UNIVERSITAT ROVIRA i VIRGILI

21st International Workshop on Data Privacy Management

A Privacy-Preserving Architecture for Secure Appliance-Level Demand Response in Virtual Power Plants

DPM 2026

Joan Ferré-Queralt · Jordi Castellà-Roca · Alexandre Viejo
Nicolás Orduz Álvarez · Takao Tsuji

Universitat Rovira i Virgili, Spain
Yokohama National University, Japan

Presenter
Joan Ferré-Queralt

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
Cofinanciado por la Unión Europea
AGENCIA ESTATAL DE INVESTIGACIÓN
Crises data security & privacy

From grid need to trusted appliance-level response

The argument follows the research question from motivation to guarantees.

1 INTRODUCTION

Why the grid needs distributed demand flexibility

Need

2 SYSTEM OVERVIEW

Who participates, what is stored, and how the protocol runs

Design

3 EVALUATION

Functional coverage, privacy, and security

Assess

4 CONCLUSIONS

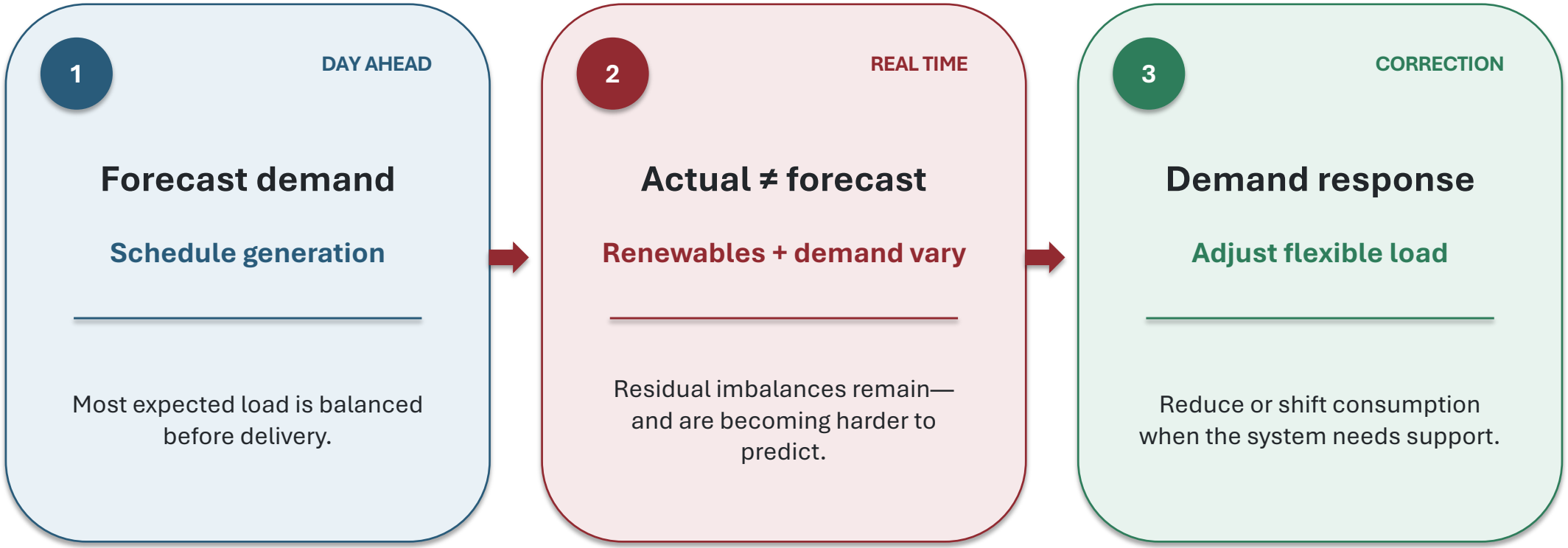
What the architecture establishes—and what remains

Takeaway

Can small appliances provide flexibility without exposing or misusing user behavior?

The grid must continuously balance supply and demand

Most expected demand is balanced one day ahead—but the forecast is never exact.

