Secure Onboarding & Zero-Touch Provisioning for Millions of Smart City Devices with Compliance Mapping to Saudi Smart-City Guidance: A Systematic Review (2020–2025)

Adeel Sadaqat

Ph.D, Research Scholar, Institut Universitaire du Bénin (IUB), Ayimlonfide, Porto-Novo, Benin, ORCID: 0009-0002-2367-6292

doi.org/10.64643/IJIRTV12I8-189606-459

***Abstract*—Saudi smart city schemes involve the use of cyber-physical systems on a massive scale, such as environmental sensors, smart meters, intelligent transport endpoints, and video analytics cameras installed all over the city. With a potential increase from thousands to millions of units per fleet, the viable approach of manually enrolling units (performing credential injection, site-by-site configuration, and ad-hoc authorization decisions) becomes implausible from the standpoint of operational feasibility and/or security risks. This systematic review integrates the 2020-2025 peer-reviewed literature with widely accepted standards and regulative control frameworks relating to secure enrollment procedures of massive numbers of IoT devices. The literary sources cover voucher-based bootstrap and transfer-of-ownership provisioning, device management bootstraps, remote attestation frameworks and token structures, firmware update frameworks, and policy-based authorization according to the principles of the Zero Trust Architecture. From these sources, we extract four primitives described below for modern-day enrollment: (P1) device-anchored identity with protected roots, (P2) ownership transfer w.r.t late binding to limit trusted installers, (P3) posture attestation as a statement w.r.t verifiable evidence, and (P4) policy-based authorization as a least-privilege and purpose-bound directive. We combine the above primitives to form a reference architecture by composition, which is called the Zero-Touch Assurance Stack (Z-TAS). We then align the Z-TAS controls over lifecycles to Saudi smart city best practices, which include NCA Essential Cybersecurity Controls (ECC-2:2024), Cloud Cybersecurity Controls (CCC-2:2024), NDMO data management norms (2021), Saudi Personal Data Protection Law (PDPL, 2023), and CST IoT Regulations (2024). The alignment is useful for forming the basis of a compliance-by-design conclusion that, for Saudi smart cities, trust on-boarding has to be considered as an auditable lifecycle governance process that generates robust evidence artefacts (identity lineage, enrollment data, attestation appraisal results, policy decisions, and data governance markers).**

***Index Terms*—zero-touch provisioning; secure onboarding; device identity; ownership transfer; remote attestation; Zero Trust; smart cities; Saudi Arabia; ECC; PDPL; NDMO; CST IoT**

I. INTRODUCTION

“Smart city” deployments are rapidly becoming more accurately characterized by the concept of “cyber-physical systems of systems,” which refers to a collection of heterogeneous devices and subsystems, often owned by different parties, designed by different manufacturers, and interfaced through common cyber platforms. Quite often, a single smart city implementation involves millions of nodes with varying lifetimes (5 to 20+ years), varying levels of criticality (traffic monitoring cameras vs. life-critical sensors), and varying connectivity options (fiber, 4G/5G, LPWAN, satellite). This situation only serves to magnify an inherent conflict between the need for speed of deployment in a smart city and the creation of a new “security perimeter” for each node, whose breach can have implications for different services.

Conventional device-onboarding methods have presumed that a human device installer or a type of field engineer could securely configure a device, provide it with credentials, and then enroll it onto a manager system. However, such a presumption will not work for reasons below, especially within a million device scale. Firstly, it will not work from a practical or operational perspective, as device-by-device provisioning will provide a long lead-time, unreliable configurations, and become very costly. Secondly, it will not work from a security point of view; the more a task relies upon manual secret management or improvised site-by-site operations, the more likely a risk it faces regarding leaks of credentials, accepting a counterfeit device, and incorrect access configurations and audit steps. Modern best practices recommend moving the entire device onboarding from the realm of 'configure and hope' to 'automate and verify'.

The more recent literature of 2020-2025 is increasingly treating the subject of onboarding or enrollment processes that establish a first level of trust between (i) device identity based either upon manufactured or hardware-protected keys, (ii) the identity and authorization framework associated with the administrative domain, and (iii) operational rules that describe what a given device is capable of doing and what data flow is supposed to be enabled. A typical architecture for a system-of-systems enrollment process incorporates an OC that coordinates the enrollment process for devices, systems, and services through registries and certificates (Maksuti et al., 2021). As a parallel process, recommendations for Zero Trust Architecture contend that "trust is assessed, not granted. Continuously evaluate identity, context, and evidence" (NIST, 2020).

Saudi smart city initiatives introduce an additional governance element in that onboarding needs to be provably compliant with country-level cybersecurity and data governance standards. The National Cybersecurity Authority’s “Essential Cybersecurity Controls” (ECC-2:2024) and “Cloud Cybersecurity Controls” (CCC-2:2024) detail country-level governance and technical standards on controls related to governance, access control, cryptography techniques, monitoring and auditing of activities and systems, incident response and handling, and supplier assurance (NCA, 2024a and 2024b). “Guidelines on Data Classifications” from the National Data Management Office (NDMO) view classifications in terms of governance and ownership and guide on retention and management of all types of organizational-data across its entire life cycle (NDMO, 2021). The “Personal Data Protection Law” (PPLD) spells out organizational and technical guidelines on handling and processing organizations’ responsibilities in ensuring PDPL and outlines constraints on storing and transporting such data to third-party organizations (SDAIA, 2023). The “Communications Space and Technology” Internet of Things (IoT) “Regulations” give additional country-level definitions concerning responsibilities in terms and mechanisms on “providing” security and privacy to users in an “internet-of-things” environment and governance within that environment (CST, 2024

There are three questions that can be responded to by this systematic review based

RQ1: Which standards and patterns are prevalent in secure onboarding and zero-touch provisioning in large-scale IoT deployments (2020-2025)?

