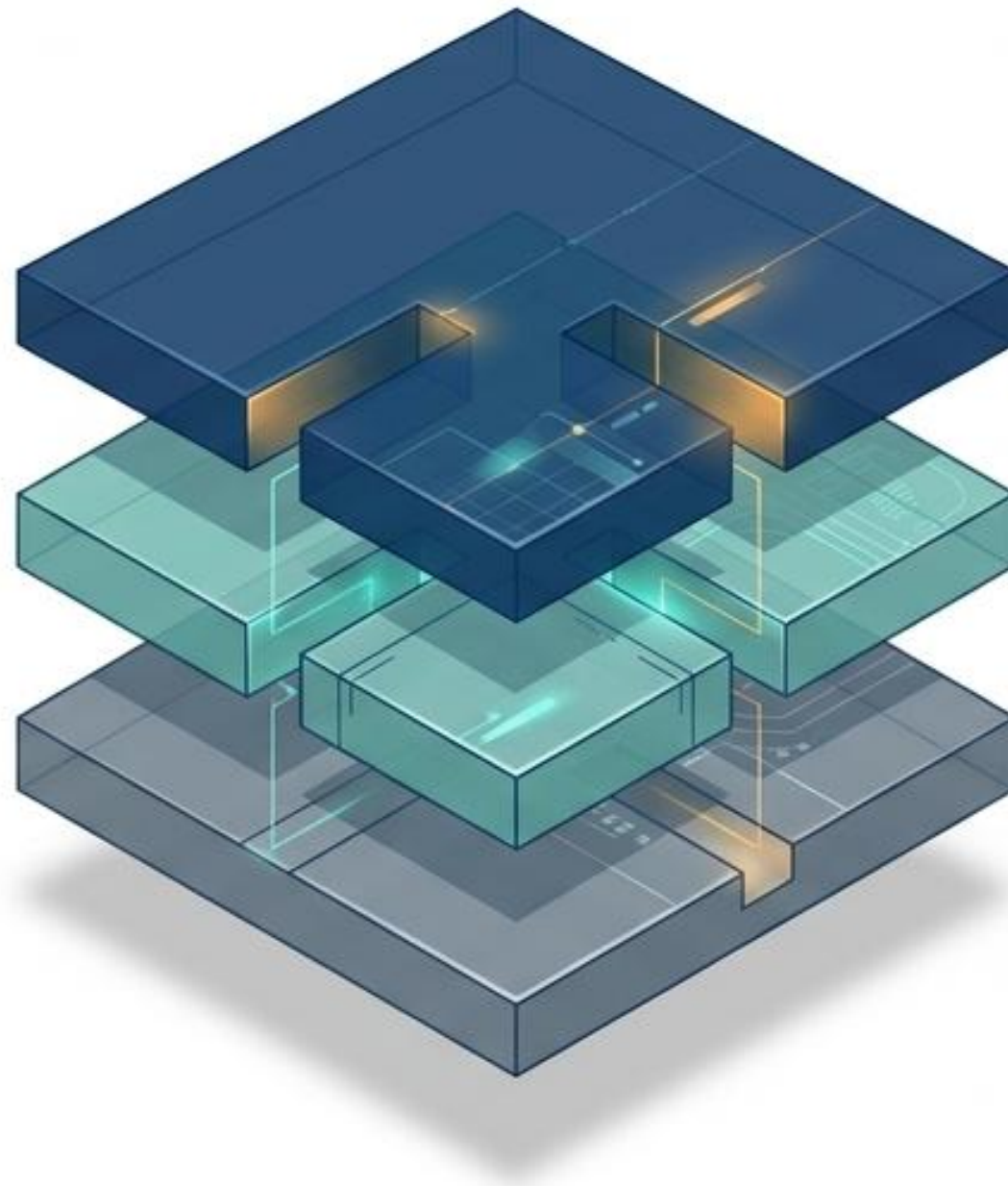


X.dpki: Implementations, industry demand and the standardization way forward



WANG HAIGUANG

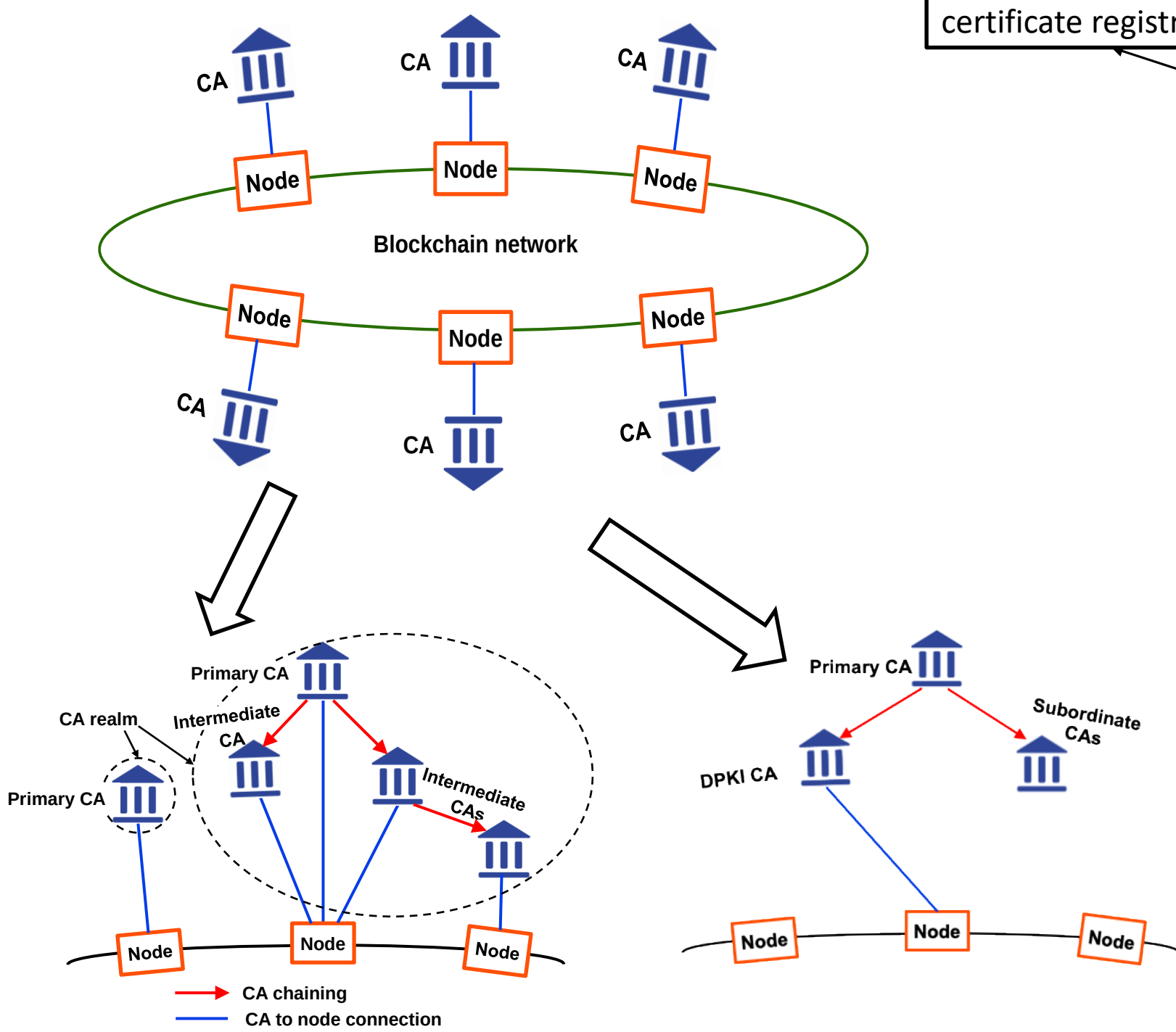
Huawei Technologies

Table of Contents

- **X.dpki draft and prototypes**
- The need from industry
- Potential way forward for the X.dpki recommendation
- Summary

