIPO]-[ANNO]-[PROGRESSIVO]
```

Esempio puramente illustrativo:

```
SIPSE-RMG-PAT-VT963-G05-2026-000001
```

L'identificativo non costituisce attestazione di validità o perfezionamento della garanzia.

Articolo 12 – Componenti dell'identificativo

Elemento	Significato
SIPSE	Sistema di appartenenza
RMG	Registro Multilaterale delle Garanzie
PAT	Area patrimoniale
VT963	Codice identificativo del soggetto o ambito registrato
G05	Categoria della garanzia
2026	Anno di registrazione
000001	Numero progressivo

Articolo 13 – Identificativo della versione

Ogni garanzia deve avere un numero di versione.

Formato:

```
RMG-ID/V01
```

Esempio:

```
SIPSE-RMG-PAT-VT963-G05-2026-000001/V01
```

Le modifiche sostanziali producono una nuova versione, senza cancellare la precedente.

Articolo 14 – Identificativo documentale

Ogni documento allegato deve ricevere un codice autonomo:

```
RMG-DOC-[RMG-ID]-[TIPO]-[PROGRESSIVO]
```

La piattaforma deve inoltre associare al documento un'impronta crittografica per consentire il controllo dell'integrità del file.

Articolo 15 – Codici delle categorie

Il sistema adotta la classificazione seguente:

Codice	Categoria
G01	Disponibilità liquide
G02	Depositi documentati
G03	Crediti
G04	Garanzie personali
G05	Beni immobili
G06	Beni mobili
G07	Metalli preziosi
G08	Titoli e strumenti finanziari
G09	Fondi vincolati o segregati
G10	Altre garanzie ammissibili

La classificazione non sostituisce la qualificazione giuridica dello strumento.

TITOLO IV – MODELLO DEI DATI

Articolo 16 – Struttura generale

Il sistema informativo deve organizzare i dati secondo entità logicamente distinte e collegate.

Le entità principali sono:

1. partecipante;
2. garante;
3. beneficiario;
4. garanzia;
5. documento;
6. verifica;
7. valutazione;
8. esposizione;
9. vincolo;
10. evento;
11. autorizzazione;

12. registrazione;
13. operazione di interoperabilità.

Articolo 17 – Scheda anagrafica della garanzia

Ogni garanzia deve contenere almeno i seguenti campi:

Campo	Obbligatorietà
RMG-ID	Obbligatorio
Denominazione	Obbligatorio
Categoria	Obbligatorio
Tipologia	Obbligatorio
Dichiarante	Obbligatorio
Garante	Se applicabile
Beneficiario	Se applicabile
Descrizione	Obbligatorio
Valore dichiarato	Obbligatorio
Unità di riferimento	Obbligatorio
Data di costituzione	Se applicabile
Data di scadenza	Se applicabile
Luogo di custodia	Se applicabile
Stato giuridico dichiarato	Obbligatorio
Documentazione	Obbligatoria
Livello di evidenza	Dopo istruttoria
Valore prudenziale	Dopo valutazione

Articolo 18 – Soggetti collegati

1. Il sistema deve distinguere il dichiarante dal garante e dal beneficiario.
2. Uno stesso soggetto può assumere più ruoli, purché siano identificati separatamente.
3. I poteri rappresentativi devono essere documentati.
4. La piattaforma non deve presumere la titolarità o la rappresentanza sulla sola base dell'inserimento dei dati.

Articolo 19 – Dati economici e monetari

Ogni importo deve indicare:

- valore numerico;
- unità monetaria o unità di conto;
- data di riferimento;
- fonte del valore;
- metodo di valutazione;
- eventuale tasso di conversione;
- categoria della quotazione;

- data di acquisizione del dato.

Il DSPP può essere utilizzato come unità comune di conto per la comparazione e la rendicontazione, senza essere automaticamente qualificato come moneta o mezzo di pagamento.

Articolo 20 – Relazione con le esposizioni

1. Ogni garanzia può essere collegata a una o più esposizioni, nei limiti della sua effettiva disponibilità e della disciplina applicabile.
2. Il sistema deve identificare l'importo massimo impegnato.
3. Deve essere impedito il conteggio duplicato della medesima garanzia.
4. Le garanzie parzialmente utilizzate devono riportare il valore residuo documentato.
5. Le sovrapposizioni devono essere segnalate e sottoposte a verifica.

Articolo 21 – Modello relazionale

La relazione logica tra le entità è la seguente:

- un partecipante può presentare più garanzie;
- una garanzia può contenere più documenti;
- una garanzia può avere più verifiche;
- una garanzia può avere più valutazioni nel tempo;
- una garanzia può essere collegata a più esposizioni;
- una garanzia può generare più eventi;
- ogni evento deve essere associato a un soggetto autorizzato.