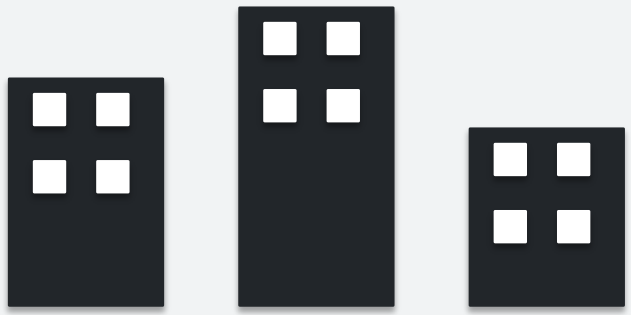


More renewables + rising consumption → greater need for responsive demand-side flexibility

See Kundur et al. (2007), Njoka et al. (2024), and Yolcan (2023).

Traditional demand response is effective—but coarse-grained

TRADITIONAL MODEL



A few large industrial loads

The grid can interrupt contracted processes when needed and compensate the participant—but control is available only in large blocks.

RECENT DIRECTION

APPLIANCE-LEVEL MODEL

HVAC

EV

WATER HEATER

FRIDGE

PUMP

Many small flexible loads

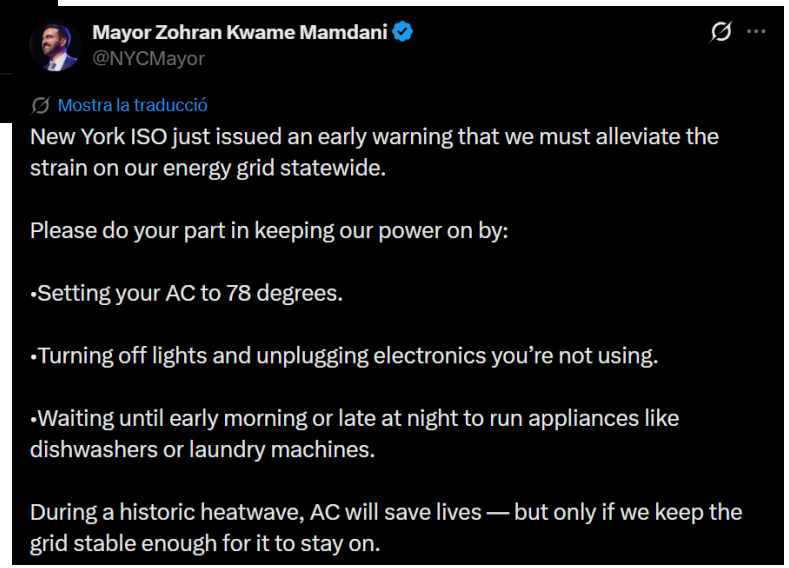
HVAC and other user appliances can briefly curtail consumption when extra balancing is required.

The opportunity shifts from a few MW-scale sites to many kW-scale resources.

Does appliance-level demand response sound far-fetched?

Public calls to reduce air-conditioning during peak demand already happen.

During an extreme heat event, millions of users were asked to change consumption at the same time to protect the grid.



SECTION 02

System Overview

02

Actors, components, and the end-to-end protocol lifecycle

Five actors separate ownership, coordination, and trust

Each role sees and controls only the information needed for its function.

U — USERS

Choose availability and comfort limits.

A — APPLIANCES

Act as OpenADR VENs; curtail and sign with an HSM.

VPP — VIRTUAL POWER PLANT

Aggregates flexibility, schedules events, and acts as OpenADR VTN.

RA — REGISTRATION AUTHORITY

Verifies devices, assigns clusters, and manages pseudonyms.

M — MANUFACTURER

Provisions trusted hardware and certified appliance credentials.

The VPP coordinates operations; the RA retains the identity-to-pseudonym mapping.

A complete privacy-preserving DR workflow

The design connects registration, scheduling, activation, verification, and remuneration.

1

Availability

Routines and occupancy may be inferred.

Encrypt reports and use pseudonyms.

2

Activation

Forged commands can disrupt operation.

Authenticate each scheduled event.

3

Evidence & payment

Forged or reused claims can misdirect rewards.

Verify signed delivery before payment.

Goal: coordinate every DR stage while limiting disclosure of user-specific information.

Paper: §§1.1–1.2 and §2.3. Prior work is summarized qualitatively.