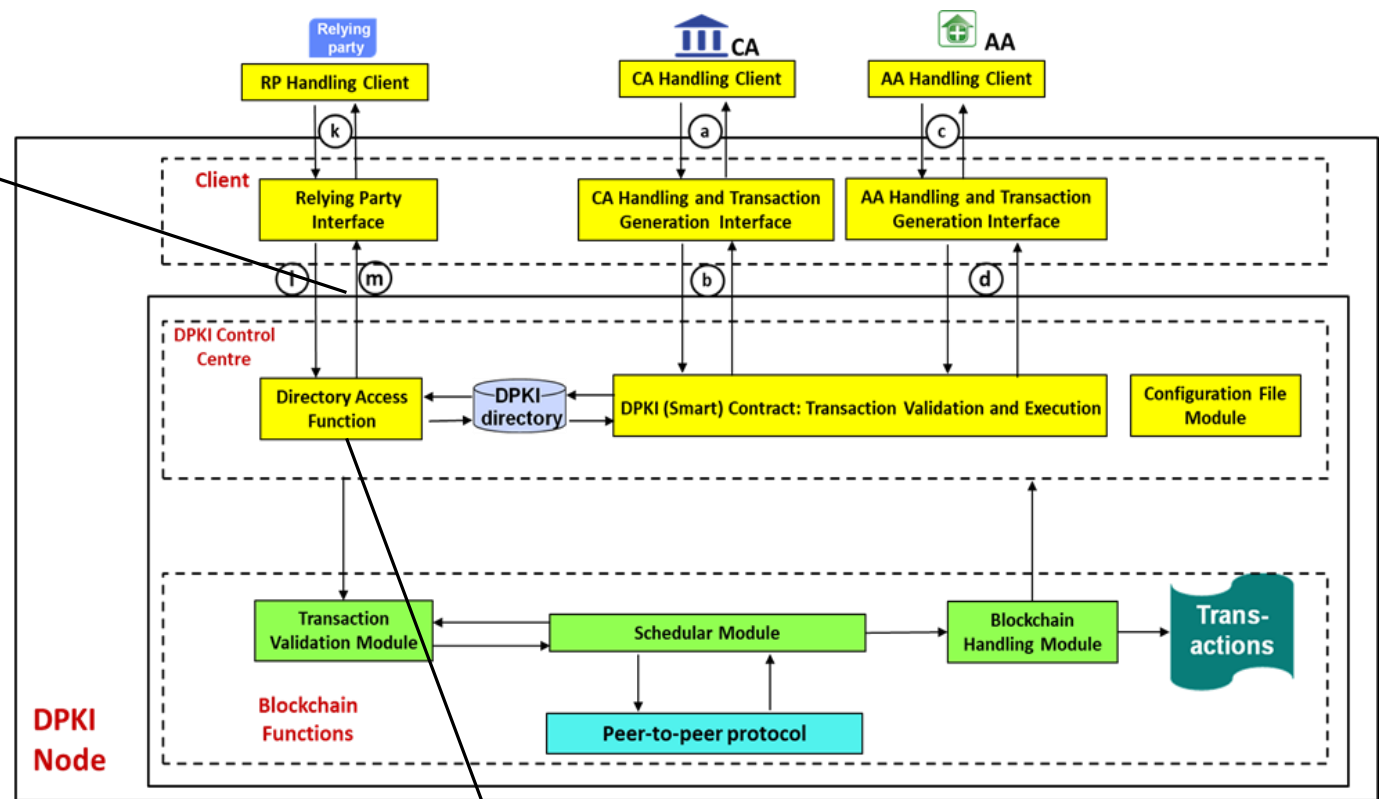
The current status of the X.dpki draft recommendation (the 20th)

Network architecture

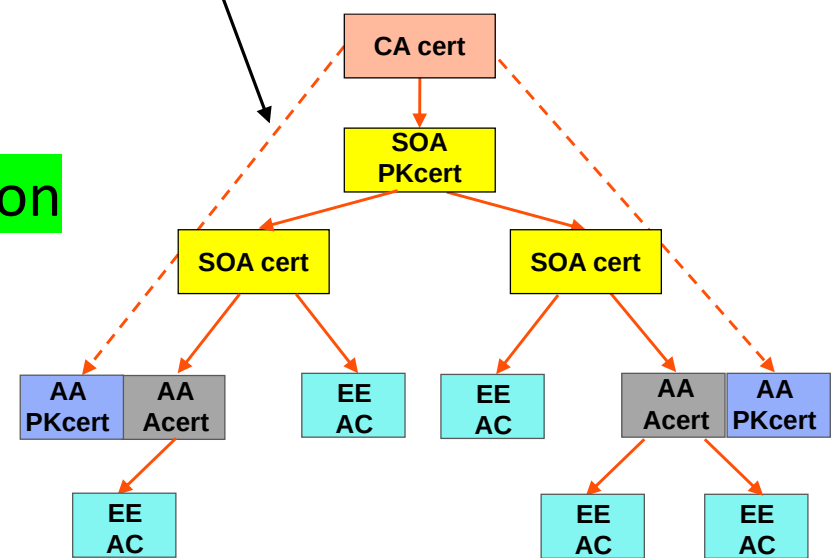


Interfaces for CA and certificate registration

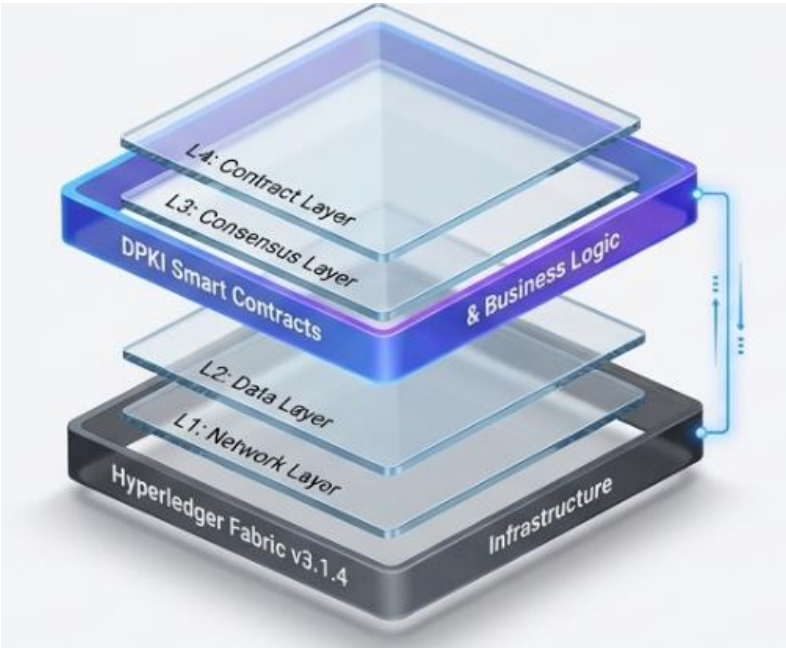
Node Structure



DPKI Direction

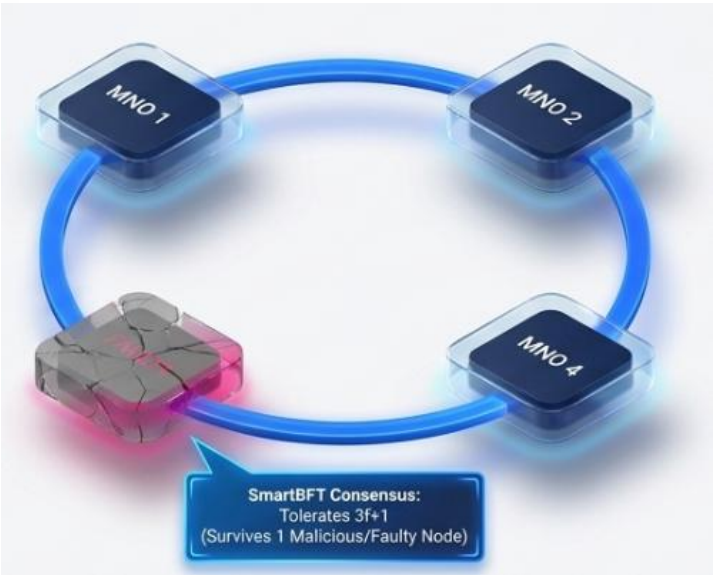
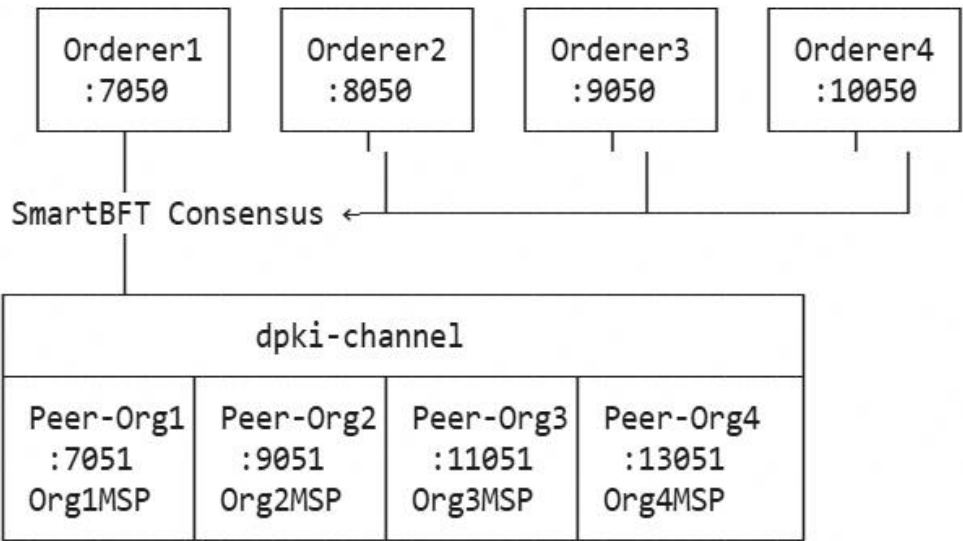


The X.dpki prototype in Hyperledger Fabric: Architecture



L4 – DPKI Management Consensus Layer Governance voting, CA admission, config updates
L3 – Certificate Directory Layer Cert Publish/Query/Revoke/Hold, OCSP Query
L2 – DLT Consensus Layer (SmartBFT) Block ordering, transaction validation, state
L1 – DLT Network Layer (Hyperledger Fabric) Node communication, MSP identity, channel

4-Node SmartBFT Network (Hyper Ledger Fabric)



