The Encryption Key Escrow

—

Context

Mini-grid operators running SparkMeter or SteamaCo equipment should not depend only on the survival of a single company to keep their purchased and installed meters working and be able to access them. The A2EI and EnAccess, as part of the “smart metering crisis response consortium,” developed an Escrow model to provide a solution for the above. The Escrow model is an approach where a nonprofit organization (the Escrow Agent) holds the keys as a safe harbor for the companies for any future access requests.

Under an agreement signed by EarthSpark Meter Ops, LLC and Access to Energy gGmbH (A2EI), the public open source release of ThunderCloud 2.0 tech stack, a royalty-free license for SparkNet-HTTP, a communications tool that enables direct communication with SparkMeter meters, and the release and transfer to an Escrow structure of encryption keys after operator approval has been agreed.

This document describes the aim and details of the transfer and deposit of SparkMeter meter encryption keys under the Escrow structure.

What the Escrow generally is for

A copy of the encryption keys needed to communicate with deployed SparkMeter meters is placed with an independent, non-commercial **Escrow Agent** (currently A2EI), provided key transfer to the Escrow Agent has been approved by the Mini-grid operator.

Encryption keys cannot simply be published the way source code can. Anyone holding them can generate valid tokens and commands for the meters they cover, which would expose operators to fraud and service disruption if published.

An Escrow is the mechanism that mitigates this risk. A custodian holds a secure copy of the keys. Any operator that wants direct control of its own meters can retrieve the keys for its meters through a simple, free process that does not depend on anyone’s commercial discretion or on the company's existence. In the meantime, the Escrow Agent and EarthSpark work through the keys that have more than one owner, so that these too can eventually be released in a way that is safe for everyone deployed on them.

The Escrow is a safety net, not a change of service. In short, the Escrow aims to deliver:

- **Continuity.** Meters can keep working regardless of what happens to any single company.
- **Control.** Operators can choose and control whether an encryption key copy to their meters shall or shall not be deposited with the Escrow Agent.
- **Choice.** With key access, operators can stay on the managed service, self-host, or migrate to the Open Metering Stack (OMS) — and can change their mind later.

- **Fair access.** The same process, the same timelines, and no fee for every operator. No operator needs permission from EarthSpark to ask for its keys.
- **Safety.** Keys are protected in transit and at rest, and are never published while multi-owner risks remain unresolved.

EarthSpark continues to maintain and support the commercial service, and Encryption Keys can also be directly requested by the operator from EarthSpark. It is possible to have the encryption keys in escrow and also transferred directly to the operator if wished. A key copy sitting in escrow changes nothing about the day-to-day operations EarthSpark can provide, but it provides the operators a choice and additional safety.

The Escrow Agent's costs are covered under the Open Metering Crisis Response, as anticipated overheads are not passed on to operators. (Exceptions are where keys are shared by sites/organisations that do not belong to the same entities, due to company split-ups or mergers. In such cases, additional effort is required. Most of these efforts will be covered by the funding for the open metering infrastructure solution, but a basic commitment fee will apply to the companies: $750 if <500 meters are involved and $1250 if >500 meters are involved).

The Escrow Agent may be replaced over time — for example by another entity deemed better-positioned by the involved stakeholders, a professional escrow provider, or by the long-term governance home of the OMS — and any successor inherits the same obligations and the same audit trail.
A technically more detailed description of the process is available here.

How the process works

Stage 0 — Approval of deposit by Grid Operator (25th of September 2026)

To allow the meter owner/grid operator ("*operator*") to take advantage of the additional safety net provided by the escrow model, written approval must be submitted via this form to EarthSpark and the Escrow Agent. The operator's written approval authorizes EarthSpark to transfer a copy of the encryption keys for the operator's meters to the Escrow Agent and notifies the Escrow Agent of the approval.

Approving the transfer does not change anything operationally — it simply means a protected backup copy of the keys exists outside EarthSpark's own systems. A first batch of Encryption Keys is transferred on the 25th of September, subject to operator approval.

Operators who do not provide the approval now maintain the option to transfer their keys to escrow in the future; their keys remain exclusively with EarthSpark until an approval for transfer is submitted. Additional transfers will be organized in batches at a later stage. Timing of those transfers will be communicated at a later stage.

