DOMUSCAN — Descrizione del progetto

> Sintesi ragionata dei documenti in `documenti per analisi/`. Spiega **cosa** deve fare DOMUSCAN, **come** deve farlo e **in che modalità** opera. Per la sequenza di lavoro vedi PIANO_IMPLEMENTAZIONE.md.

---

1. In una frase

DOMUSCAN è un **layer di certificazione indipendente** che si affianca al gestionale dell'amministratore di condominio (es. Danea Domustudio) e rende **ogni voce di spesa del rendiconto verificabile tramite un QR Code**, che porta il condomino alla fattura originale, integra e autorizzata. Lo fa **senza toccare il gestionale**: niente API, niente accesso al database, niente plug-in.

Formula sintetica dei documenti:

```
GESTIONALE = CONTABILITÀ
DOMUSCAN   = DOCUMENTO + ASSOCIAZIONE + VERIFICA + ACCESSO
```

---

2. Il problema che risolve

- Il rendiconto condominiale elenca le spese, la fattura (oggi quasi sempre FatturaPA XML via SdI) è il documento fiscale. **I due documenti non "si parlano"**: nessun terzo può verificare che una riga corrisponda proprio a quella fattura.
- Se un condomino ha un dubbio deve chiamare lo studio e ricostruire a mano la catena delibera → fattura → intervento → prezzo.
- Il gestionale conserva internamente il legame movimento-allegato, ma **non lo espone** in modo utilizzabile da terzi.
- Esiste il rischio (umano o tecnico) che il documento pubblicato sia provvisorio, non aggiornato o alterato.

3. A chi si rivolge

Soggetto	Cosa ottiene
Amministratore (cliente pagante)	Certezza che ogni importo rendicontato è legato a un documento originale immodificabile; meno telefonate di chiarimento; servizio distintivo da offrire.
Condomino / revisore	Inquadra il QR sul bilancio (cartaceo o PDF) e vede la fattura e la scheda della spesa, solo se autorizzato.
Produttori di gestionali	Non sono concorrenti né controparti: DOMUSCAN completa la loro offerta. Eventuali integrazioni ufficiali arrivano dopo, come servizio esterno opzionale.

Il prodotto si vende **all'amministratore**, non alla software house del gestionale.

Made with Markdown Inline Preview

4. Principi non negoziabili

1. **Indipendenza dal gestionale.** Nessun processo critico può richiedere API, login, database o formati proprietari del gestionale. DOMUSCAN lavora solo su ciò che l'utente può fare normalmente: importare/registrare fatture, scrivere in un campo causale/note, stampare o esportare PDF/CSV. Gli adapter verso gestionali specifici sono moduli opzionali: se si rompono, il flusso a file continua a funzionare.
2. **Fail-closed.** In assenza di certezza deterministica sull'abbinamento spesa-documento **il QR non viene generato**. Il sistema non sceglie mai "il candidato più probabile" pubblicandolo come certo. *Criterio di accettazione: zero associazioni automatiche errate. La precisione prevale sulla copertura.*
3. **Il documento originale non si altera.** Il PDF arricchito può aggiungere livelli grafici, richiami o pagine indice, ma non può coprire o modificare testi, importi, saldi, millesimi o totali.
4. **Il QR non è un'autorizzazione.** Contiene solo un URL con un identificativo casuale, opaco, non enumerabile e revocabile. Nessun importo, nome, dato personale o URL diretto al file.
5. **Tracciabilità totale.** Ogni dato estratto conserva la provenienza (file, pagina, coordinate o riga XML, metodo, versione del parser). Ogni conferma, rettifica, pubblicazione e accesso finisce in un log append-only.
6. **Veridicità.** Nessun numero (benchmark, confidenza, badge "verificato") viene mostrato come risultato finché non è calcolato e supportato da evidenze. Se i dati non bastano, si dichiara "dati insufficienti".

---

5. Come funziona — il flusso operativo

Il protocollo si chiama **DIBP — DOMUSCAN Independent Binding Protocol**. Idea chiave: DOMUSCAN **non indovina** quale fattura il gestionale ha allegato; **conosce la relazione fin dall'inizio** perché la crea lui, nel proprio registro, nel momento in cui la fattura entra nello studio.