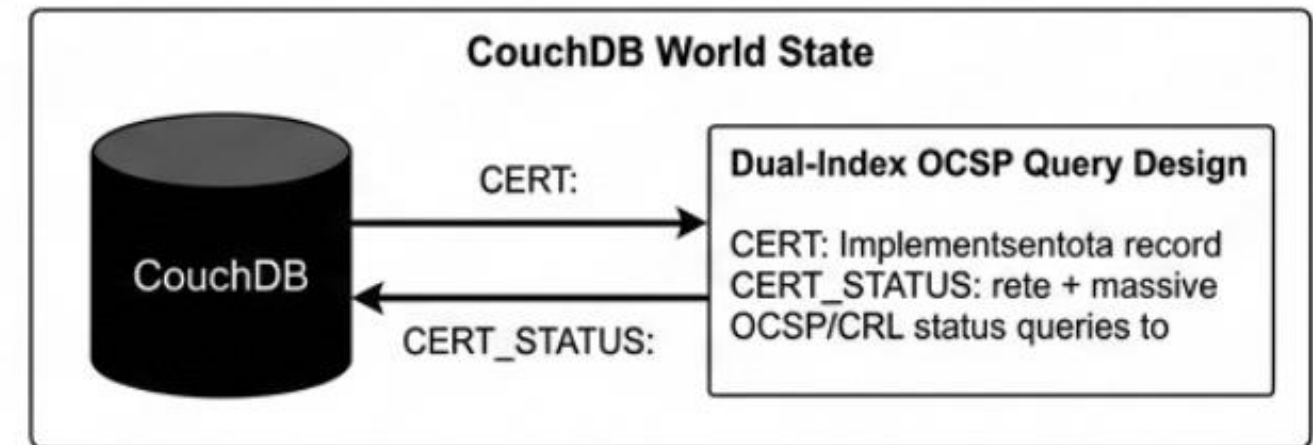
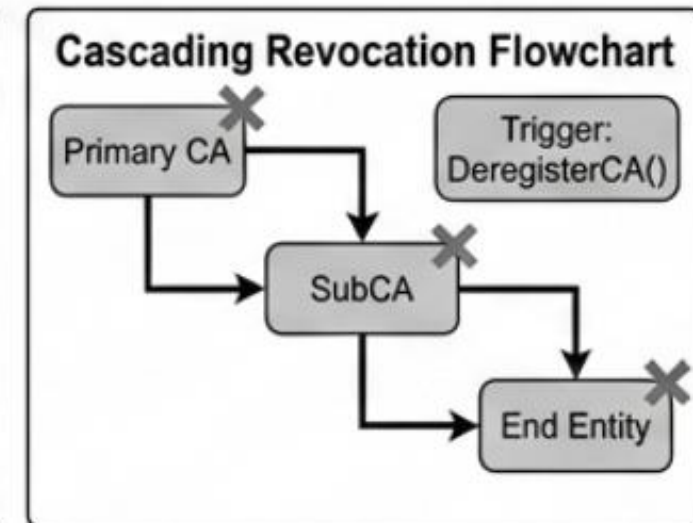
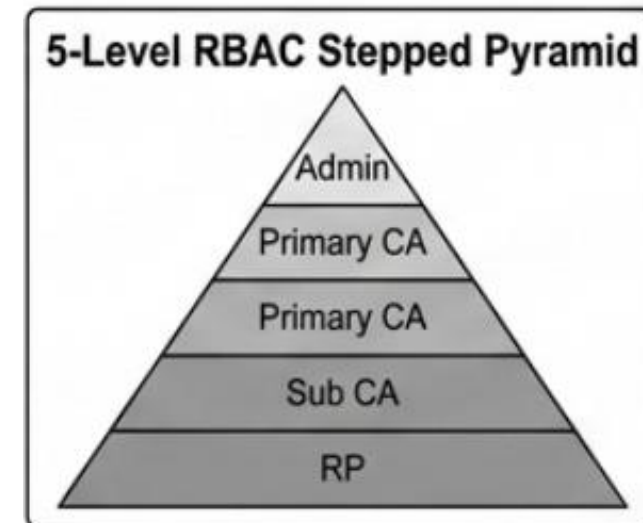
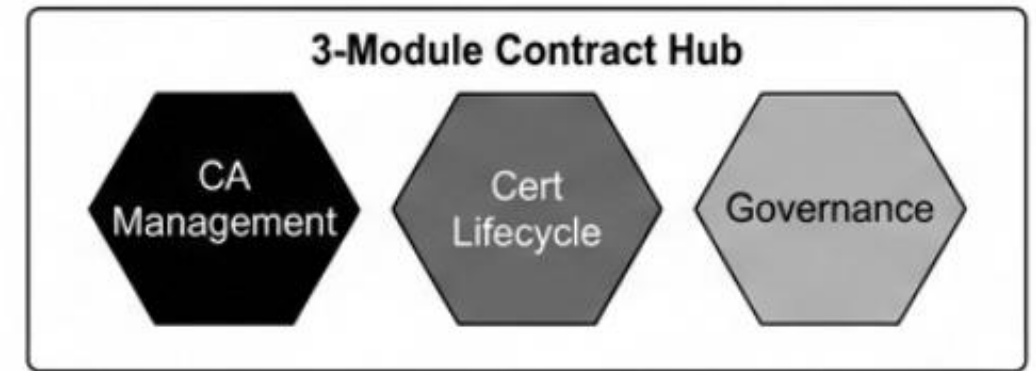
omponent	Quantity	Description
Orderer Nodes	4	SmartBFT consensus, tolerates 1 Byzantine fault
Peer Nodes	4	1 Peer per organization, chaincode installed
Organizations	5	OrdererMSP + Org1~4 MSP
Channels	1	dpki-channel
Endorsement Policy	MAJORITY	Requires endorsement from at least 3 out of 4 orgs

The X.dpki prototype: Smart Contract Logic & Certificate Lifecycle

- Three Core Contract Modules:** Implement "CA Management," "Certificate Lifecycle," and "Governance Consensus," fully unlocking the potential of smart contracts.

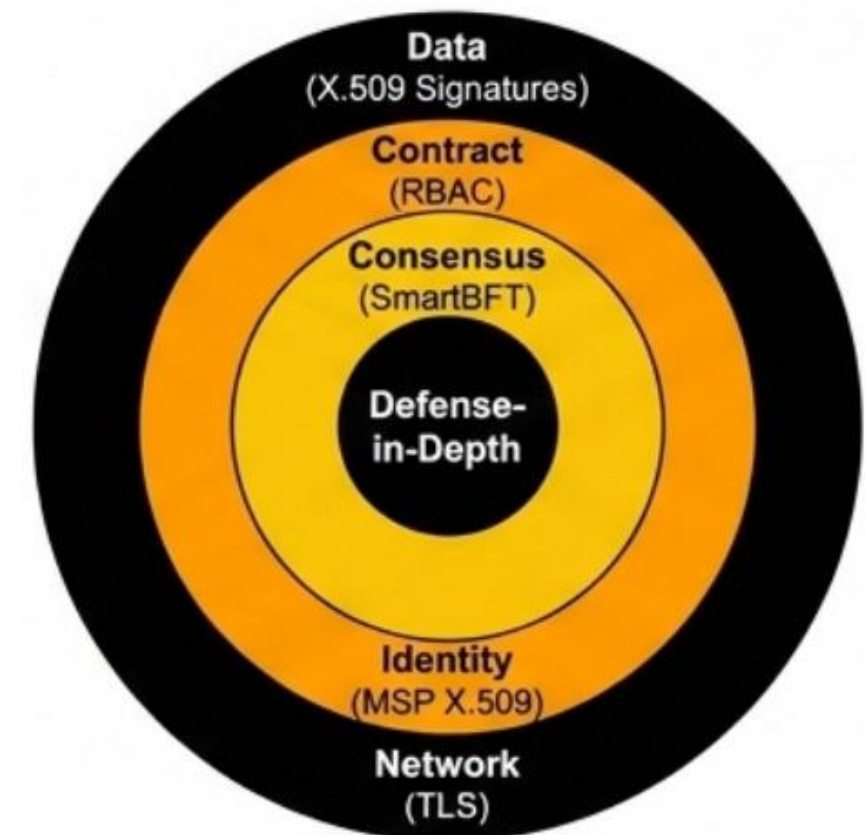
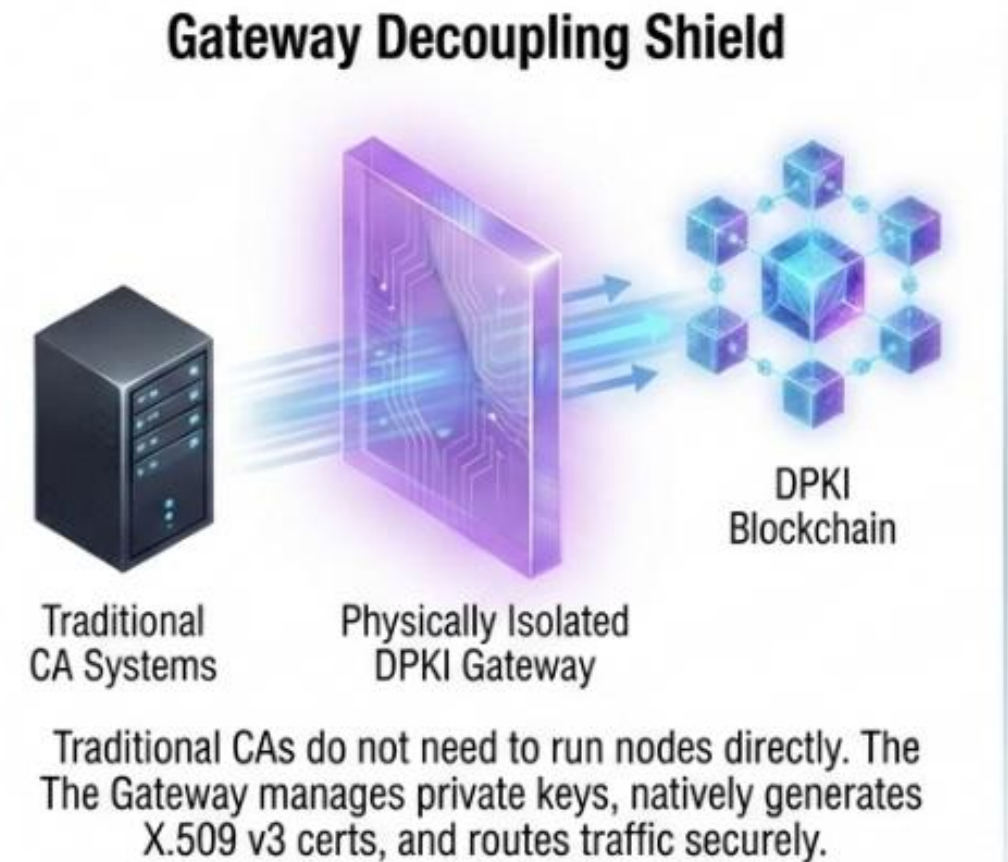
- Fine-Grained Access Control (RBAC):** Implement a 5-level role model (AdminCA, PrimaryCA, SubCA, etc.) and triggers an automated cascading revocation mechanism when a CA is deregistered.

