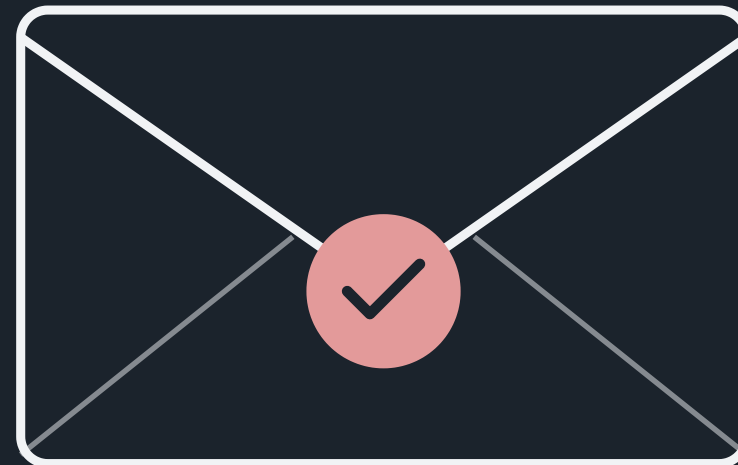


PER LE GARE PUBBLICHE

Deposito cifrato delle offerte tecniche oltre i limiti di Sintel

Il file grande sta qui, chiuso con la chiave della stazione appaltante. Su Sintel va la ricevuta.



Un'offerta tecnica, oggi, spesso non entra nella piattaforma

600 MB

Il limite di Sintel per operatore

In totale per offerta, e 100 MB per singolo file. Elaborati, modelli BIM, relazioni con immagini: la busta tecnica li supera sempre più spesso.

3

I rimedi correnti

Dividere il file, comprimerlo oltre il ragionevole, spedire un supporto fisico. Tutti indeboliscono segretezza e verifica.

0

Garanzie crittografiche

La segretezza fino all'apertura è asserita dal gestore della piattaforma, non dimostrabile da fuori.

Un deposito cifrato a fianco di Sintel, non al suo posto

- Il file è **cifrato nel browser** dell'operatore con la chiave pubblica della gara, generata dalla stazione appaltante nel *suo* browser.
- Il servizio conserva una busta che **non sa aprire**: nemmeno chi lo gestisce, nemmeno chi ha accesso al server.
- L'operatore riceve una **ricevuta** sigillata e marcata temporalmente e la allega su Sintel: la procedura resta dov'è.
- Alla scadenza la gara **si chiude da sola**; la stazione appaltante decifra sul proprio computer.

[Auctio](#) [Come funziona](#) [Stazioni appaltanti](#) [Documenti](#) [Accedi](#) [Registrati](#)

Gara A1B2C3D4E5

Oggetto	Servizio di progettazione esecutiva — lotto 2
Stato	aperta
Scadenza	19/09/2026 13:34 CEST (istante UTC 2026-09-19T11:34:00Z)
Dimensione dei blocchi	1.0 MiB
Dimensione massima del file	10.00 GiB
Volume massimo per operatore	30.0 TiB
Conservazione dopo l'apertura	90 giorni

Impronta della chiave pubblica della gara

697dbcf3b2009ce55718a80c59a98eb10ee047dbd014cdb11cbb78d60c655ffc

Confrontatela con quella riportata nel bando: il file viene cifrato per questa chiave.

[Come funziona](#) [Stazioni appaltanti](#) [Documenti](#) [Trasparenza](#) [Verifica una ricevuta](#) [Informativa sulla protezione dei dati](#)

Chiunque può verificare una ricevuta con auctio-verify, senza la piattaforma. Registro pubblico: auctio.it/log/v1
ThinkDifferent S.r.l. · info@nextlab.net

Quattro passi

1

La chiave

La stazione appaltante la genera nel browser, conserva file e kit di recupero (tre parti, due bastano), pubblica l'impronta nel bando.

2

Il deposito

L'operatore carica il file cifrato, con ripresa automatica; riceve la ricevuta in PDF/A e la allega all'offerta su Sintel.

3

La chiusura

Alla scadenza, al minuto: il verbale elenca ogni deposito, sigillato, marcato, iscritto nel registro pubblico.

4

L'apertura

La stazione appaltante decifra sul proprio computer; ogni scarico è notificato; l'esito — integro o no — è registrato.

Per costruzione, non per promessa



Segretezza fino alla scadenza

AES-256-GCM a blocchi nel browser; chiave di sessione avvolta con la chiave RSA-4096 della gara. Il server vede dimensioni e istanti, mai il contenuto.



Integrità e data certa

Ogni ricevuta: impronta SHA-256, sigillo Ed25519 del gestore, marca temporale RFC 3161, PDF/A-3 per Sintel. Il verbale di chiusura, lo stesso.



Verificabile da chiunque

Registro trasparente pubblico (albero di Merkle, checkpoint firmati, ancorati su Bitcoin). Verifica nel browser o con `auctio-verify`, senza il servizio.