Fase A — Acquisizione (automatica)

1. La fattura entra in DOMUSCAN **prima o insieme** all'import nel gestionale, da un canale osservabile (vedi §6).
2. DOMUSCAN conserva l'originale immutabile, calcola l'**hash SHA-256**, estrae i dati fiscali, propone il condominio destinatario.
3. Crea un **Document ID** interno immutabile e un **Binding Token** breve (es. `DSN-K7M4-P9Q2`).
4. L'amministratore riceve una notifica: "Hai N documenti pronti per la registrazione".

Fase B — Registrazione (il "ponte", unico gesto manuale)

5. Mentre registra la fattura nel gestionale, l'operatore incolla nel campo **causale / descrizione / note / protocollo** una causale pronta preparata da DOMUSCAN negli appunti, es.: `[DSN-K7M4-P9Q2] Manutenzione pompa centrale termica - fatt. 184/2026`
6. Il movimento resta nel gestionale, il legame (binding) resta in DOMUSCAN.

Fase C — Finalizzazione (il "timbro")

7. A fine periodo l'amministratore stampa il consuntivo in PDF **come sempre**.
8. Lo invia a DOMUSCAN (upload, cartella `DOMUSCAN_OUT` o **stampante virtuale**).
9. Il **Print Layer** ricostruisce le righe del rendiconto, trova i token, li risolve nel registro, esegue i controlli e applica i QR sulle righe (ed eventualmente rimuove il token dalla versione per i condomini).

Made with Markdown Inline Preview

10. Le righe senza prova sufficiente restano **senza QR** e compaiono nella **Review Console**.

Fase D — Verifica (lato condomino)

11. Il condomino inquadra il QR → apre il **resolver** (es. `https://verify.domuscan.it/b/<codice-opaco>`).
12. Il resolver verifica binding, diritti dell'utente, stato del documento e **integrità dell'hash**; se tutto torna mostra la **scheda spesa** con il documento in un visualizzatore sicuro. Se il file è stato alterato anche di un bit, la visualizzazione viene bloccata.

---

6. Modalità operative

6.1 Canali di acquisizione (in ordine di preferenza)

Canale	Note	Priorità
XML FatturaPA (SdI, provider, PEC, cartella)	Dati strutturati, nessun errore di lettura	Massima
PDF nativo / copia di cortesia	Fallback per fatture non XML	Alta
Casella email dedicata / inoltro PEC	Cattura allegati in automatico	Alta
Cartella sorvegliata (`DOMUSCAN_IN`)	Locale o cloud drive	Alta
Upload manuale multi-file / drag & drop	Fallback universale, sempre disponibile	Media
Scansione + OCR	Solo cartaceo o immagini	Residuale

Regola: ogni documento che deve diventare evidenza **deve passare da almeno un canale osservabile**. In onboarding si mappano i canali reali dello studio e se ne misura la copertura. La stessa fattura arrivata da più canali **non si duplica** (dedup per ID fiscale → hash del contenuto canonico → fingerprint semantico, conservando tutte le provenienze).

6.2 Modalità di aggancio (Binding Bridge)

Modalità	Descrizione
A — Token in causale (raccomandata, universale)	L'operatore incolla il token nel campo descrizione/riferimento/note.
B — Assistente appunti / overlay desktop	Piccola app desktop che prepara la causale negli appunti e mostra "Incolla in causale". Non legge né modifica il gestionale.
C — File "carrier"	Copia di lavoro con il token nel nome file (`DSN-…_Fattura_184_2026.xml`). Segnale aggiuntivo, mai unico.
D — Protocollo esterno	Se il gestionale ha un campo "protocollo", DOMUSCAN fornisce un progressivo mappato sul Document ID.