- High-Performance Data Model:** Utilizes a CouchDB dual-index design (complete record index + state secondary index), reducing the complexity of massive OCSP/CRL status queries to $O(1)$.



The X.dpki prototype: Gateway Decoupling, On-Chain Governance & Security

- **Physically Isolated DPKI Gateway:** Achieves a true cryptographic closed loop. The gateway proxies CA interactions and natively generates X.509 signatures, meaning traditional CAs do not need to run blockchain nodes directly.
- **Automated L4 On-Chain Governance:** Critical operations (such as new CA registration or network config updates) require a 67% quorum approval. Upon reaching the threshold, smart contracts automatically execute the state changes.
- **Full-Stack Observability & Cryptographic Agility:**
 - Provides comprehensive system monitoring and visualization (tracking TPS, latency, and node liveness).
 - Features a multiple-layer security architecture with dynamic algorithm whitelists.



DPKI Prototypes: Using Dockers for Blockchain Nodes

Gordon BETA

Containers

Images

Volumes

Kubernetes

Builds

Docker Hub

Docker Scout

Models

MCP Toolkit BETA

Extensions

Containers Give feedback

Container CPU usage 13.42% / 1000% (10 CPUs available)

Container memory usage 6.06GB / 7.57GB

Show charts

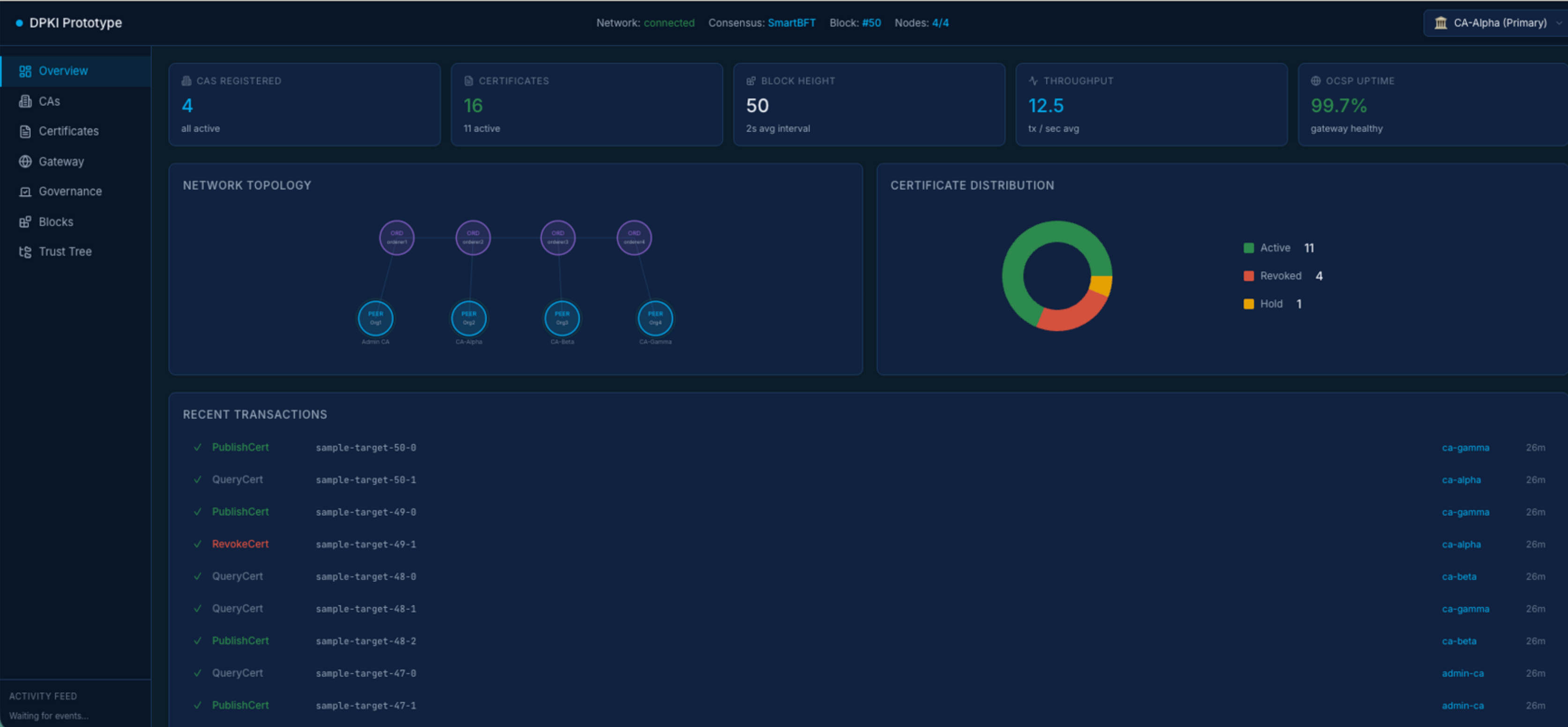
Search

Only show running containers

Name	Container ID	Image	Port(s)	CPU (%)	Memory usag...	Memory (%)	Disk read/write	Network I/O	PIDS	Actions
deer-flow-dev	-	-	-	0%	0B / 0B	0%	0B / 0B	0B / 0B	0, 0,	
gitlab	-	-	-	1.15%	3.77GB / 7.75GB	48.59%	652MB / 659KB	106KB / 60.8KB	229	
network-emulat	-	-	-	0%	0B / 0B	0%	0B / 0B	0B / 0B	0, 0,	
docker	-	-	-	12.08%	1.53GB / 100.75G	19.7%	21.21MB / 56.95M	55.93MB / 1.82M	1, 15	
dpki-cli	b77a228859a4	hyperledger/fabric-tools:latest		0%	1.01MB / 7.75GB	0.01%	49.2KB / 0B	4.63KB / 126B	1	
peer0.org3.dj	cca8253a3277	hyperledger/fabric-peer:latest	11051:11051	1.81%	279.6MB / 7.75G	3.52%	3.06MB / 13.8ME	13.8MB / 316KB	15	
peer0.org2.dj	32045a869c2b	hyperledger/fabric-peer:latest	9051:9051	3%	299.1MB / 7.75G	3.77%	2.14MB / 13.8ME	13.8MB / 342KB	15	
peer0.org4.dj	d5a2db4e05e1	hyperledger/fabric-peer:latest	13051:13051	1.68%	260.1MB / 7.75G	3.28%	250KB / 13.8MB	13.8MB / 304KB	15	
orderer4.dpki	a47f154f7693	hyperledger/fabric-orderer:latest	10050:10050 Show all ports (2)	0.02%	23.37MB / 7.75G	0.29%	135KB / 279KB	152KB / 134KB	13	
orderer1.dpki	cbffdfddd5cd	hyperledger/fabric-orderer:latest	7050:7050 Show all ports (2)	0.1%	30.22MB / 7.75G	0.38%	5.36MB / 279KB	168KB / 187KB	14	
orderer2.dpki	4b186bb99972	hyperledger/fabric-orderer:latest	8050:8050 Show all ports (2)	0.03%	27.75MB / 7.75G	0.35%	1.31MB / 279KB	150KB / 79.7KB	14	
orderer3.dpki	1f04762b48e3	hyperledger/fabric-orderer:latest	9050:9050 Show all ports (2)	0.02%	22.16MB / 7.75G	0.28%	24.6KB / 279KB	149KB / 135KB	14	
peer0.org1.dj	db73193ef077	hyperledger/fabric-peer:latest	7051:7051	3.08%	304.7MB / 7.75G	3.84%	2.26MB / 13.8ME	13.9MB / 369KB	15	
couchdb2	5334f1c12213	hyperledger/fabric-couchdb:latest	5985:5984	0.55%	79.04MB / 7.75G	1%	2.88MB / 168KB	5.23KB / 126B	37	
couchdb4	476e510a878d	hyperledger/fabric-couchdb:latest	5987:5984	0.75%	79.55MB / 7.75G	1%	1.83MB / 168KB	5.15KB / 126B	37	
couchdb1	f8ccc19e6de1	hyperledger/fabric-couchdb:latest	5984:5984	0.6%	78.41MB / 7.75G	0.99%	1.84MB / 168KB	5.45KB / 126B	37	
couchdb3	308b7c48ebc4	hyperledger/fabric-couchdb:latest	5986:5984	0.44%	78.47MB / 7.75G	0.99%	86KB / 168KB	5.28KB / 126B	37	

Showing 46 items

The X.dpkpi prototype: Overview



The X.dpki prototype: Certificate and There Status

DPKI Prototype

Network: connected Consensus: SmartBFT Block: #50 Nodes: 4/4

CA-Alpha (Primary)

Overview

CAs

Certificates

Gateway

Governance

Blocks

Trust Tree

Publish certificate

Search by subject, issuer, or serial...