TITOLO V – PROCEDIMENTO DI REGISTRAZIONE

Articolo 22 – Presentazione della domanda

La domanda di registrazione è presentata da un partecipante autorizzato.

Deve contenere:

a. dati identificativi del richiedente;

b. descrizione della garanzia;

c. categoria proposta;

d. valore dichiarato;

e. indicazione dei soggetti interessati;

f. documentazione disponibile;

g. dichiarazione di completezza e veridicità;

h. autorizzazione al trattamento delle informazioni secondo le regole applicabili.

Articolo 23 – Acquisizione

Il sistema:

1. assegna un numero di pratica;
2. registra data e ora;
3. verifica la completezza formale;
4. assegna un responsabile istruttorio;
5. genera la ricevuta di acquisizione.

La ricevuta attesta esclusivamente la ricezione della domanda.

Articolo 24 – Controllo preliminare

Il controllo preliminare riguarda:

- completezza dei campi;
- leggibilità dei documenti;
- coerenza degli identificativi;
- presenza delle dichiarazioni richieste;
- eventuali duplicazioni;
- compatibilità della categoria proposta.

La presenza di anomalie può determinare una richiesta di integrazione.

Articolo 25 – Istruttoria documentale

L'istruttoria deve identificare:

1. origine del documento;
2. soggetto emittente;
3. data di emissione;
4. validità temporale;
5. eventuale firma;
6. modalità di verifica;
7. corrispondenza tra documento e garanzia;
8. eventuali limitazioni o condizioni.

Articolo 26 – Esiti dell'istruttoria

Gli esiti possibili sono:

- ammessa all'istruttoria;
- integrazione richiesta;
- sospesa;

- respinta;
- registrata con livello V0;
- registrata con livello superiore, previa verifica.

Ogni esito deve essere motivato e tracciato.

Articolo 27 – Registrazione iniziale

La registrazione iniziale produce:

- RMG-ID;
- scheda digitale;
- fascicolo documentale;
- stato iniziale;
- livello di evidenza attribuito;
- responsabile dell'istruttoria;
- data di registrazione.

La registrazione iniziale non equivale ad approvazione definitiva della garanzia.

TITOLO VI – LIVELLI DI EVIDENZA V0–V3

Articolo 28 – Principio di classificazione

Il RMG adotta quattro livelli di evidenza, coerenti con il Regolamento n. 20/MSP.

Articolo 29 – Livello V0: dichiarata

Una garanzia è classificata V0 quando:

- è stata dichiarata dal partecipante;
- è stata acquisita dal sistema;
- non è stata ancora sottoposta a verifica documentale sufficiente.

La dicitura deve essere:

V0 – DICHIARATA, NON VERIFICATA.

Articolo 30 – Livello V1: documentata

Una garanzia può essere classificata V1 quando:

- esiste un fascicolo documentale;
- i documenti sono stati acquisiti;
- l'integrità dei file è stata registrata;
- è stata svolta una verifica di completezza formale.

La dicitura deve essere:

V1 – DOCUMENTATA, NON NECESSARIAMENTE VERIFICATA NEL MERITO.

Articolo 31 – Livello V2: verificata

Una garanzia può essere classificata V2 quando:

- la documentazione è stata esaminata;
- sono state effettuate verifiche coerenti con la natura della garanzia;
- l'esito è stato registrato;
- il verificatore è identificato;
- le eventuali limitazioni sono indicate.

La dicitura deve essere:

V2 – VERIFICATA SECONDO LE EVIDENZE E I CONTROLLI REGISTRATI.

Il livello V2 non equivale automaticamente a disponibilità, liquidità, opponibilità o perfezionamento.

Articolo 32 – Livello V3: perfezionata e disponibile

Una garanzia può essere classificata V3 soltanto quando siano documentati e verificati, secondo la natura dello strumento:

- il perfezionamento degli atti richiesti;
- la titolarità o legittimazione rilevante;
- la costituzione del vincolo;
- la disponibilità effettiva;
- l'assenza o l'indicazione di vincoli incompatibili;
- la possibilità giuridica di utilizzo per la finalità dichiarata.

La dicitura deve essere:

V3 – PERFEZIONATA E DISPONIBILE, NEI LIMITI DELLE VERIFICHE DOCUMENTATE.