RQ2: How are such patterns combined to provide an end-to-end assurance system design to serve millions of smart city devices?

RQ3: How can the derived controls be related to the guidance provided by “Saudi smart city” to ensure “Compliance by Design”?

The unique aspect of this paper is the integration consequent (not a new protocol) from the reviewed literature set, the Zero-Touch Assurance Stack (Z-TAS) and the Saudi mappings of compliance trace the ECC/CCC, PDPL, NDMO, and CST expectations in the creation of necessary on-boarding artifacts. The literature assessment is systematic (protocol-driven) and not empirical—it doesn’t do field experiments but interprets the literature and standards body of evidence.

II. METHODOLOGY (SYSTEMATIC REVIEW PROTOCOL)

We adhere to PRISMA 2020 guidelines for transparent reporting on systematic reviews (Page et al., 2021) and shaped them to fit a security and standards corpus. Seeing that onboarding practices are highly specification and control framework dependent, this review comprises both (a) peer-reviewed literature and (b) normative or quasi-normative texts such as RFCs, standards, and controls from juristic authorities that are quite popular in terms of following them.

2.1 Search strategy and sources

We searched digital libraries and standards databases from the period 2020 to 2025: IEEE Xplore, ACM Digital Library, ScienceDirect, NIST CSRC/NVL published documents, ETSI deliverables, IETF RFC Editor and Datatracker, ISO/IEC catalogs, and publicly accessible websites of the concerned Saudi authorities (NCA, SDAIA/NDMO, CST, and DGA). The search string template sets included (“secure onboarding” OR “device enrollment” OR “zero-touch provisioning” OR “remote provisioning” OR “ownership transfer” OR “late binding” OR “voucher” OR “BRSKI” OR “FDO” OR “LwM2M bootstrap ("IoT" OR "edge device" OR "smart city") AND ("attestation" OR "posture" OR "evidence" OR "Backward and forward citation chases starting from the seed articles are also carried out to extend the coverage of prominent standards-related publications, such as system of systems onboarding controller design (Maksuti et al., 2021) and smart city networking surveys incorporating slicing and multi-service isolation (Rafique et al., 2025).

2.2 Eligibility

We selected documents that have been published between the years 2020 and 2025 and

design, assess, or specify secure on-boarding/provisioning

(ii) relate to one or more of device identity, ownership transfer, bootstrap configuration, credential lifecycle, posture attestation, and/or policy-driven authorization.

(iii) the applicability of the techniques to fleet sizes (clear applicability for either large-scale fleets explicitly or by design characteristics such as late binding).

We chose to exclude research that pre-dated 2020, purely conceptual work that did not have a threat model for provisioning, and small prototypes that did not generalize well from laboratory use. Additionally, documents that were strictly about other regions of cybersecurity, such as anomaly detection that required no enrollment, were also removed.

Department of Commerce:

2.3 Data extraction and synthesis method

For each included feature, a consistent set of variables: trust anchor (keys and their location), ownership model (who can authorize feature enrollment and transfer), bootstrap process (voucher, rendezvous, bootstrap server, bootstrap server equivalent), credential management (feature issuance, refresh, revocation), posture evidence (claims, freshness, role as verifier), authorization association (enrollment as access control), scaling factors (registrar, automation, batching), and finally observability/auditability factors (which events are recorded, evidence retention). The results were synthesized into: (1) A taxonomy of onboarding patterns & standards; (2) The Zero-Touch Assurance Stack (Z-TAS), an end-to-end reference architecture; (3) A Saudi compliance mapping, aligns Z-TAS controls with ECC/CCC, PDPL, NDMO, CST IoT Regulations, digital government governance structures. (DGA, 2023).

2.4 Limitations of the Review

The review itself is systematic but not exhaustive within the model of a meta-analysis in medicine; it includes standards in the body of works cited, which are sometimes not indexed in academic sources. In our own research, therefore, we focus more on inclusiveness with regard to normal standards research and peer-reviewed articles, with visibility into sources used and mapping logic rather than statistical analysis. Meta-analysis is not possible within our project because articles include varied research methods and outcomes.

Table 1. Standards and patterns extracted from the 2020–2025 corpus.

Pattern/Standard	Core Idea	Scale Benefit	Primary Plane(s)
Voucher-based Bootstrapping (BRSKI)	Voucher binds device to operator domain at first contact	Avoids installer-held secrets; repeatable enrollment	B, E
Transfer-of-Ownership (FDO)	Device contacts rendezvous; receives owner-defined service info	Supports drop-ship logistics and untrusted installers	B, E

LwM2M Bootstrap	Bootstrap server provides initial security and management endpoints	Constrained device management at scale	B, D
RATS Architecture	Roles for evidence generation, verification, and relying party	Composability and auditability of attestation	C, E
EAT Tokens	Standard token format for attestation claims	Interoperable evidence for policy systems	C, D, E
SUIT Update Architecture	Standardized secure firmware update workflows and manifests	Fleet remediation with integrity and traceability	A, C, E
Zero Trust Architecture	Continuous verification + least privilege authorization	Policy gating for massive, multi-tenant services	D, E

