

UC6 — Digital Consumer Lifecycle Management

Disclaimer: This is a working version and subject to change. For the latest information, please refer to the India Energy Stack GitHub.

India Energy Stack (IES)

Overview

Field	Value
Use Case ID	UC6
Use Case Name	Digital Consumer Lifecycle Management
Category	Consumer Services & Identity

Problem Statement

Consumer onboarding and lifecycle changes (new connection, transfer, meter changes, role changes from consumer to prosumer) are slow and error-prone. Identity proofing, premise mapping, connection issuance, and meter assignment are handled in disconnected systems, often reconciled manually.

The result: weak, non-verifiable linkage between:

- Who the consumer is
- Where power is delivered
- Which service connection is active
- Which meter is installed
- What the consumer is allowed to do
- What they have consented to share

For prosumers, the gap widens. Asset-linked activation (rooftop solar, net metering), export limits, and eligibility depend on clean identity-premise-connection-meter linkage. These linkages are often implicit, duplicated, or overwritten without history.

When third parties need to verify any of this—aggregators onboarding consumers, banks assessing creditworthiness, programs checking eligibility—they face two paths:

- Bilateral integrations: Costly, $n \times m$ connections, walled gardens

- Manual verification: Paper documents, phone calls, slow and fraud-prone

Solution Approach

Digital Consumer Lifecycle Management defines the end-to-end workflow to onboard and manage grid-connected consumers and prosumers. It covers:

- Application intake
- Identity verification
- Premise mapping
- Service connection issuance
- Meter assignment
- Consent capture
- Asset linkage (for prosumers)
- Service activation
- Lifecycle changes (transfer, tariff change, meter swap, role change)

Verifiable Credentials (VCs) are a core building block. They establish portable, cryptographically verifiable proofs of the linkages and attestations that today exist only as database records or paper certificates.

Before IES vs After IES

Lifecycle Step	Before IES	After IES
Application intake	Paper/forms/portal fragmentation; unclear status	Standard digital intake with status callbacks
Identity proofing	Manual checks; repeated KYC across services	Reusable identity verification credentials
Premise mapping	Unstandardised addresses; duplicates; weak geo-linkage	Match-or-create with GIS + premise credential
Connection issuance	Disconnected steps; manual reconciliation	Utility Customer Credential with verifiable linkage
Meter assignment	Inventory/MDMS/CIS mismatch; overwrites without history	Credential captures meter binding with commissioning trace

Role change to prosumer	Solar activation requires coordinated system updates	Generation Profile Credential issued; consumption credentials unchanged
Consent capture	One-off forms; weak scope/validity evidence	Consent artefacts with revocation + audit trail
Lifecycle changes	Overwrites and inconsistencies across systems	Old credentials revoked, new credentials issued with clear lineage
Third-party onboarding	Each service repeats verification	Consumer presents credentials; verifier checks without issuer contact
Audit and disputes	Hard to prove what was verified, when	Cryptographic receipts with timestamps and trace IDs

Verifiable Credentials as a Building Block

What VCs Solve

Lifecycle Challenge	How VCs Address It
Identity proofing repeated across services	Issue identity verification result as a credential; consumer reuses it
Premise-connection linkage hard to prove	DISCOM issues credential attesting the linkage
Role change (consumer → prosumer)	New credential issued for generation profile; doesn't invalidate consumption credential
Program eligibility verification	Program enrollment credential proves participation without backend queries
Third-party onboarding friction	Consumer presents credentials; verifier checks without contacting issuer
Consent evidence weak	Consent captured as signed artefact with scope, validity, audit trail

Design Principle: Many Credentials, Not One Mega Credential

The objective is not a single monolithic credential. Instead: many granular credentials, each representing a specific attestation.

Credential Type	Issuer	What It Proves
-----------------	--------	----------------

Utility Customer Credential	DISCOM	Consumer number, address, meter, connection date
Consumption Profile Credential	DISCOM	Premises type, connection type, sanctioned load, tariff
Generation Profile Credential	DISCOM	Rooftop solar/DER details, capacity, commissioning
Storage Profile Credential	DISCOM	Battery system for VPP participation
Program Enrollment Credential	DISCOM/Agency	Enrollment in ToD, demand response, PM-KUSUM
Subsidy Eligibility Credential	Government	DBT program eligibility
Equipment Compliance Credential	Testing Lab	Safety and standards certification

VCs also enables selective disclosure: prove specific claims without revealing full data. A prosumer proves subsidy eligibility without exposing consumption history.

Issuance, Holding, Verification

Issuance: Trusted entities (DISCOMs, regulators, certification bodies) cryptographically sign attestations and deliver them to the consumer.

Holding: Consumers store credentials in wallets. They control what to share, with whom, when.

Verification: When a credential is presented, the verifier:

- Validates the cryptographic signature against the issuer's public key
- Checks revocation status
- Authenticates the presenter (binding check)

All without contacting the issuer.