Articolo 33 – Attribuzione del livello

1. Il livello deve essere attribuito da un soggetto autorizzato.
2. La piattaforma non deve assegnare automaticamente V2 o V3 sulla sola base di controlli informatici.
3. Ogni attribuzione deve riportare motivazione, data, autore e documentazione di riferimento.
4. Un livello può essere ridotto quando emergano nuove informazioni.

Articolo 34 – Revisione del livello

Il livello deve essere riesaminato in presenza di:

- scadenza;
- perdita di disponibilità;
- modifica del titolo;
- variazione del valore;
- contestazione;
- pignoramento o vincolo;
- deterioramento del bene;
- perdita di efficacia della garanzia;
- nuova documentazione incompatibile.

TITOLO VII – VALUTAZIONE PRUDENZIALE

Articolo 35 – Principi di valutazione

La valutazione deve considerare:

1. natura della garanzia;
2. qualità delle evidenze;
3. liquidabilità;
4. volatilità del valore;
5. tempi di realizzo;
6. costi di conservazione;
7. rischi giuridici;
8. vincoli e gravami;
9. rischio di controparte;
10. rischio di duplicazione.

Articolo 36 – Valore di riferimento

Il valore di riferimento deve essere associato a una fonte identificabile e a una data precisa.

Non è ammesso utilizzare un valore privo di fonte senza indicare che si tratta di una dichiarazione del partecipante.

Articolo 37 – Formula del valore prudenziale

Il valore prudenziale è determinato secondo la formula:

[
VP = VR \times (1-h)
]

Dove:

- (VP) = valore prudenziale;
- (VR) = valore di riferimento;

- (h) = coefficiente prudenziale di riduzione.

Il coefficiente deve essere definito in base alla categoria, alla qualità delle evidenze, alla volatilità e ai rischi.

Articolo 38 – Parametri prudenziali

I parametri numerici non sono fissati in modo automatico dal presente Manuale.

Dovranno essere approvati con specifica deliberazione tecnica sulla base di:

- dati verificabili;
- metodologie dichiarate;
- analisi dei rischi;
- eventuali valutazioni indipendenti;
- aggiornamenti periodici.

Articolo 39 – Valore non determinabile

Quando non sia possibile determinare un valore attendibile:

1. il valore prudenziale deve essere indicato come non determinato;
2. la garanzia non può essere conteggiata come copertura certa;
3. la motivazione deve essere registrata;
4. deve essere prevista, ove possibile, un'attività di integrazione.

Articolo 40 – Valore e DSPP

La conversione in DSPP deve indicare:

- valore originario;
- unità monetaria originaria;
- fonte del cambio;
- data del cambio;
- categoria SMQVM;
- risultato della conversione;
- eventuale margine di incertezza.

L'utilizzo del DSPP non modifica la natura giuridica della garanzia né determina un pagamento.

TITOLO VIII – GESTIONE DELLE ESPOSIZIONI

Articolo 41 – Collegamento alla CMCRP

Il RMG può trasmettere alla CMCRP informazioni relative a garanzie collegate a esposizioni registrate nel sistema di compensazione.

La trasmissione deve essere autorizzata e limitata ai dati necessari.

Articolo 42 – Esposizione coperta

Ai fini del monitoraggio interno, il sistema può calcolare:

[
ENC = \max(0,E-C)
]

Dove:

- (ENC) = esposizione non coperta;
- (E) = esposizione ammessa;
- (C) = copertura prudenziale effettivamente riconoscibile.

Articolo 43 – Rapporto di copertura

Il rapporto di copertura è calcolato secondo:

[
RC = \frac{C}{E}\times100
]

Se l'esposizione è pari a zero, il rapporto deve essere indicato come non applicabile.

Articolo 44 – Controllo della duplicazione

1. Ogni garanzia deve essere associata alle esposizioni per le quali è effettivamente impegnata.
2. Il sistema deve rilevare l'eventuale utilizzo della medesima garanzia in più posizioni.
3. L'utilizzo concorrente deve essere consentito soltanto quando compatibile con il titolo, la disponibilità e le condizioni applicabili.
4. In caso di dubbio, il sistema deve segnalare l'anomalia e sospendere il conteggio prudenziale contestato.

Articolo 45 – Aggiornamento delle esposizioni

Le informazioni relative alle esposizioni devono essere aggiornate in occasione di:

- nuove obbligazioni;
- pagamenti;
- regolamenti;
- estinzioni;
- variazioni contrattuali;
- escussioni;
- eventi di inadempimento.

La registrazione di un'operazione contabile non equivale alla prova del regolamento effettivo.