III. RESULTS

3.1 A unifying perspective: Onboarding as “Trust Establishment Plus Evidence”

Throughout the corpus of 2020-2025, the best practice of secure onboarding as a convergence point emerges as a device registration system that not only registers the device as a subject within an authorization system but instead assesses its identity and its state of security. This perspective aligns with the guidelines by Zero Trust that identify trust as a dynamic (NIST, 2020), context-dependent construct:

Primitive P1 - Device-bound identity. The device shall have a distinct cryptographic identity that is protected by hardware or equivalent security, enabling high-level authentication, anti-cloning, and management of credentials through functions such as "cryptography requirements" (ETSI, 2020; NIST, 2020; NIST, 2021a; NIST, 2021b; NISTIR, 2020). For smart cities, such identity has to endure environmental characteristics in addition to support for inventory within assets.

Primitive P2 – Ownership transfer and late binding. Zero-touch designs distinguish “installation” from “ownership authority.” Voucher-based bootstrapping from schemes like BRSKI lets a device trust an operator domain upon initial interaction without revealing long-term credentials to an installer (IETF, 2021).

FIDO Device Onboard (FDO) describes an abstract transfer-of-ownership method so devices can be shipped without packaging, with activation performed by an untrusted installer, yet with cryptographically secure verification of ownership transfer (FIDO Alliance, 2022; Cooper, 2024). Device management solutions like LwM2M Bootstrap enable standardization of initial setup and security control delivery (OMA SpecWorks, 2022; OMA SpecWorks, 2020).

Primitive P3 – Posture attestation and evidence formats. Posture assessment by modern devices is conceptualized based on evidence generation, verification, and authorization by the relying party. The RATS architecture describes the roles (attester, verifier, and relying party) and the process flow for appraisal of the evidence (IETF, 2023). Entity Attestation Token (EAT) development provides a basis for representing claims through tokens that can be used for interoperable attestation processes (IETF, 2025). Research work done through the survey highlighted that scalable verification could be possible based on standardization of what is assessed, freshness, and runtime attacks (Kuang et al., 2022).

Primitive P4 — Policy-Based Authorization in Zero Trust.

To this end, the requirement catalog developed by NIST serves as an additional baseline, allowing for the use of high-level requirements in establishing onboarding acceptance criteria on the basis of device types (NIST, 2024).

Enrollment has increasingly been regarded as a gatekeeping process for other benefits to happen, such as the issuance of licenses to broadcast telemetry, respond to commands, or stream video as authorized under identity and posture assertions. This supports least privilege, segmentation, and constant verification in Zero Trust Architecture (NIST, 2020). Within multi-service smart cities, such policies may integrate with other concepts such as network slicing to limit the blast radius to suit the level of required services (Rafique et al., 2025).

3.2 System-of-systems onboarding:

device, system, andA major trend in the smart city area is the extension of onboarding from devices towards subsystems as well as services. Maksuti et al. in 2021 show how the onboarding of a system-of-systems could be accomplished through a structure that has an Onboarding Controller managing three types of onboarding: device onboarding, system onboarding, and service onboarding. This tackles the issue of how a smart city "devices" often are road side units or a combination of devices; in cases in which only the endpoint has been enrolled but the service side has not been managed, the trust chain is busted.

3.3 Operational themes: automation, registries, and cohort management

Large fleet.Onboarding often employs the use of registries (device registration, system registration, service registration), in addition to operations along cohorts in which policies and evidence are organized by type of device and risk category, instead of per device. Industrial Internet Consortium best practices advise extended late binding, common provisioning pipelines, together with interoperable device management frameworks such as BRSKI, FDO, & LwM2M (IIC, 2022). Recent works propose the use of distributed systems such as blockchain registries in order to avoid single sources of failure in addition to improving auditable ownership chains, which are a current development in this sector of practice (Jarcau et al., 2025; Krishnan et al., 2024).

3.4 Alignment of Saudi compliance and "fifth primitive" evidence longevity

Applying this to Saudi guidance, a key implication is that compliance requirements introduce a "fifth primitive" to onboarding—a demonstration of longevity. ECC/CCC stress monitoring, governance, and non-certification assurance (NCA, 2024a, 2024b). NDMO stresses retention, categorization, and stewardship (NDMO, 2021). PDPL stresses protection and lawful processing of personal data (SDAIA, 2023). Overall, this means that onboarding needs to create long-lived artifacts: Identity Lineage Records, approval for enrollment, configuration baseline, attestation history, and decisions on access and audit logs. Many tech designs start with enrollment security but lack sufficient description on supporting these artifacts in a regulator-accessible fashion.

3.5 Threat model for zero-touch onboarding in smart cities

This review is only beneficial in so far as it can enlighten what the onboarding system has to protect against. The 2020–2025 corpusseries implies and explicitly indicates the regular risksserieses, which become more serious in an urban context. These are grouped in five categories, keyed according to the Z-TAS planes.

T1 - Substitution in the supply chain and substitution of counterfeit devices.

As substitution attacks in smart city implementations involve complex chains of manufacturers, distribution, logistics, and several integrating firms, an adversary may try to introduce substitution attacks by attempting to inject substitute devices, substitute devices in transit, and with untested verification of device origin. The need to establish device-based identity and origin in foundational IoT security recommendations mitigates this risk by promoting distinct credentials and securing key material (ETSI, 2020; NISTIR, 2020; NIST, 2021a).