AllActiveRevokedHold

Subject	Issuer	Serial	Status	Published	Actions
www.example.com	ca-alpha	01	Active	4/23/2026	ⓧⓂ
mail.example.com	ca-alpha	02	Active	4/24/2026	ⓧⓂ
api.example.com	ca-alpha	03	Active	4/25/2026	ⓧⓂ
db.internal.net	ca-alpha	04	Active	4/26/2026	ⓧⓂ
auth.example.com	ca-alpha	05	Revoked	4/21/2026	
old.example.com	ca-alpha	06	Revoked	4/18/2026	
staging.example.com	ca-alpha	07	Hold	4/28/2026	Ⓜ
secure.techcorp.io	ca-beta	01	Active	4/23/2026	ⓧⓂ
vpn.techcorp.io	ca-beta	02	Active	4/25/2026	ⓧⓂ
mail.techcorp.io	ca-beta	03	Revoked	4/19/2026	
dev.techcorp.io	ca-beta	04	Active	4/30/2026	ⓧⓂ
ci.techcorp.io	ca-beta	05	Active	5/1/2026	ⓧⓂ
portal.trustnet.de	ca-gamma	01	Active	4/27/2026	ⓧⓂ
id.trustnet.de	ca-gamma	02	Active	4/29/2026	ⓧⓂ
vpn.trustnet.de	ca-gamma	03	Active	5/1/2026	ⓧⓂ
legacy.trustnet.de	ca-gamma	04	Revoked	4/24/2026	

ACTIVITY FEED

Waiting for events...

The X.dpki prototype: List of Cas and Certificate Directory

DPKI Prototype

Overview

CAs

Certificates

Gateway

Governance

Blocks

Trust Tree

Search CAs...

admin-ca

Active

C=INT, O=DPKI Network, CN=Admin CA

Registered: 4/3/2026 Fingerprint: a34f2b1c8e9d0f3a...

ca-alpha

Active

C=CN, O=Example Corp, CN=Root CA Alpha

Registered: 4/13/2026 Fingerprint: 7ed13a4b5c6d7e8f...

ca-beta

Active

C=US, O=SecureTech Inc, CN=Root CA Beta

Registered: 4/18/2026 Fingerprint: f1e2d3c4b5a69788...

ca-gamma

Active

C=DE, O=TrustNet GmbH, CN=Root CA Gamma

Registered: 4/23/2026 Fingerprint: b2c3d4e5f6a7b8c9...

DPKI Prototype

Network: connected

Overview

CAs

Certificates

Gateway

Governance

Blocks

Trust Tree

Certificate trust tree (16 certificates across 4 CAs)

DPKI Network SmartBFT · 4 CAs · 16 certs

admin-ca AdminCA C=INT, O=DPKI Network, CN=Admin CA

ca-alpha PrimaryCA C=CN, O=Example Corp, CN=Root CA Alpha

www.example.com Active

mail.example.com Active

api.example.com Active

db.internal.net Active

auth.example.com Revoked

old.example.com Revoked

staging.example.com Hold

ca-beta PrimaryCA C=US, O=SecureTech Inc, CN=Root CA Beta

secure.techcorp.io Active

vpn.techcorp.io Active

mail.techcorp.io Revoked

dev.techcorp.io Active

ci.techcorp.io Active

ca-gamma PrimaryCA C=DE, O=TrustNet GmbH, CN=Root CA Gamma

portal.trustnet.de Active

id.trustnet.de Active

vpn.trustnet.de Active

legacy.trustnet.de Revoked

ACTIVITY FEED

Waiting for events...

Active

Revoked

Hold

AdminCA

PrimaryCA

The X.dpki prototype: The Gateway Nodes

DPKI Prototype

Network: connected Consensus: SmartBFT Block: #50 Nodes: 4/4

CA-Alpha (Primary)

Overview

CAs

Certificates

Gateway

Governance

Blocks

Trust Tree

OCSP Responder

Endpoint: http://localhost:8080/ocsp
Status: Running (mock mode)

CRL Publisher

Endpoint: http://localhost:8080/crl/
Status: Running (mock mode)

OCSP live test

Issuer DN

C=CN, O=Example Corp, CN=Root CA Alpha

Serial number

01

Query OCSP

>_ Equivalent openssl command:

```
$ openssl ocsp -url http://localhost:8080/ocsp \
  -issuer rootCA.pem -cert server.pem
```

Certificate Revocation List (CRL)

4 revoked - 1 on hold - Last updated: 5/3/2026, 11:01:42 PM

Status	Subject (CN)	Issuer CA	Serial	Revocation reason	Revoked at
Revoked	auth.example.com	ca-alpha	05	keyCompromise	4/23/2026, 10:33:34 PM
Revoked	old.example.com	ca-alpha	06	keyCompromise	4/20/2026, 10:33:34 PM
Revoked	mail.techcorp.io	ca-beta	03	keyCompromise	4/21/2026, 10:33:34 PM
Revoked	legacy.trustnet.de	ca-gamma	04	keyCompromise	4/26/2026, 10:33:34 PM
Certificates on hold (1)					
Hold	staging.example.com	ca-alpha	07	Held since 4/28/2026, 10:33:34 PM	

Table of Contents

- X.dpki draft and prototypes
- **The need from industry**
- Potential way forward for the X.dpki recommendation
- Summary

Emerging 6G Requirements: NPNs and AI Orchestration

Non-Public Networks (NPNs)

Distributed authentication for localized, slice-specific networks operating at the edge. Fine-grained security isolation preventing cross-attack risks.

AI Agent Ecosystems

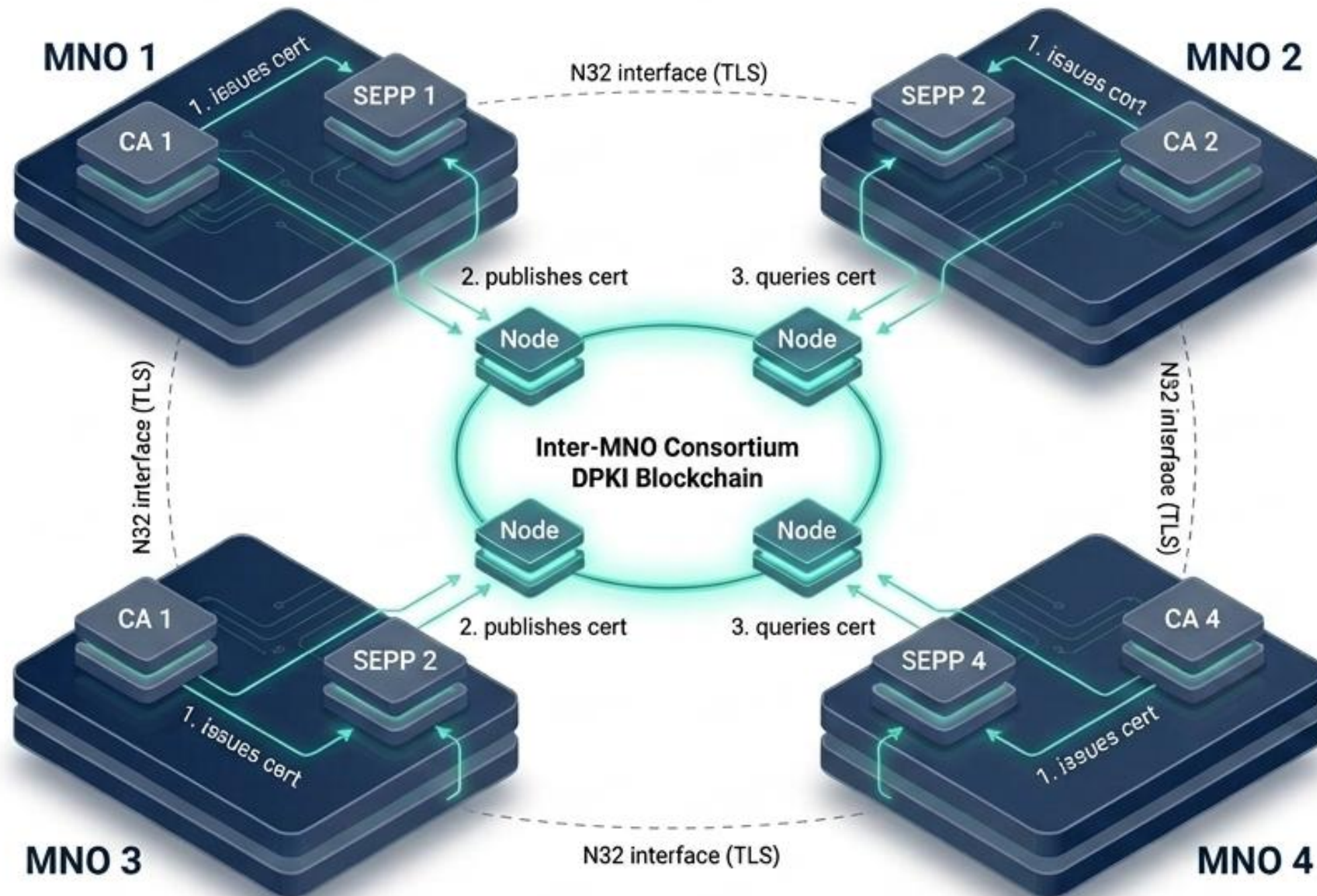
Secure profiling and global reachability for 3rd-party AI agents interacting with the 6G network (requiring robust, decentralized MSISDN mapping).