TITOLO IX – STATI E CICLO DI VITA

Articolo 46 – Stati della garanzia

Il sistema prevede i seguenti stati:

Codice	Stato	Significato
S00	Bozza	Inserimento non trasmesso
S01	Presentata	Domanda ricevuta
S02	In istruttoria	Verifiche in corso
S03	Integrazione	Documenti richiesti
S04	Registrata V0	Dichiarazione acquisita
S05	Documentata V1	Fascicolo completo formalmente
S06	Verificata V2	Controlli documentati
S07	Perfezionata V3	Requisiti verificati
S08	Attiva	Garanzia utilizzabile nei limiti attestati
S09	Sospesa	Utilizzo cautelativamente bloccato
S10	Scaduta	Termine superato
S11	Contestata	Contestazione registrata
S12	Revocata	Registrazione revocata secondo procedura
S13	Estinta	Garanzia terminata
S14	Archiviata	Fascicolo conservato

Articolo 47 – Transizioni

Ogni transizione deve essere:

- autorizzata;
- motivata;
- datata;
- attribuita a un soggetto;
- registrata nel log;
- eventualmente collegata a documentazione.

Non sono ammesse transizioni non autorizzate.

Articolo 48 – Sospensione

La sospensione può essere disposta in presenza di:

- documentazione sospetta;
- contestazione;
- perdita temporanea di disponibilità;
- rischio di duplicazione;
- scadenza non chiarita;

- provvedimento dell'autorità competente;
- incongruenze rilevanti.

Articolo 49 – Revoca ed estinzione

1. La revoca della registrazione e l'estinzione della garanzia sono eventi distinti.
2. La revoca riguarda la posizione nel Registro.
3. L'estinzione riguarda la cessazione della garanzia secondo il titolo e la disciplina applicabile.
4. Il sistema deve conservare lo storico anche dopo la revoca o l'estinzione.

TITOLO X – INTEROPERABILITÀ CON I SISTEMI MSP

Articolo 50 – Principio generale

L'interoperabilità è realizzata mediante interfacce controllate, autenticazione reciproca e scambio di dati strutturati.

Ogni sistema conserva la responsabilità dei dati di propria competenza.

Articolo 51 – Integrazione con la CMCRP

La CMCRP può ricevere dal RMG:

- RMG-ID;
- categoria;
- livello di evidenza;
- valore prudenziale;
- disponibilità residua;
- stato;
- data dell'ultima verifica;
- eventuali limitazioni.

La CMCRP non deve considerare una garanzia utilizzabile se non risultano soddisfatte le condizioni di ammissibilità e di riconoscimento previste dal relativo regolamento.

Articolo 52 – Integrazione con il RMUM

Il collegamento con il Registro Multilaterale delle Unità Monetarie consente di verificare i codici delle unità monetarie utilizzate nella documentazione.

L'iscrizione di un'unità nel RMUM non costituisce attestazione automatica del valore o della liquidità della garanzia.

Articolo 53 – Integrazione con lo SMQVM

Il RMG può acquisire dati di valorizzazione dallo SMQVM.

Ogni dato deve mantenere:

- codice della quotazione;
- categoria Q1–Q7;
- fonte;
- data;
- metodologia;
- eventuali limitazioni.

Articolo 54 – Integrazione con il DSPP

Il DSPP può essere impiegato per:

- comparazione dei valori;
- rendicontazione;
- calcolo delle esposizioni;
- rappresentazione delle coperture.

Il DSPP non diviene per questo mezzo di pagamento o regolamento.

Articolo 55 – Integrazione con SMRC

Il sistema SMRC può trasmettere informazioni sulle obbligazioni commerciali che richiedono copertura.

La trasmissione deve contenere identificativo dell'operazione, importo, unità di conto, soggetti e stato dell'obbligazione.

Articolo 56 – Integrazione con LIS-Clear

Le informazioni relative a garanzie eventualmente collegate a operazioni LIS-Clear devono essere trasmesse secondo le interfacce autorizzate.

Non si presume alcun rapporto fisso tra LIS, EUR e ZEC.

Articolo 57 – Integrazione con SIPSE Pay

SIPSE Pay può ricevere informazioni necessarie a controllare eventuali condizioni di copertura associate a operazioni di pagamento.

Il RMG non dispone direttamente l'esecuzione di pagamenti e non sostituisce le verifiche dell'infrastruttura di pagamento.

Articolo 58 – Integrazione con BNVSM

L'eventuale integrazione con il Banco Nazionale Veneto San Marco deve essere disciplinata da specifici accordi tecnici e giuridici.

Le informazioni relative a depositi, disponibilità o garanzie emesse devono provenire da fonti effettivamente autorizzate a confermarle.

Il sistema non deve qualificare una dichiarazione del partecipante come attestazione del Banco.