T2 – Installer compromise and credential exposure.

Installers are seldom inside the trusted security boundary. If enrollment involves keyboard-entry password and key injection or downloading long-term secrets, compromised laptops or insiders can scale up credential exposure. That's what late-binding protocols aim to solve. Voucher bootstrapping (BRSKI) ties devices to the operator domain without secret exposure to the installer, and transfer of ownership provisioning (FDO) enrollment similarly doesn't require handling long-term keys during activation (IETF, 2021; FIDO Alliance, 2022). As regards Saudi ECC expectations on access and cryptographic keys and Saudi compliance, minimizing secret handling also satisfies ECC's ECC expectations (NCA, 2024a).

T3 - Rogue enrollment and domain impersonation.

A simple type of join attack is to trick the device into enrolling in an attacker-controlled domain or to trick the platform into joining the device if it is not authorized. Such an attack can be attempted through DNS and/or routing, trust and credentialized rendezvous, and message replay attacks to initiate the enrollment process. The standards examined do this by enforcing mutual authentication and enrolling based on verifiable concepts (such as vouchers and ownership transfer) and not based on authentication and input from unauthenticated network location (IETF, 2021; IIC, 2022). In Z-TAS, Plane B ensures that rogue device enrollment is associated with the appropriate and legal domain, while Plane E ensures that the occurrence is logged sufficient enough to aid in future audit trail.

T4 - post-enrollment compromise and configuration drift.

Devices may be compromised after enrollment by unresolved vulnerabilities, exposed debugging interfaces, and risky firmware update systems. For these reasons, contemporary enrollment architecture continues to move towards incorporating state verification (posture checking or attestation) and secure firmware update architecture. RATS contains a normative model of appraisal for evidence-based proofs of state claims (IETF, 2023). EAT token work for cross-vendor attestation statements is ongoing support for IETF 2025. SUIT specs prescribe architecture and normative information models for firmware update architecture that enhances update integrity (IETF, 2021b; IETF, 2022). These are actualized in Z-TAS by Plane C and Plane D of a city that can decrease privilege in case of stale evidence and drift in Plane D, consistent with NIST's Zero Trust model of continuous verification (NIST, 2020).

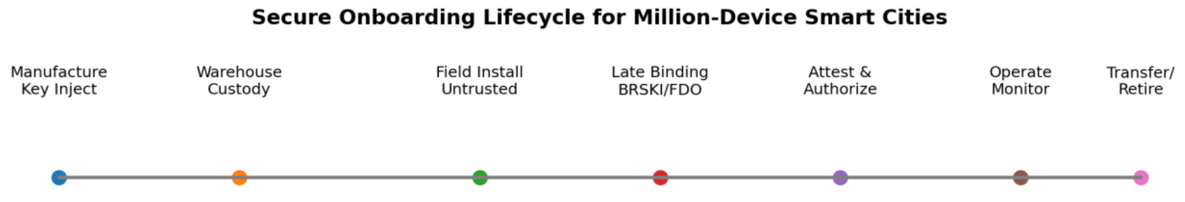
T5 – Data misuse, privacy breeches, and lack of accountability.

Smart city devices are known to process personally identifiable information directly (video and vehicle info streams) or indirectly (consumption patterns from meters). Consequently, onboarding should serve to both authenticate and bind policy limitations to both data processing and access. PDPL demands that organizations are responsible for ensuring that personally identifiable information is secured and that they are accountable in everything they do. NDMO specifically points out classifications and management and retention of data (SDAIA, 2023; NDMO, 2021). "Zero trust" policy systems are ideal tools for carrying out this task. These are capable of policy formulation that either limits the use to which certain streams are put or that requires role-defined roles in accessing said streams and logging decisions taken for audit trail purposes (NIST, 2020; NCA, 2024a).

For Z-TAS, this category focuses on Planes D and E. In brief, threat modeling extends a vital lesson of synthesis: secure onboarding is not just about Day One. Secure onboarding is where a lifecycle of governance begins, after all, that deals with issues of identity, evidence, access, and accountability. The requirements of compliance from the kingdom of Saudi Arabia make all things about evidence artifacts even more crucial.

Table 2. Threat model and mitigation mapping (synthesized).

Threat Class	Example Attack	Mitigating Controls (Z-TAS)
T1 Supply-chain substitution	Counterfeit device inserted during logistics	Plane A provenance; device-anchored identity; supplier assurance evidence
T2 Installer compromise	Installer laptop leaks credentials	Late binding (BRSKI/FDO); no installer-held domain secrets
T3 Rogue enrollment	Device enrolls into attacker domain	Mutual authentication; vouchers/ownership evidence; pinned trust anchors
T4 Post-enrollment compromise	Unpatched firmware exploited	Attestation + policy gating; secure updates (SUIT); revocation logs
T5 Data misuse/privacy	Unauthorized access to camera feeds	Policy enforcement; least privilege; audit trails; PDPL purpose tags



IV. SYNTHESIZED REFERENCE ARCHITECTURE: THE ZERO-TOUCH ASSURANCE STACK (Z-TAS)

Z-TAS is a compositional reference architecture derived from the review, intended to be implementable using existing standards rather than inventing new primitives. Z-TAS defines how identity, ownership transfer, bootstrap configuration, evidence, policy authorization, and observability can be integrated into one lifecycle model appropriate for million-device smart cities.

4.1 Architectural planes

Plane A — Identity and provenance (manufacture to warehouse).