Stage 1 — Deposit (by 28th of September 2026)

EarthSpark places an encrypted copy of the Encryption Keys with the Escrow Agent, together with an index that records which keys correspond to which meters, sites, and operators.

Every operator whose keys have been transferred to it is written to directly, and the Consortium Escrow Agent maintains a public page describing the process.

Stage 2 — Retrieval (starting from 5th of Octobre)

Any operator can ask the Escrow Agent for the keys covering the meters it operates. The steps are:

Step	Who	What happens
1	Operator *(or designated trustee)*	Submits a single Key Request form to the Escrow Agent, listing the meters or sites concerned, attaching reasonable evidence of deployment, and enclosing a signed Operator Undertaking.
2	Escrow Agent	Acknowledges receipt within 2 working days and forwards the request to EarthSpark for a cross-check against its operator records.
3	EarthSpark	Within 7 working days, either confirms the operator's identity and the scope of the deployment, or raises a specific factual objection. No response within 7 working days counts as confirmation.
4	Escrow Agent	Once the request is confirmed and any cross-operator security issue has been cleared, releases the keys within a further 3 working days over an encrypted channel agreed in advance. EarthSpark is notified of the release, and the release is recorded in the audit log.
5	Operator *(or designated trustee)*	Countersigns a short acknowledgment of receipt, and can from that point operate the relevant meters independently of any SparkMeter cloud service.

EarthSpark's role at Step 3 is limited to confirming the facts of the deployment and flagging any multi-owner key risk. It is not an approval step. If a factual question cannot be settled between the operator and EarthSpark within 10 working days, it is referred to the Consortium for a non-binding opinion, after which the Escrow Agent decides. There is no fee at any stage.

In parallel, the possibility for EarthSpark customers to request their keys directly from EarthSpark remains available, while EarthSpark is able and willing to do so.

What the operator commits to

An operator retrieving keys signs a short undertaking: to use the keys only for its own deployed meters or to migrate them to the OMS, to store them securely and restrict access to named staff, not to pass them on, and to report any suspected compromise promptly. Because keys can damage a fleet if mishandled, the operator assumes responsibility for their security once they are received.

Accessing keys directly from EarthSpark Meter Ops or pulling keys out of escrow will trigger a change to the terms of the Operator's customer agreement(s) with EarthSpark Meter Ops.

Oversight

The Escrow Agent keeps an audit log of every access and every release, publishes a quarterly summary of activity, at least to EarthSpark and the Consortium, and notifies affected parties and the Consortium within seven days of any suspected compromise. Operators are named beneficiaries of the access rights described here.

The escrow agent, in its capacity as escrow agent, is strictly a secure lockbox for the safekeeping of the keys. It does not itself gain rights to use the keys or view or use the data for any purpose other than the safekeeping of keys on behalf of the grid operators.

ANNEX: Technical Note – SparkMeter Meter

—

1. Scope: what "Encryption Keys" means here

The escrowed material is the cryptographic material in EarthSpark's custody that is required to communicate with, or to generate valid tokens or commands for, deployed SparkMeter meters. Under the agreement, this covers:

Material	Function	Why it matters
Communication encryption keys	Protect the SparkNet link between head-end and meter.	Required for legitimate two-way operation; also the credential that prevents an unauthorised head-end from talking to a fleet. Confidentiality and integrity of metering traffic.

One property of this material drives the whole design of the Escrow.

It is not always single-owner. SparkMeter was built as a closed ecosystem in which one company operated the entire head-end. Encryption keys were made unique for each operator ; but throughout the life of a utility, mergers, acquisitions and asset sales resulted in change of ownership for assets. In some cases, these situations resulted in assets now operated by separate entities, but using the same keys. As a result, some escrowed keys cover meters belonging to more than one operator. This is the single biggest technical obstacle to simply handing every operator its keys on request, and it is why the Escrow exists as an intermediate step rather than as a one-off distribution exercise.

2. Why the keys are not published

The ThunderCloud 2.0 software is published because publication is exactly what makes it durable. Keys are the opposite case. Published issuer or vendor material would allow any third parties to generate valid meter commands, leading to temporary service disruption and poor network performance. The agreement is explicit that keys are subject to release *in principle*, but that unrestricted publication is not the route.