TITOLO XI – SICUREZZA E PROTEZIONE DEI DATI

Articolo 59 – Autenticazione

L'accesso al RMG deve avvenire mediante credenziali individuali e sistemi di autenticazione adeguati al rischio.

Per le operazioni sensibili è prevista l'autenticazione a più fattori.

Articolo 60 – Profili di autorizzazione

Sono previsti i seguenti profili:

Profilo	Funzione
RMG-ADM	Amministrazione tecnica
RMG-REG	Registrazione delle domande
RMG-VER	Verifica documentale
RMG-VAL	Valutazione prudenziale
RMG-AUD	Audit e controllo
RMG-LEG	Verifica giuridica
RMG-READ	Consultazione autorizzata
RMG-API	Accesso applicativo

Articolo 61 – Separazione dei compiti

1. L'amministratore tecnico non può modificare il merito delle valutazioni.
2. Il dichiarante non può validare la propria garanzia.
3. Il verificatore non può modificare retroattivamente le evidenze.
4. L'auditor dispone di accesso in lettura ai registri di controllo.
5. Le autorizzazioni devono essere periodicamente riesaminate.

Articolo 62 – Cifratura

Il sistema deve prevedere:

- cifratura dei dati in transito;

- cifratura dei dati conservati;
- gestione sicura delle chiavi;
- segregazione degli accessi;
- protezione dei documenti riservati;
- registrazione delle operazioni di accesso.

Articolo 63 – Integrità documentale

Ogni documento acquisito deve essere associato a un'impronta crittografica.

La modifica di un documento deve generare una nuova versione e una nuova impronta.

L'impronta crittografica dimostra l'integrità rispetto al file acquisito, non la veridicità del contenuto né l'autenticità sostanziale dell'emittente.

Articolo 64 – Registro degli eventi

Ogni operazione rilevante deve produrre un evento contenente:

- identificativo;
- data e ora;
- utente;
- ruolo;
- operazione;
- oggetto;
- valore precedente, ove applicabile;
- valore successivo;
- motivazione;
- esito.

I log devono essere protetti da alterazioni non autorizzate e conservati secondo una politica definita.

Articolo 65 – Protezione dei dati

Il trattamento dei dati personali deve rispettare la normativa applicabile, compresi i principi di:

- liceità;
- correttezza;
- trasparenza;
- limitazione delle finalità;
- minimizzazione;
- esattezza;
- limitazione della conservazione;
- integrità e riservatezza.

La pubblicazione di dati nel Registro deve essere limitata alle informazioni per le quali esista una base giuridica adeguata.

TITOLO XII – MONITORAGGIO E CONTROLLI

Articolo 66 – Monitoraggio periodico

Ogni garanzia attiva deve essere sottoposta a controlli periodici secondo la categoria, il rischio e la durata.

Articolo 67 – Eventi di allerta

Il sistema deve generare segnalazioni in caso di:

- prossima scadenza;
- documentazione non aggiornata;
- riduzione del valore;
- perdita di disponibilità;
- variazione del garante;
- contestazione;
- doppia registrazione;
- modifica dei vincoli;
- incoerenza con le esposizioni;
- anomalia nella documentazione.

Articolo 68 – Classificazione delle anomalie

Livello	Descrizione	Azione
A1	Anomalia informativa	Richiesta chiarimenti
A2	Incongruenza documentale	Sospensione istruttoria
A3	Rischio di copertura	Riesame prudenziale
A4	Possibile perdita della garanzia	Sospensione cautelativa
A5	Possibile frode o alterazione	Escalation e conservazione evidenze

Articolo 69 – Reportistica

Il RMG deve consentire la produzione di:

1. report delle garanzie registrate;
2. report per partecipante;
3. report per categoria;
4. report per livello V0–V3;
5. report delle garanzie attive;
6. report delle garanzie sospese;
7. report delle scadenze;
8. report dei valori prudenziali;
9. report delle esposizioni collegate;

10. report delle anomalie;
11. report delle verifiche;
12. report delle variazioni.

Articolo 70 – Audit

Le attività di audit devono essere indipendenti dalle funzioni operative oggetto di verifica.

L'audit deve poter ricostruire il procedimento dalla domanda iniziale fino allo stato attuale.

TITOLO XIII – CONTINUITÀ OPERATIVA

Articolo 71 – Backup

Il sistema deve adottare procedure di backup periodiche e verificabili.

I backup devono comprendere:

- database;
- documenti;
- configurazioni;
- log;
- metadati;
- registri di autorizzazione.

Articolo 72 – Ripristino

Devono essere definite procedure di ripristino e testate periodicamente.