Network-Aware Resource Exposure

Authorizing localized access to xPU/computing resources for authorized third parties via smart city and XR/holographic use cases.



Industry Demand: 3GPP 6G Inter-MNO Roaming



The Challenge

Managing large number of CA cross-certification for Security Edge Protection Proxies (SEPPs) across multiple Mobile Network Operators (MNOs).

The DPKI Solution

A shared, immutable Inter-MNO Consortium Blockchain.

The Flow

CAs issue certificates internally, publish to the DPKI Node. The target SEPP queries the ledger, achieving mutual authentication without bilateral agreements.

DPKI Gateway: On-Chain Function Access

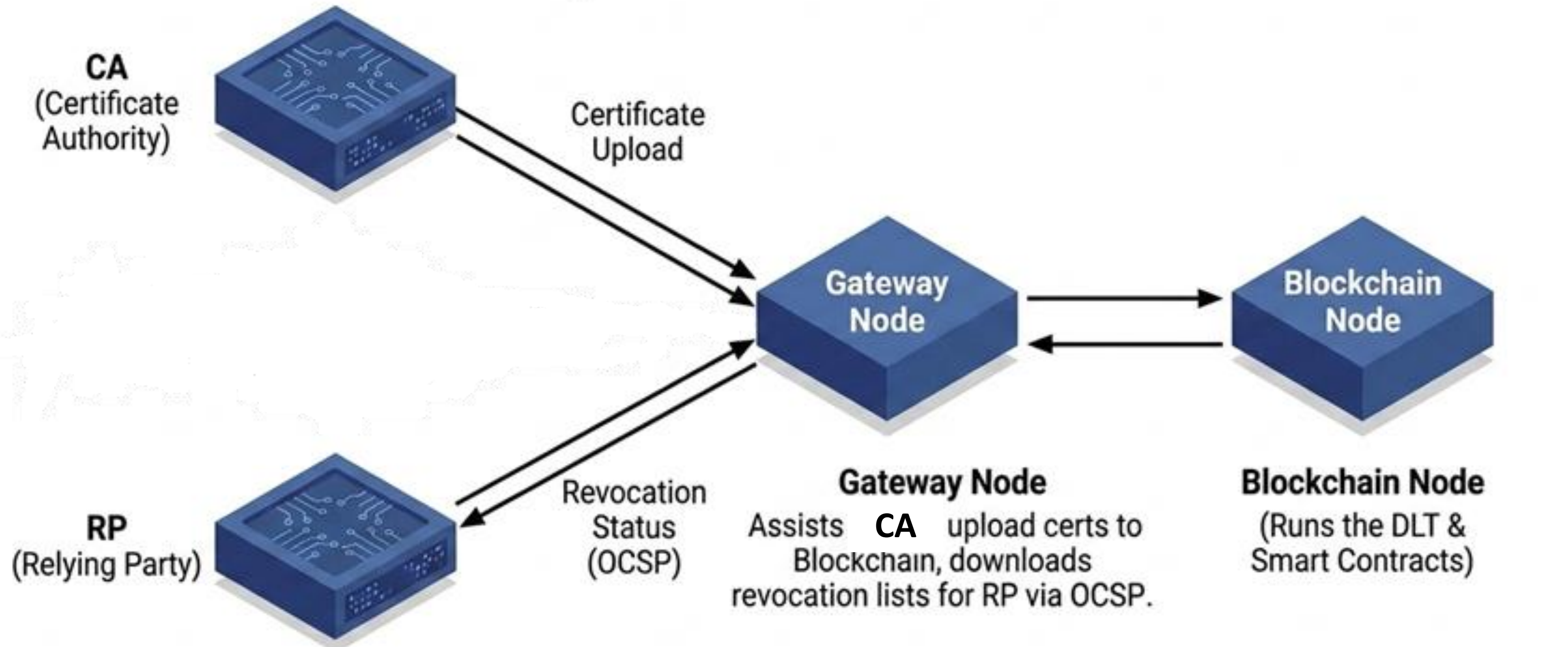
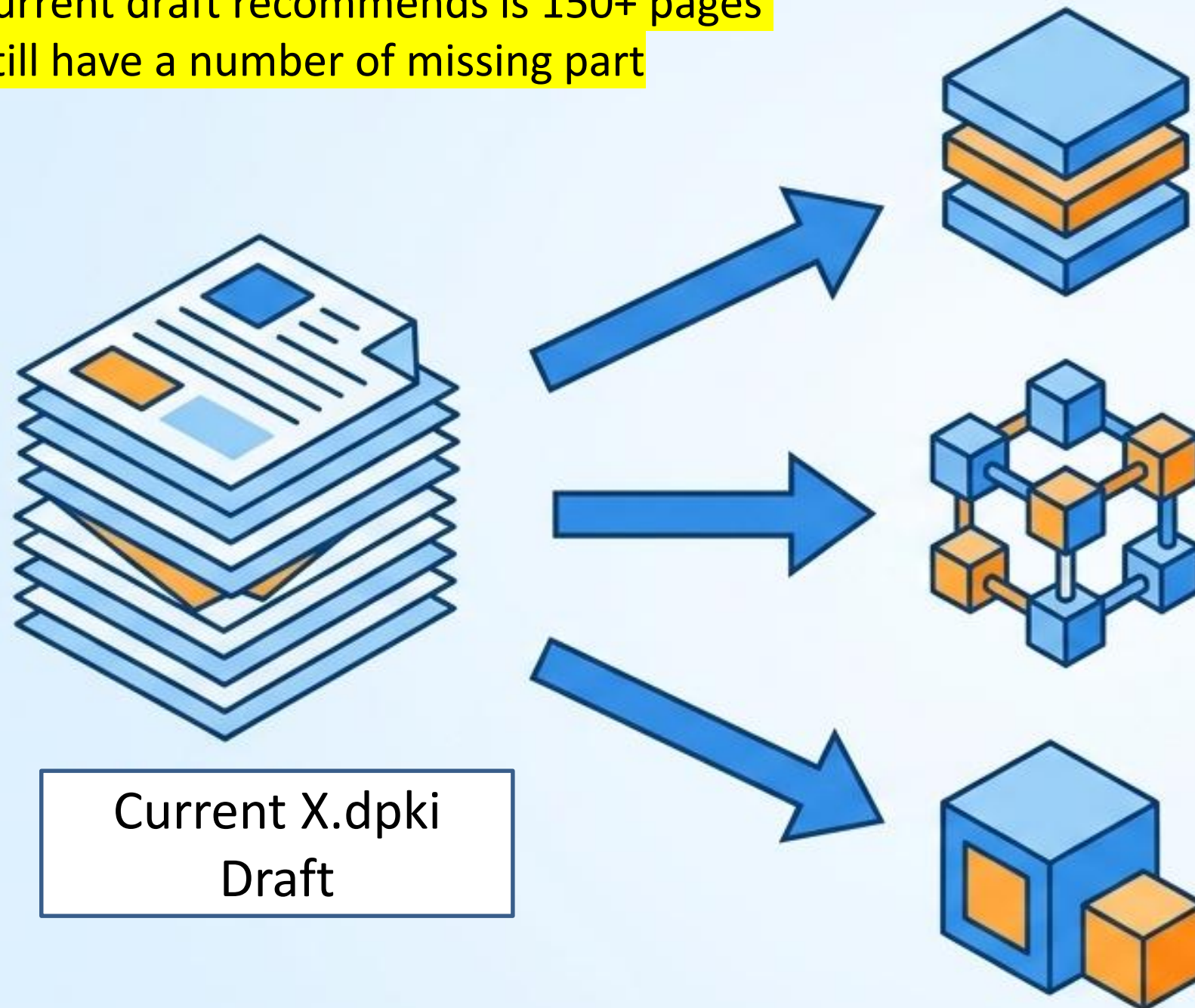


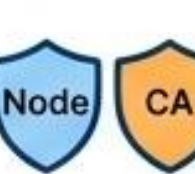
Table of Contents

- X.dpki draft and prototypes
- The need from industry
- **Potential way forward for the X.dpki recommendation**
- Summary

Structural Optimization & Refinement

The current draft recommends is 150+ pages and still have a number of missing part



-  Clarifying Protocol vs. Application Logic
-  Harmonizing Role Definitions
-  Streamlining Core Framework Scope
-  Aligning with ITU-T X.1400 & ISO 23257
-  Separating Node & CA Identities

Harmonization with Global Standards

ITU-T X.509

Acts as the foundation. Certificate formats and path validation rules remain fully compatible.

ITU-T X.1400 Series

Provides the established baseline for DLT security requirements and threat modeling.