The Escrow substitutes controlled, verified, per-operator release for publication.

3. Custody arrangements

Deposit. EarthSpark deposits an encrypted copy of the key set with the Escrow Agent, together with a written index mapping keys to meters, sites and operators. EarthSpark does not transfer material it is not legally permitted to transfer. Before an operator's keys are copied into escrow, EarthSpark obtains that operator's written confirmation of the transfer.

Storage. The Escrow Agent holds the material:

- encrypted at rest, on a system that is not exposed to the public internet;
- accessible only to a small, named set of authorised personnel;
- under an audit log that records every access and every release, including recipient, scope, date and method.

The Escrow Agent is held to the standard of care it applies to its own most sensitive credentials, and must act without preference between operators.

Incidents. Any suspected compromise of escrowed material is notified without delay, and in any event within seven days, to EarthSpark, the consortium members (A2EI, EnAccess Foundation) and the affected operator.

Reporting. The Escrow Agent publishes a quarterly summary — requests received, approved and refused, aggregate keys released, any incidents — redacted so that operator identities and sensitive material are not disclosed. The full audit log is available to EarthSpark and the consortium on request.

Continuity. The escrowed material and the audit log stay with the Escrow Agent role. If the role passes to another body, both transfer with it, so the release process and its history are unaffected

4. Verification and release

Verification is deliberately factual rather than discretionary. An operator's request establishes:

1. **Who is asking** — the legal entity, its country of registration, and an authorised signatory.
2. **What is being asked for** — meter IDs, site identifiers, utility names, or whatever else uniquely identifies the deployment.
3. **Evidence of deployment** — a service contract with SparkMeter or EarthSpark, deployment or installation records, a statement from EarthSpark, or equivalent.

EarthSpark then cross-checks against its own operator records. Its input is confined to two things: confirming or disputing the factual scope of the deployment, and flagging whether any requested key is multi-owner material. Silence for seven working days is treated as confirmation, which prevents the process from stalling. Unresolved factual disputes go to the consortium for a non-binding opinion, after which the Escrow Agent decides, acting reasonably.

Transfer. Keys are released over an encrypted channel agreed with the operator in advance of the release — typically PGP-encrypted mail against a public key whose fingerprint has been verified out of band. Key material is never sent in plaintext, and never over email or chat without encryption. The operator countersigns a short acknowledgment of receipt, which closes the audit entry.

5. Multi-owner keys and the de-coupling workstream

Where requested material covers only the requesting operator's meters, release is straightforward. Where it does not, releasing it as-is would give one operator credentials that reach another operator's fleet.

The escrow period is therefore also a working period. The Escrow Agent and EarthSpark are working through the index to establish, per key, which operators are in scope, and to identify where operator-specific credentials can be issued in place of shared ones — so that a request can be satisfied at the narrowest scope that is technically possible rather than at the widest scope that happens to exist today. Requests touching shared material are progressed as that work resolves, not refused; operators in this position are told which category their request falls into and why.

Operators should expect that in some cases the durable answer is re-keying rather than release of legacy material.

6. What an operator should have in place before requesting keys

Retrieval transfers real risk to the operator, who accepts responsibility for the security of the keys once received. Before requesting, an operator should be able to answer:

- **Where will the keys live?** Encrypted storage — a hardware security module, or at minimum a properly managed secrets store or credential vault. Not a shared drive, not a spreadsheet, not a chat thread.
- **Who can reach them?** A small number of named individuals, with access recorded, and a documented procedure for adding and removing people.
- **What happens if that person leaves?** Custody documentation and a recovery copy held under equivalent protection, so the operator does not create a new single point of failure inside its own organisation.
- **What happens on suspected compromise?** A named contact, and an obligation to notify the Escrow Agent within seven days.
- **What are the keys for?** Under the Operator Undertaking, keys may be used only to operate the operator's own deployed equipment. They may not be used against meters the operator does not run, and may not be redistributed, outside of affiliates, contractors, hosting providers, and service providers bound by the same terms and precautions.

An operator that is not ready to meet this standard is better served by leaving its keys in escrow. The keys will still be there.