Four components turn private appliance choices into schedulable flexibility

Encrypted detail stays off-chain; verifiable coordination stays on-chain.

FLEXIBILITY CLUSTER — $\theta_c = (P_c, max_c, rec_c)$

Groups appliances with compatible power and operating constraints.

CLUSTER SMART CONTRACT — $CSC_{(c)}$

Stores authorized pseudonyms, CIDs, schedules, event hashes, and payment state.

OPERATIONAL PSEUDONYM — $(Addr, pk^{op})$

Lets each appliance participate without publishing its owner's identity.

IPFS — Encrypted availability

Stores encrypted reports while only their content identifiers appear on-chain.

Together: appliance-level privacy with cluster-level scheduling and event-level accountability.

Setup and registration

One-time system setup is followed by registration of each appliance.

1 SYSTEM SETUP

Deployment

VPP + RA

Keys and certificates

VPP

Clusters and smart contracts

Manufacturer

HSM + certified appliance key

→

2 APPLIANCE REGISTRATION

Create a pseudonym

Create an address and key pair.

Blockchain address + operational public key

Private signing key stays inside the appliance's HSM.

→

3 REGISTRATION AUTHORITY

Authorize its use

Verify

Certified appliance + signature

Assign

A compatible flexibility cluster

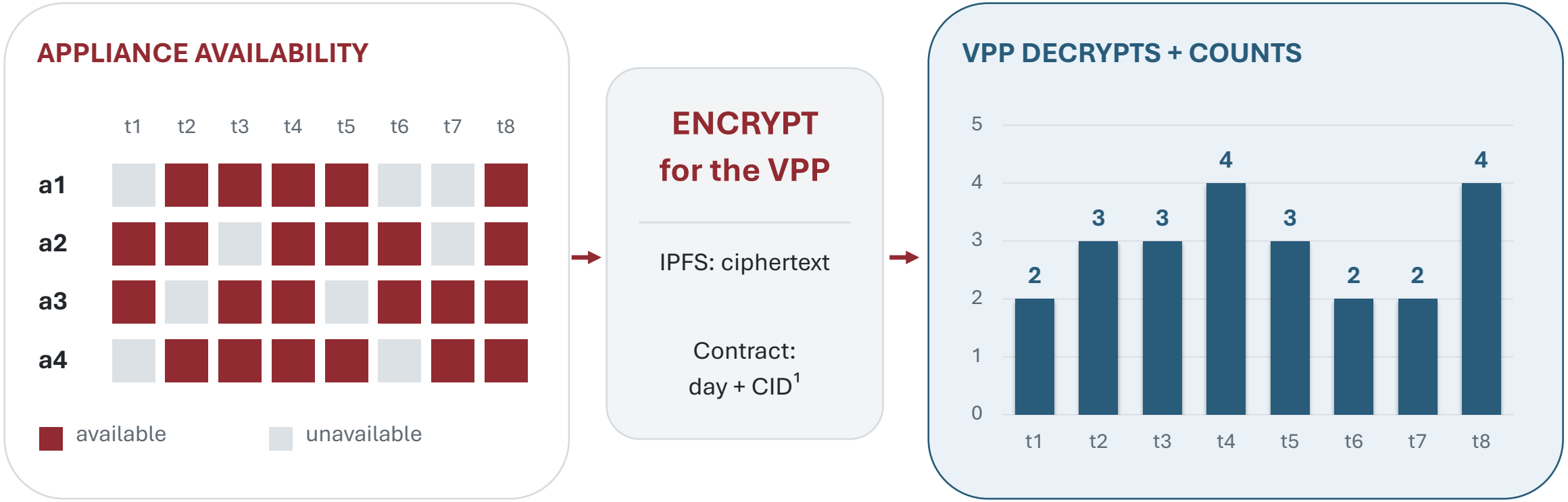
Register

Address + public key in the cluster smart contract

RA keeps the user ↔ pseudonym mapping. The VPP operates with the pseudonym.

Encrypted reports

Illustrative example: the VPP counts available appliances in each time slot.