Devices ship with a unique identity bound to hardware-protected keys (secure element, TPM, eSIM secure enclave, or equivalent). Baseline device capabilities include secure storage, unique credentials, secure update, and disclosure resistance, aligned to ETSI consumer IoT baseline requirements and NIST IoT capability baselines (ETSI, 2020; NISTIR, 2020; NIST, 2021a). For high-risk devices (e.g., cameras in public spaces), provenance should also include supplier identity and version lineage to support supplier assurance and vulnerability response, consistent with ECC's third-party and vulnerability expectations (NCA, 2024a).

Plane B — Ownership transfer and bootstrap (warehouse to field activation).

On first network contact, devices are imprinted into the operator domain using a late-binding process. Voucher-based bootstrapping (BRSKI) enables a device to join the correct domain without installers handling domain secrets (IETF, 2021). FIDO Device Onboard supports transfer-of-ownership onboarding where the device contacts rendezvous services and receives an owner-defined "service information" bundle to complete provisioning (FIDO Alliance, 2022). Where constrained device management is needed, LwM2M bootstrap servers can deliver initial configuration parameters and access control settings (OMA SpecWorks, 2022). Industrial best-practice guidance highlights that late binding is a core property for scalable provisioning because it separates manufacturing from operational system selection (IIC, 2022).

Plane C — Evidence and attestation

After bootstrap, devices provide evidence of software/firmware state and relevant posture claims. The RATS architecture defines roles and the appraisal model needed to make attestation composable and auditable (IETF, 2023). EAT tokens can encode attestation claims in a verifiable structure that can be used by relying parties to enforce policy decisions (IETF, 2025). For smart cities, this plane supports "trust but verify" onboarding: enrollment does not automatically grant long-lived privileges; privileges are conditioned on fresh evidence and maintained through periodic checks. The review finds that without evidence freshness, onboarding becomes brittle: devices can drift, be partially compromised, or be downgraded without detection (Kuang et al., 2022).

Plane D — Policy-driven authorization and segmentation (service enablement).

Z-TAS applies Zero Trust principles to device authorization. A device identity plus evidence is evaluated against policy rules to determine allowed flows (telemetry upload, command execution, video streaming, firmware update). Zero Trust guidance emphasizes explicit verification and least privilege, which translates naturally into per-flow authorization for IoT services (NIST, 2020). At smart-city scale, policy is reinforced by network segmentation and service isolation. Network slicing literature suggests that beyond-5G slicing can support differentiated security and performance requirements for distinct smart-city service classes, such as critical infrastructure monitoring versus public Wi-Fi sensors (Rafique et al., 2025). Policy and segmentation together reduce blast radius and help align compliance requirements with service criticality.

Plane E — Observability, audit evidence, and lifecycle governance.

Z-TAS treats onboarding as a governance process that produces evidence. All enrollment events, ownership changes, configuration baselines, attestation appraisals, and policy decisions are logged, retained, and reportable. This plane is essential for Saudi compliance alignment: ECC requires monitoring, logging, and auditability; CCC extends these obligations to cloud services; NDMO requires stewardship, classification, and retention; and PDPL requires accountability and protection measures for personal data (NCA, 2024a; NCA, 2024b; NDMO, 2021; SDAIA, 2023). Importantly, Plane E also supports operational resilience: fleet operators can perform cohort-level analytics to detect drift, vulnerabilities, or anomalous behavior across device populations.

4.2 Design rules derived from the corpus

The review yields seven practical design rules for million-device smart cities:

DR1 — Prefer late binding to pre-provisioned domain secrets. Voucher or transfer-of-ownership onboarding reduces installer trust and supply-chain exposure (IETF, 2021; FIDO Alliance, 2022).

DR2 — Bind enrollment to asset inventory. Every onboarding event must create or update an authoritative asset record; otherwise, "shadow devices" appear that cannot be governed (NCA, 2024a; NDMO, 2021).

DR3 — Require freshness for posture evidence. Attestation evidence must be time-bound and appraised under a defined verifier role (IETF, 2023; Kuang et al., 2022).

DR4 — Make policy decisions explicit and auditable. Authorization should be expressed as decisions with inputs (identity, evidence, context) and outputs (allowed flows), enabling audit and incident review (NIST, 2020; NCA, 2024a).

DR5 — Treat firmware update as a security dependency of onboarding. Secure updates are required to remediate vulnerabilities; firmware update architectures and manifests provide a standardized basis for update integrity (IETF, 2021; IETF, 2021b).

DR6 — Use cohort-based governance. Millions of devices require policy, evidence, and compliance reporting at cohort level (by device type and risk class) while preserving device-level traceability (IIC, 2022).

DR7 — Align cloud ingestion to identity and evidence checks. For cloud-native smart-city platforms, CCC implies that devices should not be granted ingestion privileges without verified identity and policy controls (NCA, 2024b).

V. COMPLIANCE MAPPING TO SAUDI SMART-CITY GUIDANCE

Saudi programs typically require that smart-city systems align with national cybersecurity and data governance instruments. This section translates those obligations into onboarding-relevant controls. The mapping is expressed at the level of "what must be controlled and evidenced," because implementation details will vary across vendors and architectures.

5.1 NCA Essential Cybersecurity Controls (ECC-2:2024)

ECC sets minimum cybersecurity requirements across domains including governance, defense, resilience, and third-party assurance (NCA, 2024a). For onboarding, ECC implies:

- Identity and access management: enforce unique device identities and least-privilege access to management systems. Evidence includes certificate issuance logs, access policy baselines, and approval trails for ownership changes.
- Cryptography and key management: require secure key storage, rotation, revocation, and controlled use of cryptographic material. Evidence includes key

lifecycle records and cryptographic configuration baselines.