6.3 Ordine di riconciliazione di una riga del rendiconto

1. Binding Token esplicito
2. Protocollo DOMUSCAN

Made with Markdown Inline Preview

3. Chiave fiscale canonica completa: `CF/P.IVA destinatario + CF/P.IVA fornitore + tipo doc + numero normalizzato + data + totale + valuta`
4. Combinazione univoca fornitore + numero + data + totale
5. Matching probabilistico → **solo proposta all'operatore, mai pubblicazione automatica**

6.4 Livelli di decisione

Livello	Condizione	Azione
A — Deterministico	Token valido nel Binding Registry	Associazione automatica
B — Deterministico fiscale	Chiave fiscale canonica unica	Associazione automatica con audit
C — Forte ma non univoco	Più candidati o dati incompleti	Conferma obbligatoria
D — Debole	Solo importo/descrizione simili	Nessuna associazione, solo proposta
E — Incoerente	Importo, destinatario o hash non coerenti	Blocco e segnalazione

6.5 Casi complessi

- **Una fattura su più voci** (es. stessa fattura ripartita tra scala A e scala B): si genera **un solo QR** legato alla fattura e lo si copia su tutte le voci **solo se** hanno la stessa chiave fattura (numero|fornitore|data normalizzati) **e la somma delle voci è uguale al totale al centesimo**. Altrimenti nessuna voce riceve il QR: o chiude tutto il gruppo, o non si copia nulla. In apertura il layer ricontrolla somma e chiave.
- **Più fatture in una voce aggregata**: il QR apre una pagina di riepilogo con l'elenco dei documenti e la somma, che deve coincidere con la voce.
- **Note di credito, acconti/saldi, fatture sostituite**: relazioni esplicite tra documenti, versioning e revoca.
- **Registro molti-a-molti**: ogni associazione ha importo allocato e motivazione; la somma allocata non supera il totale.
- **Correzioni (storni)**: una correzione è **sempre una nuova entry** che punta all'originale; un binding pubblicato non si sovrascrive, si revoca e se ne crea una nuova versione. Il QR punta a un identificativo stabile che risolve sempre la versione valida.

6.6 Il sigillo

Il sigillo lega in modo verificabile la voce di bilancio alla fattura. I documenti ne descrivono due varianti che vanno unificate in fase di progetto:

- **Sigillo con segreto** (schema "la catena che chiude"): `S = hash(Hd + Hs + Hc + k)` dove `Hd` = hash del documento (fisso, mai ricalcolato), `Hs` = hash della registrazione contabile (immutabile), `Hc` = hash della catena di storni, `k` = segreto **non salvato nel database**. Se gli storni puntano all'entry originale e la somma algebrica torna e `Hd` è immutato, S viene ricalcolato e il token resta valido; altrimenti accesso negato, senza intervento di un admin.
- **Sigillo con firma** (bozza brevettuale): hash del file XML + identificativo della voce + timestamp (variante: marca temporale eIDAS) + **firma con chiave privata**, verificabile con la chiave pubblica senza aprire il gestionale.

Made with Markdown Inline Preview

6.7 Revisione (Review Console)

Unica interfaccia in cui l'amministratore interviene attivamente. Mostra contatori (verificate / eccezioni), elenco eccezioni con stato (es. *Ambiguità*, *Token assente*, *Verificato*) e azioni: conferma, rifiuto, associazione manuale, split, merge, rettifica, recupero token. Ogni azione registra attore, data, vecchio/nuovo valore e motivo; le correzioni approvate diventano ground truth per i test.

---

7. Architettura

7.1 Componenti

Componente	Funzione
Intake	Riceve XML, PDF, email, cartelle, upload, stampa virtuale
Document Vault	Conserva originale immutabile + SHA-256, cifrato
Parser / Estrattore	XML FatturaPA strutturato; PDF testo+coordinate; OCR selettivo; parser versionati, ad "adapter" con ancore testuali (es. "Fattura n.") e non template rigidi
Binding Bridge	Token, causale negli appunti, overlay desktop
Binding Registry (sidecar ledger)	Relazioni documento ↔ registrazione ↔ voce, con stati e audit
Matching Engine	Riconciliazione deterministica + proposte
Print Layer / Overlay	Legge il consuntivo, inietta QR/richiami senza alterare l'originale
Review Console	Gestione eccezioni e conferme
Resolver pubblico + Secure Viewer	Verifica QR, autorizzazioni, integrità; scheda spesa
Audit log	Append-only per caricamenti, estrazioni, correzioni, pubblicazioni, accessi

7.2 Stack indicato

- **Backend**: Node.js e/o Python, pipeline asincrona a job (`ingest → parse → match → review → analyse → publish`), job idempotenti e ripetibili.
- **Database**: PostgreSQL (relazionale; un grafo solo se giustificato in futuro). MongoDB Atlas citato come alternativa.
- **Deploy**: Cloud-Native, microservizi in container Docker.
- **Hosting** (a carico del cliente): Google Cloud Run (costo a consumo) oppure Hetzner Cloud / DigitalOcean (costo fisso, UE, GDPR).
- **Client desktop** (Windows): widget/overlay token e, dalla V1, stampante virtuale.
- **Domini**: `domuscan.it` e `domuscan.org` registrati (20/05/2026, Register.it). Il resolver previsto è su `verify.domuscan.it`.