Nessun cambio di procedura, nessun software

- Un browser: la chiave si genera e si usa lì.
- Tre righe nel disciplinare: l'indirizzo della gara, l'impronta della chiave, la ricevuta nella busta tecnica.
- Prima della scadenza: niente da fare, niente da vedere.
- All'apertura: file della chiave (o due parti del kit), scarico e decifratura sul proprio computer, esito integro / non integro verbalizzato.
- Anni dopo: il verbale si verifica ancora, da chiunque.

[Auctio](#) [Le mie gare](#) [Il mio account](#) Connesso come rup (stazione appaltante) [Esci](#)

Apertura dei depositi — gara A1B2C3D4E5

Servizio di progettazione esecutiva — lotto 2 — [chiusa](#)

I depositi vengono decifrati in questo browser e salvati sul vostro disco. Il file della chiave e la passphrase non lasciano il browser. Ogni scarico è registrato e notificato all'operatore.

✓ Chiave aperta. Scegliete un deposito da decifrare.

I file vengono salvati dove indicate, in streaming.

Deposito	Operatore	Dimensione	Esito
✓ 7cfe55296ca4238797bea846b9e77c0 ricevuta	7ae84617f8bea79c1e868cbd72e4774e	6.0 MIB	✓ Integro: offerta-tecnica.zip (SHA-256 ea49b2ef683b3a48062a82c05c51dcd275a133999abf6ffcfce302798f43f42d8)

[Decifra e salva](#)

Apertura completata

Quando tutti i file sono stati consegnati alla commissione, chiudete l'apertura: parte il periodo di conservazione, dopo il quale i cifrati vengono distrutti.

[Dichiara completata l'apertura](#)

[Come funziona](#) [Stazioni appaltanti](#) [Documenti](#) [Trasparenza](#) [Verifica una ricevuta](#) [Informativa sulla protezione dei dati](#)

Chiunque può verificare una ricevuta con auctio-verify, senza la piattaforma. Registro pubblico: [auctio.it/log/v1](#)

ThinkDifferent S.r.l. · [info@nexlab.net](#)

Registrarsi, depositare, allegare la ricevuta

- Registrazione con partita IVA (verificata su VIES), PEC, e-mail; accesso con codice via e-mail.
- Il file non lascia mai il computer in chiaro; il caricamento riprende da dove si era interrotto.
- La ricevuta in PDF/A prova cosa è stato depositato e quando, e vale da sola.
- Notifica a ogni scarico da parte della stazione appaltante.

 **Auctio** [I miei depositi](#) [Il mio account](#)

Connesso come rossi-costruzioni (operatore economico) [Esci](#)

Deposito per la gara A1B2C3D4E5

Servizio di progettazione esecutiva — lotto 2 — Scadenza: 19/09/2026 13:34 CEST
(2026-09-19T11:34:00Z)

Impronta della chiave pubblica della gara:

697dbcf3b2009ce55718a80c59a98eb10ee047dbd014cdb11cbb78d60c655ffc

Confrontatela con quella riportata nel bando: il file viene cifrato per questa chiave.

Il file viene cifrato in questo browser con una chiave casuale, che a sua volta viene cifrata per la chiave pubblica della gara. Il gestore riceve solo il cifrato.

✓ Deposito 7cfe55296ca4238797bea8466b9e77c0 registrato. Scaricate la ricevuta in PDF e allegatela all'offerta su Sintel come dichiarazione di deposito: contiene il record sigillato, verificabile da chiunque.

[Scarica la ricevuta \(PDF\)](#) [Ricevuta in JSON](#)

[Come funziona](#) [Stazioni appaltanti](#) [Documenti](#) [Trasparenza](#) [Verifica una ricevuta](#) [Informativa sulla protezione dei dati](#)

Chiunque può verificare una ricevuta con auctio-verify, senza la piattaforma. Registro pubblico: auctio.it/log/v1
ThinkDifferent S.r.l. · info@nextlab.net

Ciò che serve per non fidarsi di noi

- **Registro pubblico** in formato standard (tlog-tiles), origine e chiave di verifica pubblicate, prove di inclusione e coerenza.
- **Ancoraggio su Bitcoin** (OpenTimestamps) di ogni tree head: riscrivere il passato lascia traccia.
- **Il codice che cifra**: moduli serviti con le impronte SHA-256 pubblicate, nessuna libreria di terzi, nessun codice in linea.
- **Software libero** (EUPL 1.2), build riproducibile: il binario in produzione è confrontato byte per byte con una compilazione indipendente.
- Verifica indipendente nel browser e con `auctio-verify` (Linux, macOS, Windows).

Verifica di una ricevuta di deposito

Questa pagina verifica una ricevuta o un verbale di chiusura di Auctio con lo stesso codice dello strumento `auctio-verify`, nel browser, senza inviare nulla: i file restano su questo computer. Funziona anche da disco, con la piattaforma spenta.