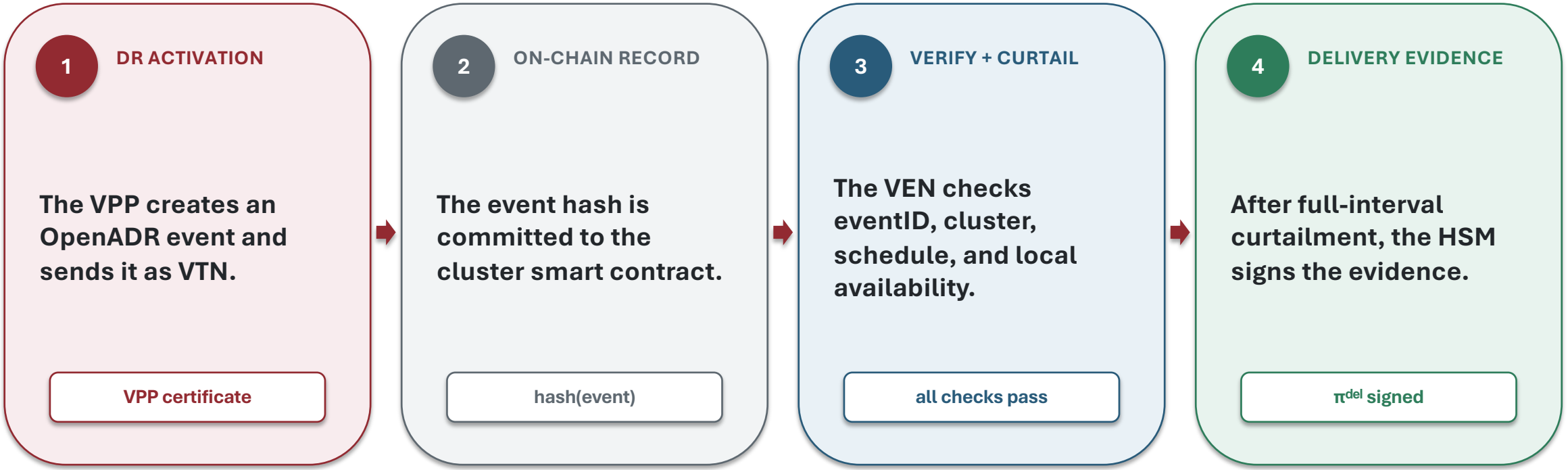


Available cluster power: $A_{c,d}[t] = N_{c,d}[t] \times P_c$

[1] CID = content identifier. Records use operational addresses. Slot durations are unspecified in this illustration.

A scheduled event becomes signed proof of delivery

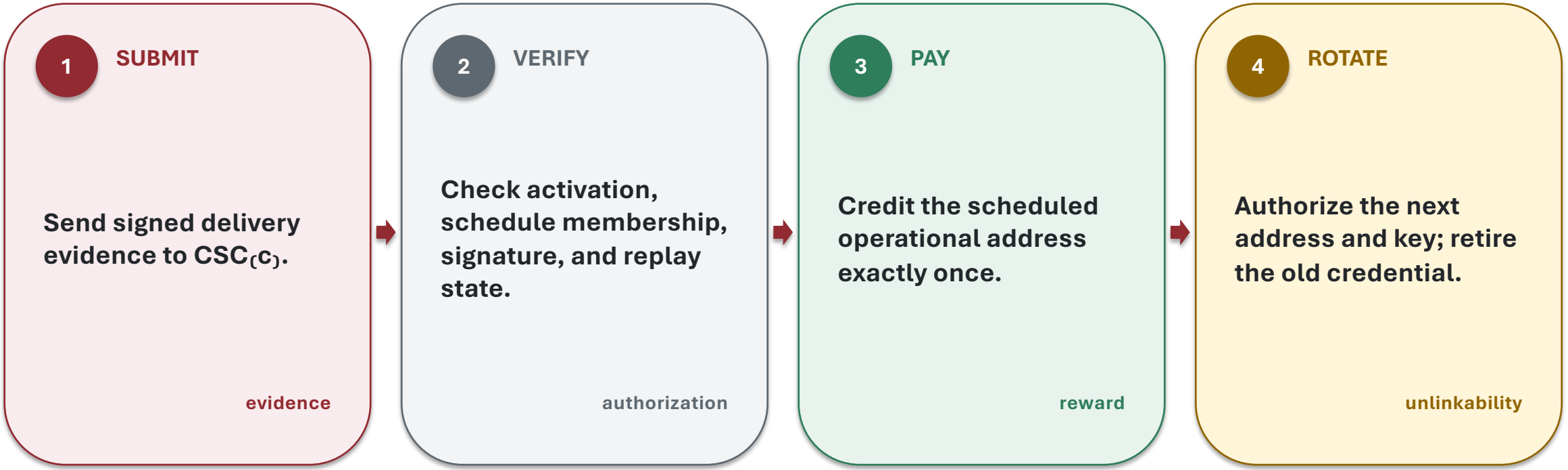
Each transition is authenticated, bound to the schedule, and checked for freshness.