Gli obiettivi di ripristino devono essere approvati in funzione del rischio e delle risorse effettivamente disponibili.

Articolo 73 – Continuità operativa

Il piano di continuità deve prevedere:

- indisponibilità temporanea;
- perdita di connettività;
- guasto infrastrutturale;
- incidente informatico;
- compromissione delle credenziali;
- perdita o corruzione dei dati;
- indisponibilità di servizi esterni.

Articolo 74 – Gestione degli incidenti

Ogni incidente deve essere:

1. identificato;
2. classificato;
3. registrato;
4. contenuto;
5. analizzato;
6. risolto;
7. sottoposto a verifica;
8. documentato nel rapporto conclusivo.

TITOLO XIV – COLLAUDO E ATTIVAZIONE

Articolo 75 – Principio di attivazione

L'attivazione del RMG deve avvenire progressivamente e soltanto dopo il completamento delle verifiche necessarie.

Articolo 76 – Collaudo funzionale

Il collaudo deve verificare:

- acquisizione delle domande;
- generazione degli identificativi;
- caricamento documentale;
- classificazione;
- livelli di evidenza;
- valutazione prudenziale;
- gestione degli stati;
- autorizzazioni;
- audit;
- reportistica.

Articolo 77 – Collaudo di sicurezza

Il collaudo deve comprendere:

- autenticazione;
- autorizzazioni;
- segregazione dei ruoli;
- protezione dei dati;
- cifratura;
- integrità;
- gestione delle sessioni;
- sicurezza delle interfacce;
- backup e ripristino.

Articolo 78 – Test di interoperabilità

Devono essere testati gli scambi con CMCRP, RMUM, SMQVM, DSPP, SMRC, LIS-Clear, SIPSE Pay e BNVSM, ove le relative interfacce siano effettivamente disponibili e autorizzate.

Articolo 79 – Verbale di collaudo

Il collaudo deve concludersi con un verbale che riporti:

- test eseguiti;
- risultati;
- anomalie;
- difetti residui;
- azioni correttive;
- responsabili;
- esito;
- raccomandazione di attivazione o non attivazione.

Articolo 80 – Avvio operativo

L'avvio operativo richiede un provvedimento interno espresso, successivo alle verifiche tecniche, organizzative e giuridiche.

Il presente Manuale, da solo, non attiva un'infrastruttura informatica né conferisce autorizzazioni esterne.

TITOLO XV – DISPOSIZIONI FINALI

Articolo 81 – Responsabilità del dichiarante

Il dichiarante risponde della correttezza delle informazioni fornite secondo gli accordi e le norme applicabili.

Articolo 82 – Responsabilità del verificatore

Il verificatore deve documentare i controlli effettivamente svolti, evitando attestazioni eccedenti l'ambito delle proprie competenze.

Articolo 83 – Modifiche del Manuale

Le modifiche devono essere approvate mediante atto o deliberazione competente, con indicazione della versione precedente, della nuova versione e delle ragioni della modifica.

Articolo 84 – Interpretazione

Le disposizioni del presente Manuale devono essere interpretate in conformità al Regolamento n. 20/MSP e agli altri atti applicabili del MSP.

Articolo 85 – Clausola di salvaguardia

Nessuna disposizione del presente Manuale può essere interpretata come:

- dichiarazione di esistenza di riserve;
- attestazione di fondi disponibili;
- certificazione di solvibilità;
- prova automatica della titolarità di beni;
- autorizzazione all'esercizio di attività riservate;
- riconoscimento di una garanzia da parte di soggetti terzi;
- certificazione di convertibilità di ZEC, LIS o wZEC;
- ordine di pagamento;
- prova di avvenuto regolamento.

Articolo 86 – Entrata in applicazione

Il Manuale costituisce specifica tecnico-organizzativa di riferimento dalla sua approvazione da parte dell'organo SIPSE competente.

La sua applicazione informatica è subordinata alla realizzazione, al collaudo e all'eventuale autorizzazione dei sistemi e dei servizi necessari.