Verificatore pronto: `auctio wp-17-2-g2d5da53-dirty (2d5da53, 2026-09-19)`
ricevuta.pdf → ricevuta-7cfe55296ca4238797bea846b9e77c0.json - chiavi dal file keys.json

File da verificare

Ricevuta di deposito (il PDF allegato su Sintel, o il JSON)

ricevuta.pdf

Verbale di chiusura (PDF o JSON, facoltativo: verifica che elenchi la ricevuta)

No file chosen

File originale dell'offerta (facoltativo: verifica l'impronta dichiarata)

offerta-tecnica.zip

Chiavi pubbliche del gestore

Il file `keys.json` (GET /log/keys) va conservato da una fonte diversa dalla ricevuta: dal giorno del bando, dal sito del gestore, da un verbale precedente.

File delle chiavi

keys.json

Senza un file delle chiavi verranno usate quelle pubblicate da questo stesso server (127.0.0.1:8635): valide solo quanto il server.

☒ Accetta marche e ancoraggi finti (solo installazioni di sviluppo)

VERIFICATA: ogni passo è superato

ok	seal — canonical, hashed, sealed by 4af9b79eacd25b5d...
ok	checkpoint — origin auctio.it/log/v1, size 1, signed by auctio.it/log/v1
ok	inclusion — leaf 0 of 1
ok	timestamp — FAKE token from a development adapter: no evidential value
ok	plaintext — SHA-256 ea49b2ef683b3a48062a82c05c51dcd275a133999abf6ffc302798f43f42d8
skip	tree head — no anchored tree head in the export yet: download it again once one covers the leaf

Un passo **skip** non è stato verificato (gli ancoraggi sulle catene richiedono la rete): il dettaglio dice cosa cercare su un explorer pubblico. Lo strumento `auctio-verify` li verifica con `--bitcoin-api` e `--evm-rpc`.

Auctio - auctio wp-17-2-g2d5da53-dirty (2d5da53, 2026-09-19) - EUPL-1.2

Cosa è protetto, da chi, e cosa resta a chi

MINACCIA	DIFESA	RESTA A
Il gestore, o chi ha accesso al server, legge un'offerta prima della scadenza	impossibile: la chiave privata non è mai stata sul server	—
Un deposito viene alterato o sostituito	ogni blocco autenticato e legato alla posizione; impronta nella ricevuta; esito «non integro» all'apertura	—
Il gestore antedata o cancella un deposito	marca temporale di un terzo; registro a sola aggiunta ancorato su Bitcoin; ricevuta in mano all'operatore	—
La stazione appaltante apre prima della scadenza	il servizio non serve i blocchi prima della chiusura; ogni scarico è registrato e notificato	la custodia della chiave (come per ogni piattaforma)
Il computer dell'operatore o della stazione appaltante è compromesso	—	a loro: il file è in chiaro lì, prima e dopo
Perdita della chiave della gara	file della chiave verificato prima della pubblicazione; kit di recupero 2 su 3	alla stazione appaltante

Piccolo da gestire, difficile da rompere

Un binario, due container

Go, PostgreSQL 16, podman rootless, filesystem in sola lettura, nessun privilegio. Un host qualsiasi con nginx davanti; in esercizio su auctio.it.

Si controlla da solo

Ogni notte: ricalcolo dell'impronta di ogni deposito, verifica dei registri contro l'ultima testa ancorata, archivio cifrato. Ogni lavoro con esito nella pagina del gestore.

Fornitori sostituibili

Marca temporale RFC 3161 (qualificata eIDAS), OpenTimestamps, SMTP/PEC, VIES: adattatori, configurazione, nessun contratto vincolato al software.

Fase A in esercizio; la fase B è disegnata

Oggi (0.1, settembre 2026)

- Deposito, ricevute, chiusura, apertura, registro, ancoraggio, verifica, PDF/A
- Audit di sicurezza completo, 17 rilievi risolti
- Suite di manomissione: ogni attacco del modello rilevato da fuori
- Prova di carico: 600 MB × 40 in parallelo su rete limitata
- In produzione su auctio.it

Prossimi passi

- **SPID / CIE / CNS** per l'accesso; la ricevuta con l'identità di chi deposita
- **Riconciliazione con Sintel**: il Documento d'offerta firmato, con l'impronta della ricevuta, abbinato al deposito all'apertura
- Marca temporale qualificata del fornitore scelto dall'ente
- Fase B: il percorso verso la piattaforma certificata (regole AgID)

CONTATTI

auctio.it

Il sito, i manuali, la trasparenza, la verifica.

Per attivare una stazione appaltante:

info@nexlab.net

ThinkDifferent S.r.l. · Software libero, licenza EUPL 1.2 · Il codice, i documenti e le impronte di ogni versione sono pubblicati.