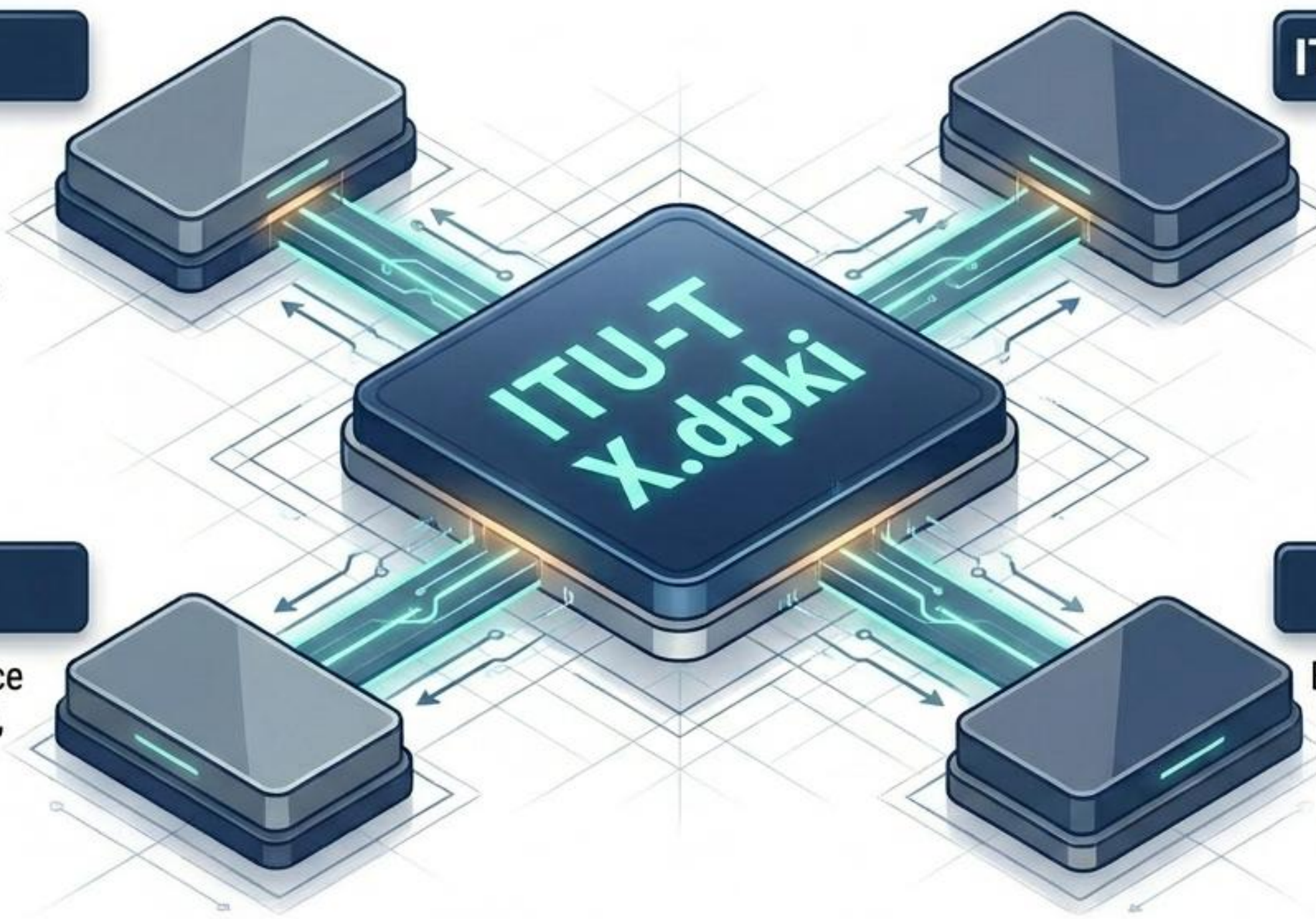
ISO 23257

Adopted for DLT reference architecture terminology, ensuring global naming consistency.

W3C DID/VC

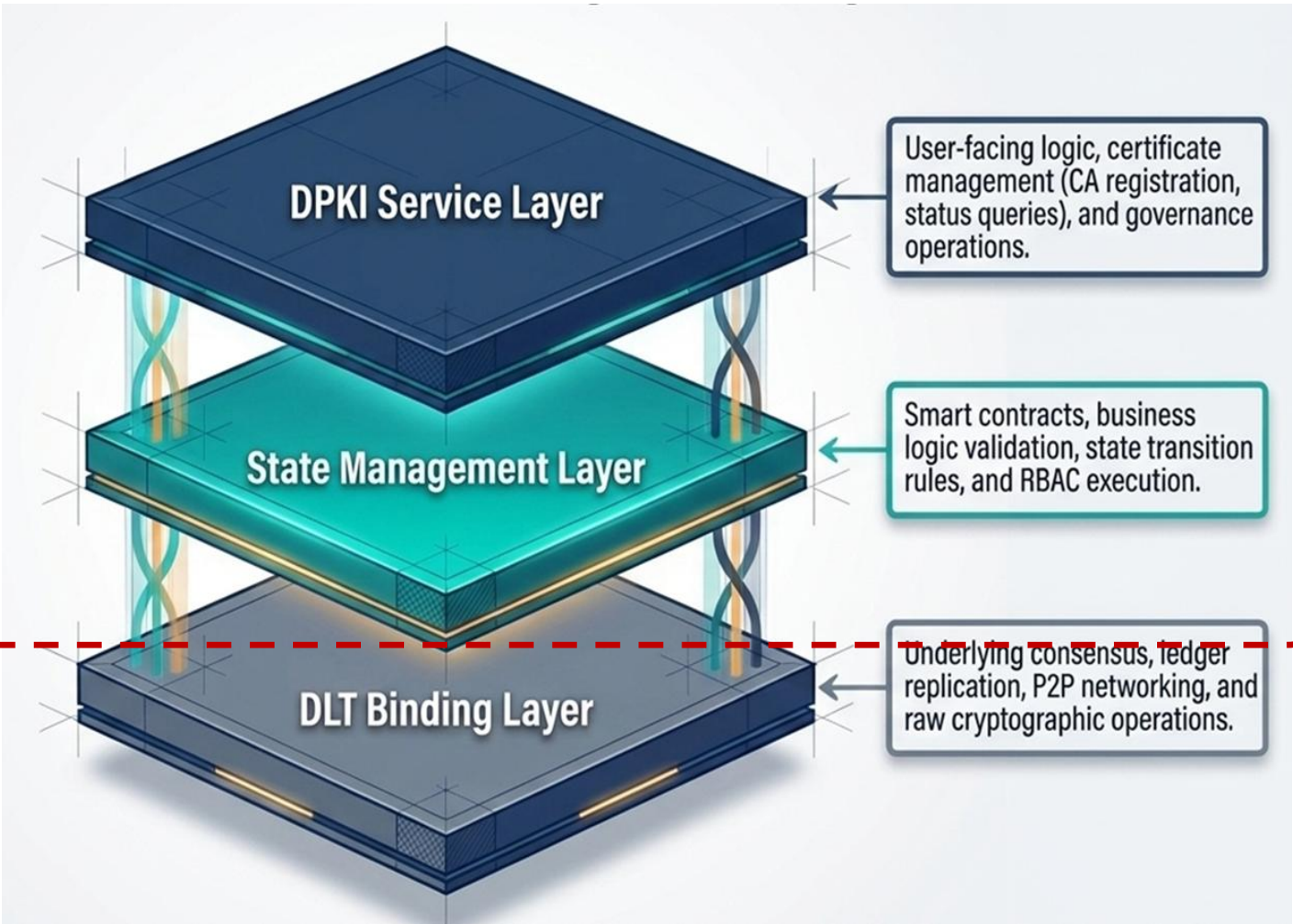
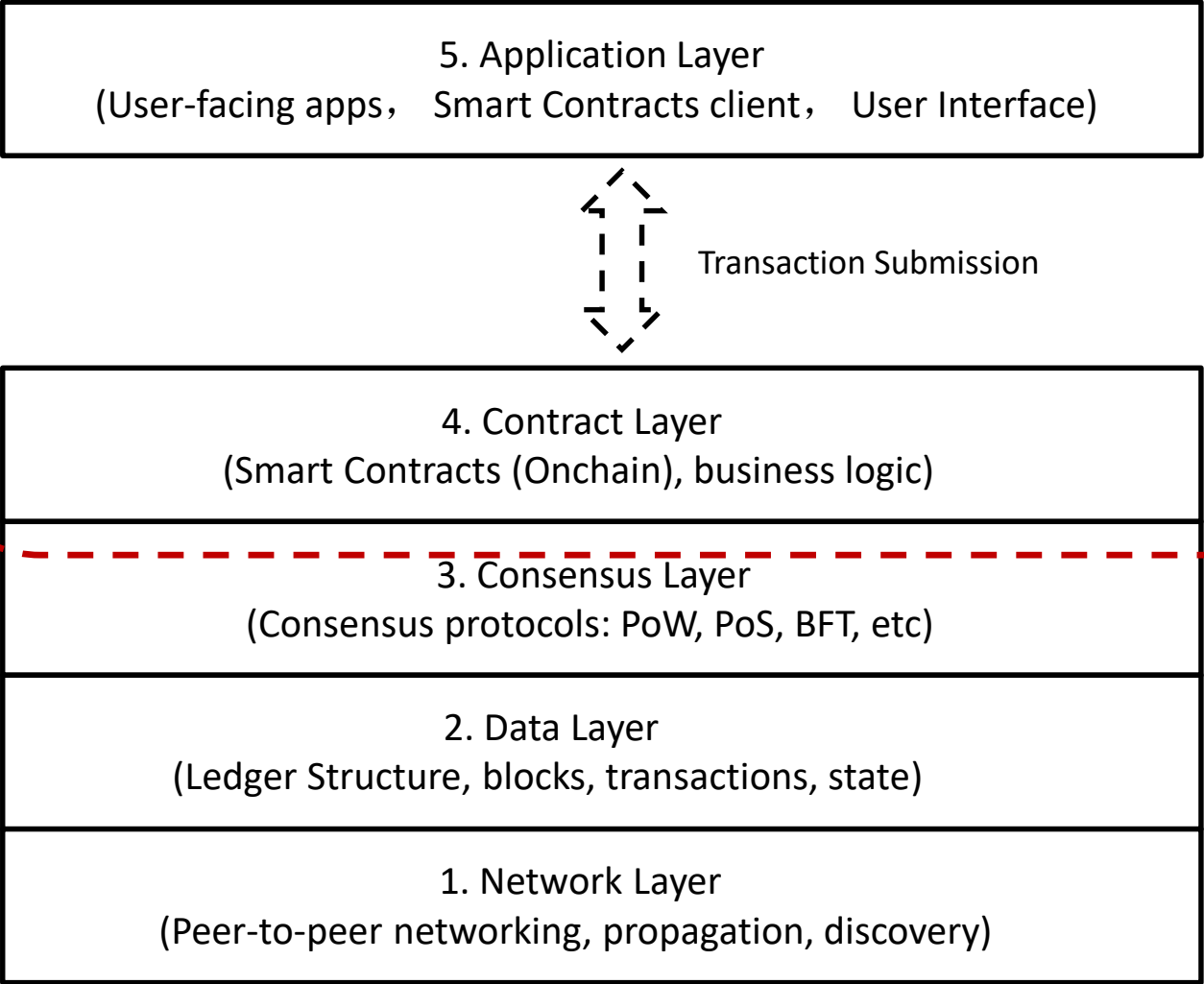
Establishes clear boundaries. X.dpkI manages institutional X.509 certificates, while Web3 DID manages decentralized, self-sovereign identity formats. Interoperability bridges (eIDAS) will be supported.