• Monitoring and incident readiness: require centralized logging and monitoring of onboarding and device actions, supporting detection of compromised devices and anomalous enrollments. Evidence includes onboarding event logs and correlation identifiers linking devices to incidents.

• Third-party and supply-chain management: require supplier assurance and vulnerability response, motivating provenance linkage and update capability (NCA, 2024a).

In Z-TAS terms, ECC touches all planes (A–E), but it concentrates strongly on Plane E (monitoring/auditability) and Plane D (access control and segmentation).

5.2 NCA Cloud Cybersecurity Controls (CCC-2:2024)

CCC defines cloud security responsibilities and control expectations for cloud usage (NCA, 2024b). For smart-city onboarding, CCC implies that:

• Device ingestion platforms must be secured as cloud services with monitoring, access control, and key management.

• Data flows from devices to cloud must be governed by policy and logging, and cloud tenants must configure security controls to meet compliance requirements.

• Cloud-based provisioning services should integrate with identity and evidence mechanisms to prevent unauthorized device enrollment.

This aligns primarily to Plane B (bootstrap via cloud services), Plane D (policy authorization), and Plane E (cloud logging and audit).

5.3 NDMO data management standards (2021)

NDMO standards articulate data governance requirements including classification, stewardship, retention, and quality (NDMO, 2021). For onboarding, this means that device telemetry, video streams, and operational logs are governed datasets. Onboarding controls should therefore:

• Associate devices with data classification and purpose tags at enrollment.

• Ensure traceability from device identity to datasets and derived analytics outputs.

• Apply retention and deletion policies to device data, including onboarding evidence, consistent with governance rules.

NDMO mapping primarily reinforces Plane E (evidence retention) and Plane D (purpose-limited policies controlling data flows).

5.4 PDPL (2023)

PDPL establishes obligations to protect personal data and defines controller responsibilities (SDAIA, 2023). For smart cities, cameras, mobility sensors, and smart meters can directly or indirectly relate to individuals. PDPL-aligned onboarding therefore requires:

• Purpose limitation: the device's permitted data flows and analytics uses must match declared purposes and authorized roles.

• Access control and minimization: limit who can access sensitive data streams; enforce least privilege; and log access for accountability.

• Secure processing and incident response: ensure technical and organizational measures to protect personal data and support incident handling.

PDPL mapping concentrates on Plane D (policy-driven access) and Plane E (audit trails and accountability).

5.5 CST IoT Regulations (2024)

CST IoT Regulations are designed to regulate IoT services in KSA and strengthen the regulatory landscape for IoT (CST, 2024). From an onboarding standpoint, CST reinforces obligations on service providers and ecosystem participants to implement secure provisioning, maintain security governance, and support compliance expectations across connectivity and service layers.

5.6 Digital government governance structures

Smart-city platforms often integrate with government digital services. The Digital Government Authority's regulatory framework provides an organizing structure for digital government compliance and reinforces the need for consistent governance and standardized documentation (DGA, 2023). For onboarding, this translates into standardized evidence artifacts and service catalog governance at Plane

5.7 Synthesis: compliance-by-design evidence artifacts

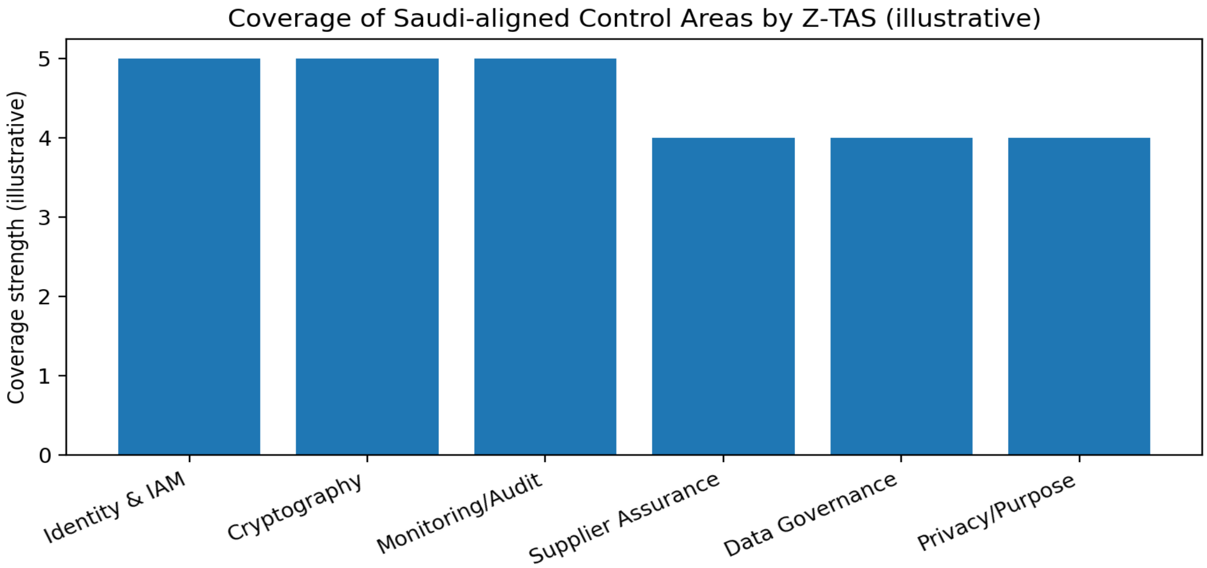
The mapping implies a concrete evidence package that smart-city operators should be able to produce on demand:

(1) Identity lineage record: device identity, supplier provenance, cohort classification.
(2) Ownership and enrollment record: voucher/transfer evidence, timestamps, approving authority.
(3) Configuration baseline: initial policy and config parameters applied at bootstrap.
(4) Attestation history: evidence tokens and appraisal decisions with freshness metadata.
(5) Access decision logs: per-flow authorization outcomes, including exceptions and overrides.
(6) Data governance tags and retention mapping: classification, purpose tags, and retention policies linked to device and datasets.