No evidence exists without trusted control; no activation is accepted without schedule-bound checks.

One accepted proof authorizes one reward—and a fresh identity

Payment and credential rotation are bound to the same verified delivery.



The RA processes rotation without publishing an explicit old-address ↔ new-address link.

SECTION 03

Evaluation

03

Functional feasibility, privacy properties, and security requirements

The protocol covers the complete demand-response workflow

The functional assessment traces each required operation to a concrete mechanism.

F1

REGISTRATION + CLUSTERING

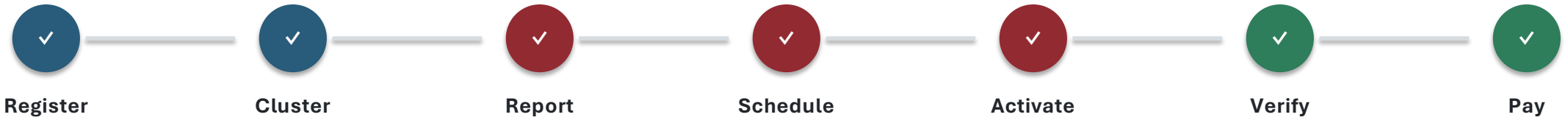
The RA authenticates each appliance and assigns it to a compatible flexibility cluster.

F2

SCHEDULING

The VPP decrypts reports, aggregates availability by slot, and computes cluster-level flexibility.

COMPLETE WORKFLOW



Functional feasibility: every stage from registration to remuneration has an explicit protocol path.

Privacy limits disclosure; security binds actions to authorization

The guarantees are qualitative and depend on the stated trust model.

PRIVACY REQUIREMENTS

P1 — **Availability confidentiality**
Encrypt before storage in IPFS.

P2 — **User–availability unlinkability**
Use operational pseudonyms, not real identities.

P3 — **Activation privacy**
Record pseudonyms and rotate them periodically.

SECURITY REQUIREMENTS

S1	**Authentic activation**	VPP certificate + event hash
S2	**Replay protection**	Fresh event IDs + one-payment state
S3	**Valid evidence**	Registered key + signed evidence
S4	**Authorized payment**	Scheduled address + valid proof

TRUST MODEL • RA trusted • VPP honest-but-curious • no RA–VPP collusion • appliance HSMs trusted

SECTION 04

Conclusions and Future Work

04

What the architecture establishes—and what still needs implementation

1 INTRODUCTION

2 SYSTEM OVERVIEW

3 EVALUATION

4 CONCLUSIONS

Private flexibility, secure control, verifiable reward

One architecture connects the complete appliance-level demand-response lifecycle.

1

PRIVATE FLEXIBILITY

Encrypted availability
Operational pseudonyms

2

AUTHENTICATED CONTROL

OpenADR authentication
Schedule-bound activation

3

VERIFIABLE REWARD

HSM-backed evidence
One-time contract payment

Next: implement the architecture, measure its cost, and integrate VPP schedulers.

Paper: §5 Conclusions. Research support: SAFE/DATA PID2024-156914OB-C42; FPU23/01275.

UNIVERSITAT ROVIRA i VIRGILI

Thank you

Questions?

A Privacy-Preserving Architecture for Secure Appliance-Level Demand Response in Virtual Power Plants

joan.ferreq@urv.cat

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
Cofinanciado por la Unión Europea
AGENCIA ESTATAL DE INVESTIGACIÓN

SAFE/DATA · PID2024-156914OB-C42
FPU23/01275

Crises data security & privacy