Made with Markdown Inline Preview

7.3 Modello dati minimo

Binding Registry: `binding_id`, `tenant_id`, `condominium_id`, `document_id`, `binding_token`, `ledger_external_ref`, `ledger_date`, `ledger_amount`, `allocation_amount`, `status`, `method` (token / fiscal_key / manual / import), `confidence` (solo diagnostica), `confirmed_by`, `confirmed_at`, `audit_hash`.

Entità canoniche: Tenant, Condominio, Esercizio, Bilancio, Voce, Movimento, Documento, Fornitore, Componente, Categoria, Associazione, Analisi, Benchmark, Utente, AccessGrant, AuditEvent.

Stati del binding: `PROPOSED → VERIFIED → CONFIRMED → PUBLISHED`; qualunque stato → `REJECTED`; `PUBLISHED → REVOKED → nuova versione`.

Stati del documento/voce: `IMPORTED → PARSED → NEEDS_REVIEW / MATCHED → ANALYSED → APPROVED → PUBLISHED` (+ errore e revoca separati).

7.4 API interne previste

`POST /documents` · `POST /documents/{id}/extract` · `POST /bindings` · `POST /bindings/{id}/confirm` · `POST /bindings/{id}/revoke` · `POST /reconcile` · `POST /reports/preflight` · `GET /resolver/{publicCode}` — più webhook firmati per i completamenti.

7.5 Controlli prima della pubblicazione di un QR

Binding `confirmed` · documento non revocato · condominio della riga = destinatario del documento · importo coerente con l'allocazione · hash del file uguale a quello registrato · nessuna anomalia privacy bloccante · policy di accesso e validità definite.

---

8. Sicurezza e privacy

- Cifratura a riposo e in transito, chiavi gestite separatamente, backup e restore testati, scansione malware.
- Separazione logica di tenant (studi) e condomini; **zero accessi cross-tenant** è un requisito assoluto, testato anche alterando gli ID nelle richieste.
- Ruoli: amministratore, collaboratore, condomino, revisore, operatore DOMUSCAN (RBAC/ABAC per condominio e documento). Autenticazione account/OTP (SPID come variante futura).
- Log di visualizzazione/download; retention e cancellazione configurabili; mascheramento dei dati non pertinenti.
- Nessuna attività invasiva sui gestionali (reverse engineering, scraping, accesso al DB): fuori dal perimetro del prodotto.
- Gate legale prima di usare dati reali: ruoli privacy (titolare/responsabile), informative, accordi con studi, eventuale DPIA, trasferimenti a fornitori IA.

---

9. Funzionalità successive all'MVP

- **Scheda spesa intelligente con spiegazione IA**: un LLM spiega la fattura usando **solo** i campi forniti, distingue fatti/ipotesi, non inventa cifre; prompt e modello versionati, difese da prompt injection nei documenti.
- **Tassonomia specialistica** condominiale versionata, con mapping dal piano dei conti originale (mai perso).
- **Congruità / benchmark prezzi**: confronto con prezzari regionali, listini delle Camere di commercio e storico. Calcolo deterministico separato dall'LLM, campione minimo, "dati insufficienti" come fallback. *Corrisponde* (la fattura è quella) ≠ *Congruo* (il prezzo è nel riferimento).

Made with Markdown Inline Preview

- **Anomalie storiche** (duplicati, variazioni improvvise, concentrazione fornitori), sempre come "da approfondire", mai accuse.
- **Integrazione SdI diretta**, API pubbliche, adapter opzionali, white label, SSO.
- **Global Shadow Layer**: espansione internazionale tramite **Country Pack** versionati (formati fattura, ID fiscali, lessico, riparti, privacy) senza modificare il core. 40 giurisdizioni prioritarie in 5 wave (Europa core → Europa estesa → Americhe → APAC → Medio Oriente/Africa), ognuna con gate G0–G5. **L'Italia è il Country Pack di riferimento**: il core va progettato da subito con un modello canonico estendibile.