Presenter Authentication

Verifiers must confirm the credential belongs to the presenter—not just that the credential is valid. Supported approaches:

- Wallet-based: Credential bound to wallet; presenting requires proving wallet control

- Verifiable ID seeding: Credential subject includes a DID; presenter proves ownership

Without binding verification, credentials can be replayed by interceptors.

Revocation

When a credential must be invalidated (consumer transfers, meter decommissioned, program ends), the issuer updates their revocation registry. Verifiers check this during verification.

Revocation lists are maintained by issuers themselves. Discoverability uses a public directory protocol like DeDi—verifiers locate the correct revocation endpoint without hardcoded configurations.

```
"credentialStatus": {
  "id": "https://dedi.global/dedi/query/did:web:bescom.karnataka.gov.in/VC_revocation_registry"
  "type": "dediregistry"
}
```

Lifecycle Workflows

New Connection Onboarding

- Consumer submits application (portal/app)
- Identity verification (eKYC or document-based)
- Premise mapping (GIS integration)
- Connection created, meter assigned
- Credentials issued:
 - Utility Customer Credential
 - Consumption Profile Credential
- Consumer stores in wallet

Prosumer Activation

- Consumer installs rooftop solar
- DISCOM verifies installation, commissions net metering
- Additional credentials issued:
 - Generation Profile Credential
 - Program Enrollment Credential (net metering)
- Existing consumption credentials remain valid

Lifecycle Changes

Change Type	Credential Action
-------------	-------------------

Meter swap	New Utility Customer Credential with updated meter; old credential revoked
Tariff change	New Consumption Profile Credential; old revoked
Transfer/move-out	All credentials revoked; new consumer gets fresh credentials
Program enrollment	New Program Enrollment Credential issued
Program exit	Program credential revoked

Third-Party Service Onboarding

- Consumer wants to join demand response aggregator
- Aggregator requests proof of: valid connection, load profile, eligible tariff
- Consumer presents credentials from wallet
- Aggregator verifies (signature, revocation, binding)
- Onboarding completes without backend integration to DISCOM

Example Credentials

Utility Customer Credential

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://nfh-trust-labs.github.io/vc-schemas/energy-credentials/utility-customer-vc/context"
  ],
  "type": ["VerifiableCredential", "UtilityCustomerCredential"],
  "issuer": {
    "id": "did:web:bescom.karnataka.gov.in",
    "name": "BESCOM - Bangalore Electricity Supply Company"
  },
  "issuanceDate": "2025-01-15T10:30:00Z",
  "credentialStatus": {
    "id": "https://dedi.global/dedi/query/did:web:bescom.karnataka.gov.in/VC_revocation_registry",
    "type": "dediregistry"
  },
  "credentialSubject": {
    "id": "did:example:consumer:priya123",
    "consumerNumber": "BESCOM-2025-MR4-567890",
    "fullName": "Priya Sharma",
    "installationAddress": {
      "fullAddress": "42, 3rd Cross, Indiranagar",
      "city": "Bengaluru",
      "stateProvince": "Karnataka",
      "postalCode": "560038"
    },
    "meterNumber": "BESCOM-SM-2025-789456",
    "serviceConnectionDate": "2020-03-15"
  }
}
```

Consumption Profile Credential

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://nfh-trust-labs.github.io/vc-schemas/energy-credentials/consumption-profile-vc/contexts/v1",
  ],
  "type": ["VerifiableCredential", "ConsumptionProfileCredential"],
  "issuer": {
    "id": "did:web:bescom.karnataka.gov.in",
    "name": "BESCOM - Bangalore Electricity Supply Company"
  },
  "issuanceDate": "2025-01-15T10:30:00Z",
  "credentialStatus": {
    "id": "https://dedi.global/dedi/query/did:web:bescom.karnataka.gov.in/VC_revocation_registry",
    "type": "dediregistry"
  },
  "credentialSubject": {
    "id": "did:example:consumer:priyal23",
    "consumerNumber": "BESCOM-2025-MR4-567890",
    "premisesType": "Residential",
    "connectionType": "Single-phase",
    "sanctionedLoadKW": 5,
    "tariffCategoryCode": "LT-2a"
  }
}
```

Stakeholders

Stakeholder	Role
Consumer/Prosumer	Applicant, credential holder, controls sharing
DISCOM	Onboarding authority, primary credential issuer
Regulators	Maintain approved issuer lists, issue license credentials
Certification Bodies	Issue compliance/safety credentials
Aggregators/Third Parties	Verifiers; onboard consumers via credential proofs
Wallet Providers	Secure storage and presentation

Standards and References

- W3C Verifiable Credentials Data Model
- Decentralized Identifiers (DIDs)
- DeDi Protocol — registry discoverability
- IES Energy Credentials Specification