ALLEGATO A

MODELLO STANDARD DELLA SCHEDA RMG

Identificazione

- RMG-ID:
- Versione:
- Data di registrazione:
- Partecipante:
- Codice partecipante:
- Responsabile istruttoria:

Descrizione della garanzia

- Denominazione:
- Categoria:
- Tipologia:
- Descrizione:
- Garante:
- Beneficiario:
- Dichiarante:
- Eventuale custode:

Dati economici

- Valore dichiarato:
- Unità di riferimento:
- Data di valutazione:
- Fonte:
- Valore documentato:
- Valore verificato:
- Valore prudenziale:
- Coefficiente prudenziale:

Dati giuridici

- Titolo della garanzia:
- Legge applicabile:
- Data di costituzione:
- Data di scadenza:
- Vincoli:
- Gravami:
- Condizioni:
- Stato del perfezionamento:

Classificazione

- Livello: V0 / V1 / V2 / V3
- Stato:
- Data dell'ultima verifica:
- Verificatore:
- Limitazioni:
- Note:

ALLEGATO B

MODELLO DEL FASCICOLO DIGITALE

Ogni fascicolo deve contenere:

1. domanda di registrazione;
2. identificazione del dichiarante;
3. documentazione della garanzia;
4. documentazione del garante;
5. eventuale documentazione del beneficiario;
6. attestazioni di custodia;
7. valutazioni;
8. verifiche;
9. autorizzazioni;
10. comunicazioni;
11. eventi;
12. verbali;

13. storico delle versioni.

Ogni file deve essere associato a un codice, una data, un autore, una tipologia e un'impronta crittografica.

ALLEGATO C

MATRICE DEI LIVELLI DI EVIDENZA

Requisito	V0	V1	V2	V3
Dichiarazione	Sì	Sì	Sì	Sì
Fascicolo documentale	Parziale	Sì	Sì	Sì
Controllo formale	Non necessario	Sì	Sì	Sì
Verifica sostanziale	No	Non necessariamente	Sì	Sì
Verifica del titolo	No	Non necessariamente	Secondo il caso	Sì, ove richiesta
Verifica disponibilità	No	No	Non necessariamente	Sì
Perfezionamento	Non attestato	Non attestato	Non necessariamente	Documentato
Utilizzo come copertura	No	Non automatico	Solo se ammesso	Nei limiti verificati

ALLEGATO D

MODELLO DEL REGISTRO DEGLI EVENTI

Campo	Contenuto
Event ID	Identificativo evento
RMG-ID	Garanzia interessata
Timestamp	Data e ora
User ID	Utente responsabile
Role ID	Profilo autorizzativo
Event Type	Tipo di operazione
Previous State	Stato precedente
New State	Nuovo stato
Reason	Motivazione
Evidence	Riferimenti documentali
Result	Esito
Integrity Hash	Impronta del record

ALLEGATO E

MODELLO DI INTEROPERABILITÀ CON LA CMCRP

Messaggio informativo esemplificativo:

```
{
  "message_type": "RMG_COVERAGE_STATUS",
  "message_version": "1.0",
  "source_system": "RMG",
  "target_system": "CMCRP",
  "reference_id": "SIPSE-RMG-PAT-VT963-G05-2026-000001",
  "evidence_level": "V2",
  "registration_status": "VERIFIED",
  "prudential_value": {
    "amount": 0,
    "unit": "DSPP",
    "valuation_date": "2026-11-16"
  },
  "availability_status": "SUBJECT_TO_VALIDATION",
  "restrictions": [],
  "issued_at": "2026-11-16T12:00:00Z"
}
```

Nota: il messaggio è un esempio di struttura tecnica. Il valore pari a zero è un dato segnaposto e non rappresenta una garanzia reale. La trasmissione non produce automaticamente ammissione della copertura o regolamento di un'obbligazione.

ALLEGATO F

MATRICE DEI PERMESSI

Operazione	ADM	REG	VER	VAL	AUD	LEG	READ
Gestione utenti	Sì	No	No	No	No	No	No
Inserimento domanda	Sì	Sì	No	No	No	No	No
Acquisizione documenti	Sì	Sì	Sì	No	No	No	No
Verifica documentale	No	No	Sì	No	No	Sì	No
Valutazione prudenziale	No	No	No	Sì	No	Consultazione	No
Modifica livello	No	No	Proposta	Autorizzazione	No	Parere	No
Consultazione audit	No	No	No	No	Sì	No	No
Consultazione ordinaria	No	Limitata	Limitata	Limitata	Sì	Limitata	Sì

I permessi definitivi devono essere configurati secondo il principio del minimo privilegio.

ALLEGATO G

PIANO MINIMO DI TEST

Test	Descrizione	Risultato atteso
T01	Inserimento nuova garanzia	RMG-ID generato
T02	Domanda incompleta	Richiesta integrazione
T03	Documento duplicato	Segnalazione
T04	Verifica V1	Registrazione esito
T05	Tentativo V3 senza evidenze	Blocco
T06	Modifica valore	Nuova versione
T07	Garanzia scaduta	Allerta
T08	Garanzia contestata	Stato contestato
T09	Duplicazione esposizione	Segnalazione
T10	Accesso non autorizzato	Rifiuto
T11	Modifica log	Rilevazione anomalia
T12	Ripristino backup	Verifica integrità
T13	Scambio CMCRP	Conferma tecnica
T14	Quotazione SMQVM	Acquisizione fonte e data
T15	Interruzione API	Gestione errore

ALLEGATO H

MODELLO DI RAPPORTO DI ANOMALIA

Identificativo anomalia:

RMG-ID interessato:

Data e ora:

Soggetto segnalante:

Categoria:

- documentale;
- giuridica;
- patrimoniale;
- monetaria;
- informatica;
- sicurezza;
- interoperabilità;
- altra.