---

10. Quadro contrattuale ed economico (offerta 21/07/2026)

SAL	Contenuto	Importo
SAL 1 — Fase A	Setup architettura Cloud-Native e database; acquisizione e hash SHA-256	2.500 €
SAL 2 — Fase B	Stampante virtuale/overlay QR; Review Console ed eccezioni	3.000 €
SAL 3 — Fase C	Resolver pubblico; test di accettazione su flussi reali; produzione	2.000 €
Totale	Chiavi in mano, al netto di imposte	**7.500 €**

Durata stimata 10–12 settimane (3 + 4 + 3-4). Fattura emessa a collaudo di ogni milestone. Costi cloud a carico del cliente.

Deliverable richiesti: codice sorgente e istruzioni (installazione, migrazioni, backup, restore, deploy); diagramma architetturale, schema dati, contratti API; corpus di test anonimizzato con ground truth; manuale operatore; piano di osservabilità, incidenti e retention.

---

11. Punti aperti da decidere

I documenti non sono del tutto allineati. Prima di iniziare servono queste decisioni:

1. **Dove sta il file.** L'analisi Basilotta suggerisce il "puntatore certificato" (DOMUSCAN conserva solo hash e link al cloud dello studio); la Specifica DIBP e il Capitolato richiedono un **Document Vault** DOMUSCAN con copia autorizzata e cifrata. *Proposta: Vault come default (garantisce il controllo dell'hash e la disponibilità), puntatore come opzione per tenant.*
2. **Auto-associazione probabilistica.** La Specifica DIBP la vieta (solo proposta); il Capitolato (D04) la ammette sopra una soglia calibrata sul pilota. *Proposta: nell'MVP auto-pubblicazione solo per i livelli A e B; il probabilistico va sempre in revisione.*
3. **Tipo di sigillo.** Hash con segreto `k` fuori DB oppure firma asimmetrica con timestamp (eIDAS). Va scelto anche in base alla strategia brevettuale.
4. **Perimetro MVP rispetto al budget.** L'offerta da 7.500 € copre acquisizione, overlay, console e resolver. Spiegazione IA, tassonomia, scheda intelligente e RBAC completo (indicati come MVP nel Capitolato) vanno ripianificati o quotati a parte.
5. **Autenticazione del condomino** (account, OTP, link a scadenza) e chi gestisce gli inviti.
6. **Corpus pilota**: quali studi, quali gestionali (almeno Danea + un secondo), quanti bilanci e fatture autorizzati.

Made with Markdown Inline Preview

12. Fonti

Documento	Contenuto
`DomusScan.pdf`	Analisi e proposta tecnica (Dott.ssa F. Basilotta): modello "ponte", stack, roadmap A/B/C, pitch, flusso giornaliero, SdI, storage
`DOMUSCAN_Specifica_Tecnica_Associazione_Indipendente.pdf`	Specifica DIBP v1.0 (12/07/2026, Ing. C. Canino): token, registry, livelli decisionali, API, stati, test T01–T12
`Domuscan_Capitolato_Layer_Stampa_Intelligente.pdf`	Capitolato v1.0 (24/09/2026): requisiti A/D/P/I/S/E, priorità MVP/V1/Evoluzione, fasi 0–3, test
`Domuscan_Global_Shadow_Layer.pdf`	Specifica internazionale v1.0: Country Pack, modello canonico globale, 40 paesi, wave e gate
`Schema_rivendicazioni_bilanci_condominiali.pdf`	Bozza per consulente brevettuale: rivendicazioni 1–6 (sigillo, verifica indipendente, congruità, multi-gestionale)
`Offerta economica Domuscan.pdf`	Offerta 7.500 € in 3 SAL
Immagini WhatsApp	"Layer QR — stessa fattura, due voci" e "La catena che chiude" (sigillo e storni)
Email Register.it / NIC	Registrazione domini `domuscan.it` e `domuscan.org`

> Dati sensibili presenti nella cartella (codice auth-info del dominio, coordinate bancarie) **non** sono riportati qui e non vanno committati in un repository.

Made with Markdown Inline Preview