These artifacts align with ECC/CCC auditing needs, NDMO stewardship, and PDPL accountability.

Table 3. Mapping Saudi guidance to onboarding controls and evidence artifacts.

Saudi Instrument	Onboarding-relevant expectations	Z-TAS Evidence Artifacts (examples)
NCA ECC-2:2024	IAM, cryptography, monitoring, incident readiness, supplier assurance	Identity lineage, enrollment logs, policy baselines, monitoring records
NCA CCC-2:2024	Cloud governance, secure ingestion services, logging and key control	Cloud provisioning audit trail, ingestion policies, key mgmt records
NCA IoT Cybersecurity Guidelines (2024)	IoT-specific secure provisioning and lifecycle security controls	Device capability baseline, secure onboarding workflow evidence
NDMO Standards (2021)	Data classification, stewardship, retention, quality and governance	Data purpose tags, retention mappings, dataset lineage links
PDPL (2023)	Personal data protection, accountability, access control, purpose limitation	Access decision logs, minimization controls, privacy impact records



VI. DISCUSSION

Unique Findings, Practical Implications, and Research GapsBased on system-of-systems onboardings (Maksuti et al., 2021), attestation architecture designs based upon evidence-driven attestation (IETF, 2023), and authorization design principles based upon Zero Trust (NIST, 2020), the novel aim of review work is the development of a model onboarding technique that meets million-scale automation and Saudi compliance requirements. The primary innovative outcome is the design of the Zero

Touch Assurance Stack (Z-TAS) and the Saudi compliance mapping associated with "controls."

6.1 Smart energy management of buildings

Implication 1 — Multi-layer onboarding is required in smart cities.

It is rare for a device to exist in a solitary manner; it communicates through gateways, platforms, and microservices. When a device is securely enrolled but a gateway/service layer is unmanaged, assumptions of trust break down. The onboard controller concept and registry patterns are of greater importance in smart cities than single-tenant IoT systems (Maksuti et al. 2021; IIC, 2022).

Implication 2 – Ownership transfer is the security choke point.

Often, IoT device deployment incidents are related to the "handoff point," which involves changing ownership of the device from the manufacturer to the integrator and finally to the operator. The late-binding approach resulted in low installer trust and assurance of the legitimacy of domains through cryptographic evidence, as offered by IETF in 2021 and FIDO Alliance in 2022. The implementation in Saudi Arabia will therefore facilitate governance, as changes of ownership can now be recorded.

Implication 3: Attestation makes possible not only security, as compliance. By requireing

Saudi is dependent on effective monitoring and proof of compliance. Attestation makes enrollment an ongoing control rather than an initial one. The RATS systems break down the evidence creation and assessment phase and allow various implementations to work together (IETF, 2023; Kuang et al., 2022).

Implication 4

Policy bridges the chasm between security and privacy.

PDPL & NDMO are primarily about data processing and data governance in a specific manner. A Zero Trust policy solution represents a structured means of enforcing purpose restriction & least privilege in particular high-risk data streams like video analysis (NIST, 2020; SDAIA, 2023).

Implication 5: While network isolation can be a complement to identity, it cannot instead provide identity itself.

Network slicing and segmentation both work to reduce blast radius and enable variable service class enforcement, but they cannot prevent counterfeit device subscription. Identity, ownership transfer, and evidence requirements should be enforced before giving network and/or application privileges to the device (NCA, 2024a).

6.2 Recommendations

From the synthesis and Saudi mapping conducted, we propose the following phased roadmap in implementing smart city initiatives:

Stage 1 - Foundations of identifying/asset inventory. Implement device capability baseline standards such as ETSI, 2020, and NISTIR, 2020. Each device should then have a distinctive, hardware-based identity tied to their asset.

Stage 2 - Implement late-binding onboarding (Plan B). Voucher/Ownership Transfer onboarding (IETF, 2021; FIDO Alliance, 2022) can lower installer trust and facilitate drop-shipped scale.