ITU-T
X.dpkI

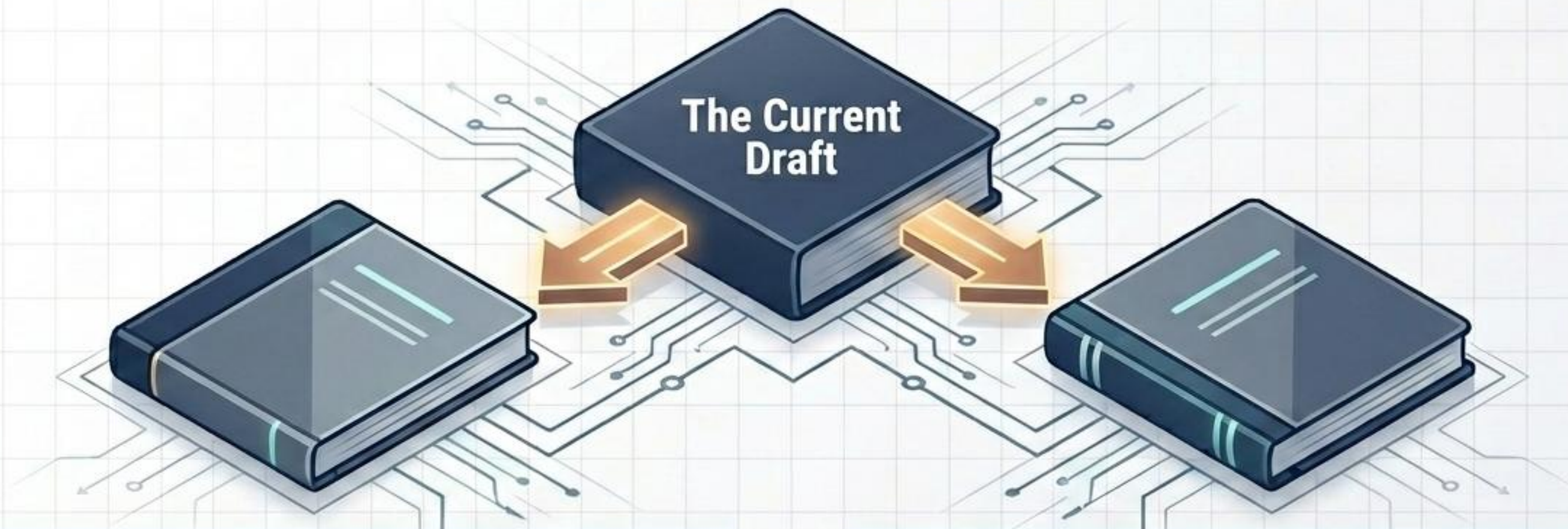


Take a Layered Measure in Standard Development

Focus of X.dpkgi standard development



Possible recommendation development strategy for Consideration



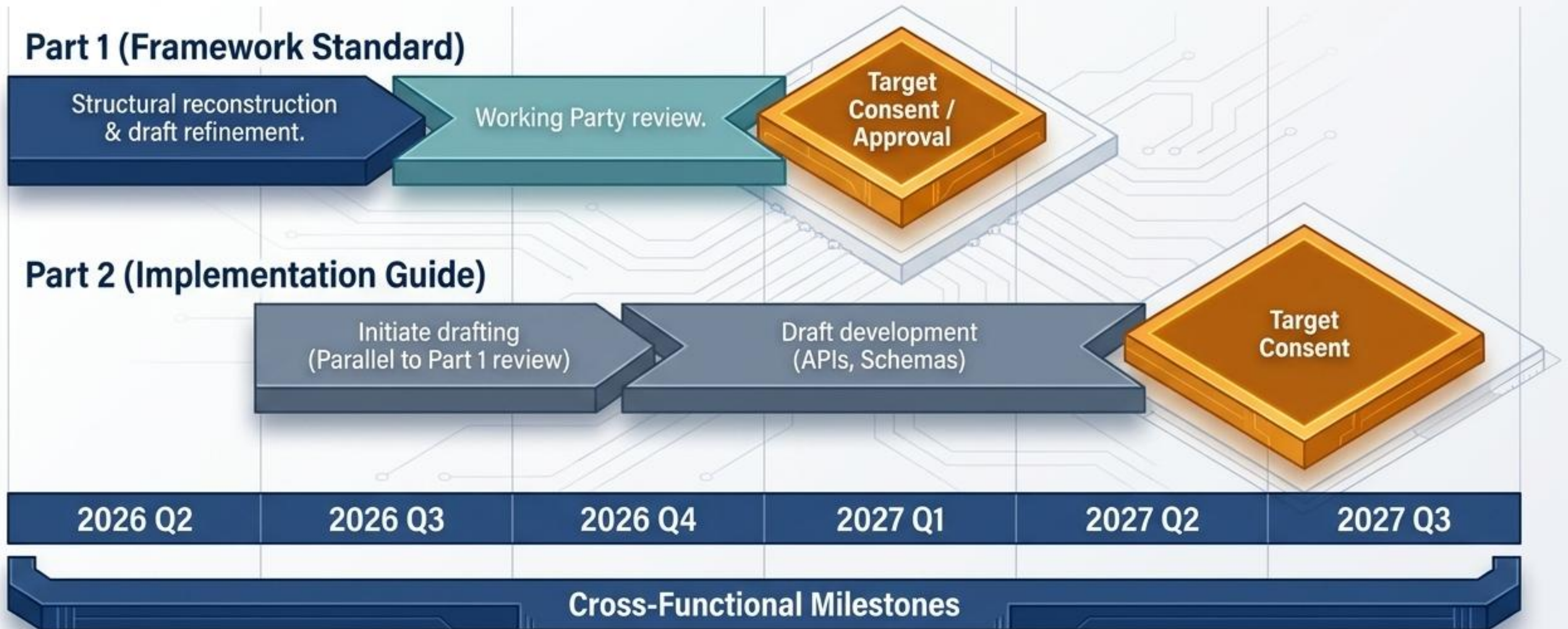
Part 1: Architecture & Security Framework (Priority)

- System Architecture & Layering
- Trust Models & Security Requirements
- Governance and Access Control
- PQC Migration Requirements

Part 2: Implementation Guidelines (Subsequent)

- Data Structures & Schema Encodings
- Smart Contract Interface Definitions
- API Specifications & Protocol Bindings
- DPKI Gateway Implementation

Standardization Roadmap (2026–2027)



3GPP/GSMA liaison integration; NIST PQC synchronization.

Table of Contents

- The current status of the X.dpki draft recommendation
- The need from industry
- Potential way forward for the X.dpki recommendation
- **Summary**

Summary

Considering the demand from industry, the X.DPKI recommendation may follow a two-part strategy:

Part 1: Framework & Architecture (Priority)

- Separate recommendation development.
- Take architecture design from baseline.
- Amend with: Trust model, Security reqs, DLT reqs, PQC migration reqs

Part 2: Implementation & Verification (Subsequent)

- Continue development effort.
- Develop with help of prototypes.
- Verify interface design.

Submit Part 1 for approval and publish in 2027, while continuing Part 2 development.