Descrizione:

Evidenze disponibili:

Impatto potenziale:

Misura cautelativa:

Responsabile della gestione:

Esito:

Data di chiusura:

ALLEGATO I

CHECKLIST DI RILASCIO

Prima dell'eventuale passaggio in ambiente PROD devono risultare verificati:

- ☒ architettura approvata;
- ☒ modello dati validato;
- ☒ ruoli e permessi configurati;
- ☒ autenticazione testata;

- ☒ protezione dei documenti verificata;
- ☒ audit trail attivo;
- ☒ backup verificato;
- ☒ ripristino collaudato;
- ☒ test funzionali completati;
- ☒ test di sicurezza completati;

- ☐ interfacce validate;
- ☐ anomalie critiche risolte;
- ☐ documentazione aggiornata;
- ☐ responsabili nominati;
- ☐ provvedimento di attivazione adottato.

ALLEGATO L

MODELLO DI RAPPORTO PERIODICO RMG

Il rapporto periodico deve contenere almeno:

1. numero totale delle registrazioni;
2. distribuzione per categoria;

3. distribuzione V0–V3;
4. numero di garanzie attive;
5. numero di garanzie sospese;
6. numero di garanzie scadute;
7. valore dichiarato complessivo;
8. valore documentato complessivo;
9. valore verificato complessivo;
10. valore prudenziale riconoscibile;
11. esposizioni collegate;
12. anomalie aperte;
13. verifiche scadute;
14. garanzie prossime alla scadenza;
15. variazioni significative;
16. incidenti informatici;
17. raccomandazioni operative.

I valori aggregati devono essere accompagnati da criteri di calcolo, data di riferimento e indicazione dei dati non verificati.

ALLEGATO M

MATRICE DELLE RESPONSABILITÀ

Attività	Responsabile primario	Controllo
Presentazione domanda	Partecipante	Ufficio RMG
Acquisizione	Ufficio RMG	Responsabile Registro
Verifica documentale	Verificatore	Responsabile istruttoria
Verifica giuridica	Funzione legale	Responsabile competente
Valutazione patrimoniale	Valutatore	Funzione di controllo
Attribuzione V2/V3	Organo autorizzato	Audit
Gestione informatica	Amministratore	Responsabile sicurezza
Interoperabilità	Responsabile tecnico	Responsabile sistema
Controllo periodico	Funzione di controllo	Organo competente

ALLEGATO N

MODELLO DI VERSIONAMENTO

Versione	Data	Descrizione
1.0	16 novembre 2026	Prima emissione del Manuale tecnico n. 21/MSP

Ogni successiva revisione dovrà riportare le modifiche apportate, la motivazione, l'organo proponente e l'organo approvante.

DISPOSIZIONE CONCLUSIVA

Il Registro Multilaterale delle Garanzie costituisce una componente informativa e di controllo del Mercato Sovrano dei Popoli, destinata a rendere più trasparente e verificabile il rapporto tra garanzie, coperture ed esposizioni.

La sua funzione non consiste nel creare garanzie mediante la registrazione, ma nel documentare, classificare e monitorare quelle effettivamente dichiarate e, ove possibile, verificate secondo la relativa disciplina.

La credibilità del sistema dipende dalla qualità delle evidenze, dalla separazione delle responsabilità, dalla tracciabilità dei procedimenti, dalla correttezza delle valutazioni e dalla capacità di distinguere ciò che è dichiarato da ciò che è documentato, verificato, perfezionato e concretamente disponibile.

Il principio operativo del RMG è pertanto:

NESSUNA GARANZIA SENZA IDENTIFICAZIONE; NESSUNA COPERTURA SENZA EVIDENZA; NESSUNA VALORIZZAZIONE SENZA METODO; NESSUNA DISPONIBILITÀ SENZA VERIFICA.

S.I.P.S.E. – Sistema delle Istituzioni dei Popoli per la Sovranità Economica

MERCATO SOVRANO DEI POPOLI – MSP

Manuale tecnico n. 21/MSP – SIPSE/MSP/MAN/2026/21 – Versione 1.0