Stage 3-Integrate Evidence-Based Authorization (Planes C/D). Use RATS-based attestation and authorization workflows (IETF, 2023; IETF, 2025) and tie it with policy engines compatible with Zero Trust (NIST, 2020

Stage 4 - Generate operational-level evidence of compliance. ECC/CCC NDMO PDPL-based reproducible evidence artifacts are created. Cohort-level reporting support is included in the solution so that it is ready for audits. 7. Conclusion

This systemic literature review brings together research and best practices from 2020 to 2025 to provide a roadmap for secure onboarding and direct provisioning from a smart city perspective, and specifically correlates with Saudi national best practice guidelines. Within the scholarly literature, the term 'zero-touch' arises as more than a tool for automation. By doing so as a best practice of late binding, evidence-based authorization, and logging support, the chance of credential theft risks ceases to exist. These four primitives provide the robust onboarding process all the time: device-anchored identity, late-binding ownership transfer, posture assertion as evidence, and policy-driven authorization in the context of Zero Trust. These primitives, when combined to form the Zero Touch Assurance Stack (Z-TAS), provide the lifecycle model that can be implemented for heterogeneous smart city fleets and composite systems of systems, such as gateways and edge computing nodes, into the systems of systems category. The Saudi compliance mapping also includes longevity of evidence, which has been given less importance by most technical solutions. As this review is systematic and not empirical, it shall not refer to specific measured outcomes of single city deployments. Rather, it serves as an activity-oriented synthesis that can be carried out following standardized procedures such as BRSKI, FDO, LwM2M bootstrap, RATS/EAT, and SUIT, and adapted based on real-world conditions as needed. Future research should target the following areas of significance: (i) federation architectures for inter-domain trust within utility, transport, and public-safety environments, (ii) revocation and recovery playbooks that support flexible revocation and recovery actions while maintaining essential services, and (iii) metrics for ascertaining the freshness of evidence and efficacy of policies in the fleet domain.

REFERENCES

[1] Communications, Space & Technology Commission (CST). (2024). IoT Regulatory Framework (revised) (summary and compliance expectations). CST.

[2] Digital Government Authority (DGA). (2023). Regulatory framework for digital government. DGA.

[3] ENISA. (2021). Cybersecurity for smart cities and the Internet of Things: Threat landscape and good practices. European Union Agency for Cybersecurity.

[4] ETSI. (2020). ETSI EN 303 645 V2.1.1: Cyber Security for Consumer Internet of Things: Baseline Requirements. European Telecommunications Standards Institute.

[5] FIDO Alliance. (2022). FIDO Device Onboard (FDO) Specification (Version 1.1). FIDO Alliance.

[6] GSMA. (2021). IoT SAFE: Remote SIM Provisioning Security Add-On for IoT (Specification). GSMA.

[7] GSMA. (2024). GSMA IoT Security Guidelines. GSMA.

[8] Industrial Internet Consortium (IIC). (2022). Best practices for onboarding and lifecycle management in Industrial IoT (White paper). IIC.

[9] IETF. (2021). Bootstrapping Remote Secure Key Infrastructures (BRSKI) (RFC 8995). Internet Engineering Task Force.

[10] IETF. (2021). A Firmware Update Architecture for Internet of Things (IoT) Devices (RFC 9019). Internet Engineering Task Force.

[11] IETF. (2022). A Concise Binary Object Representation (CBOR) Manifest for Secure IoT Updates (SUIT Manifest) (RFC 9124). Internet Engineering Task Force.

[12] IETF. (2023). Remote Attestation Procedures (RATS) Architecture (RFC 9334). Internet Engineering Task Force.

[13] IETF. (2025). The Entity Attestation Token (EAT) (RFC 9711). Internet Engineering Task Force.

[14] IETF. (2025). Media Types for Entity Attestation Token (EAT) (RFC 9782). Internet Engineering Task Force.

[15] ISO/IEC. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. International Organization for Standardization.

[16] ISO/IEC. (2022). ISO/IEC 27400:2022 Cybersecurity—Internet of Things (IoT) security and privacy—Guidelines. International Organization for Standardization.

[17] Maksuti, S., Tauber, M., Shahid, A., & Fitzek, F. H. P. (2021). An automated and secure onboarding architecture for system of systems. IEEE Access, 9, 114062–114082.

[18] National Cybersecurity Authority (NCA). (2024a). Essential Cybersecurity Controls (ECC-2:2024). NCA.

[19] National Cybersecurity Authority (NCA). (2024b). Cloud Cybersecurity Controls (CCC-2:2024). NCA.

[20] National Cybersecurity Authority (NCA). (2024c). Internet of Things (IoT) cybersecurity guidelines. NCA.

[21] National Data Management Office (NDMO). (2021). Data management and personal data protection standards. SDAIA/NDMO.

[22] National Institute of Standards and Technology (NIST). (2020). Zero Trust Architecture (SP 800-207). U.S. Department of Commerce.

[23] National Institute of Standards and Technology (NIST). (2021a). Core cybersecurity features for

IoT devices: Baseline requirements (NISTIR 8259A). U.S. Department of Commerce.

[24] National Institute of Standards and Technology (NIST). (2021b). IoT device cybersecurity guidance for the federal government: Establishing IoT device cybersecurity requirements (SP 800-213). U.S. Department of Commerce.

[25] National Institute of Standards and Technology (NIST). (2022). Secure software development framework (SSDF) (SP 800-218). U.S. Department of Commerce.

[26] OMA SpecWorks. (2022). Lightweight Machine to Machine Technical Specification (LwM2M) (Version 1.2.1). OMA SpecWorks.

[27] OECD. (2021). Enhancing the security of the Internet of Things: Policy and technical approaches. OECD Publishing.

[28] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71.

[29] Saudi Data & AI Authority (SDAIA). (2023). Personal Data Protection Law (PDPL) and implementing regulation (English translation). SDAIA.

[30] ENISA. (2022). ENISA threat landscape for the Internet of Things. European Union Agency for Cybersecurity.

[31] National Institute of Standards and Technology (NIST). (2024). IoT device cybersecurity guidance for the federal government: IoT device cybersecurity requirement catalog (SP 800-213A). U.S.