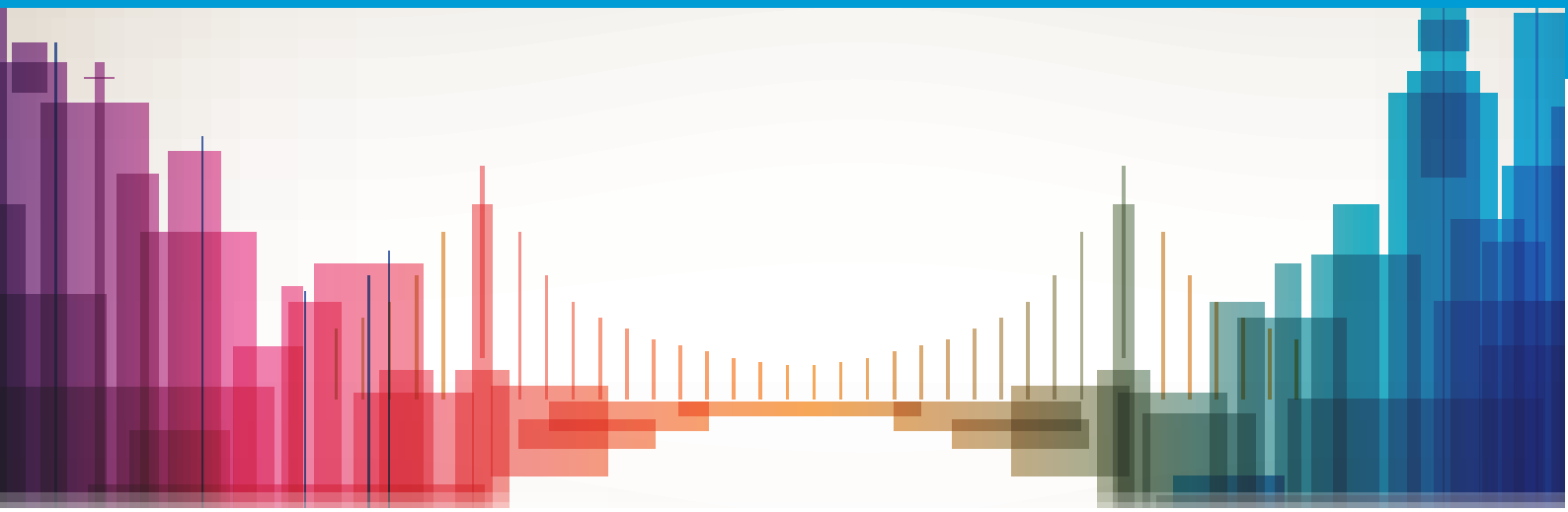
Trust at City Scale: Securing Digital Public Infrastructure in Smart Sustainable Cities



Convention on Biological Diversity

United Nations ECLAC

Food and Agriculture Organization of the United Nations

ITU

UN-HABITAT

UNDP

United Nations Economic Commission for Africa

UNECE

UNIDO

unesco

UN environment programme

UNEP FINANCE INITIATIVE

United Nations Framework Convention on Climate Change

unitar United Nations Institute for Training and Research

UNFPA

United Nations | Department of Economic and Social Affairs

UNJSPF United Nations Joint Staff Pension Fund

UN OFFICE 4 PARTNERSHIPS

UNU EGOV

UN Tourism

WORLD METEOROLOGICAL ORGANIZATION





Trust at City Scale: Securing Digital Public Infrastructure in Smart Sustainable Cities

Foreword

This publication was developed within the framework of the United for Smart Sustainable Cities (U4SSC) initiative.

Acknowledgements

The development of this deliverable was led and coordinated by Leyi Zhang (ZTE Corporation, China).

This publication was authored by Leyi Zhang (ZTE Corporation, China), Li Ping (ZTE Corporation, China), Xia Wang (ZTE Corporation, China), Ramy Ahmed Fathy (Egypt) and Mingke Ma (Oxford University).

The authors would like to thank the following contributing individuals: Xiongwei Jia (China Unicom, China), Keri A. Kitson (K. Kitson & Co, Trinidad) and Yonah Welker (MIT).

The authors wish to thank the U4SSC management team: Okan Geray (U4SSC Chair), Ramy Ahmed Fathy, Giampiero Bambagioni, Paolo Gemma, Wendy Teresa Goico Campagna, Tania Marcos and Emily Royall (U4SSC Vice-Chairs) for their assistance and contributions.

The authors also extend their gratitude to the contributing organizations along with their representatives: Oliver Hillel from the Convention on Biological Diversity (CBD), Lucy Winchester and Vera Kiss from the Economic Commission for Latin America and the Caribbean (ECLAC), Nevena Alexandrova from the Food and Agriculture Organization (FAO), Cristina Bueti from the International Telecommunication Union (ITU), Deniz Susar from United Nations Department of Economic and Social Affairs (UNDESA), Iryna Usava from the United Nations Development Programme (UNDP), James Murombedzi from the United Nations Economic Commission for Africa (UNECA), Dario Liguti and Tea Aulavuo from the United Nations Economic Commission for Europe (UNECE), Guilherme Canela from the Regional Bureau for Sciences in Latin America and the Caribbean of the United Nations Educational, Scientific and Cultural Organization (UNESCO), Gulnara Roll from United Nations Environment Programme (UNEP), Matthew Ulterino from the United Nations Environment Programme Finance Initiative (UNEP-FI), Motsomi Maletjane from the United Nations Framework Convention for Climate Change (UNFCCC), Soren Thomassen from United Nations Population Fund (UNFPA), Aline Machado da Matta and Isabel Wetzel from the United Nations Human Settlements Programme (UN-Habitat), Katarina Barunica Spoljaric and Nicholas Dehod from the United Nations Industrial Development Organization (UNIDO), Ebru Canan-Sokullu from the United Nations Institute for Training and Research (UNITAR), Dino Cataldo Dell'Accio from United Nations Joint Staff Pension Fund (UNJSPF), William Kennedy from the United Nations Office for Partnerships (UNOP), Soumaya Ben Dhaou from the United Nations University – Operating Unit on Policy-Driven Electronic Governance (UNU-EGOV), Roberta Boscolo from World Meteorological Organization (WMO) and Sandra Carvao from the World Tourism Organization (UN Tourism).

Disclaimer

The opinions expressed in this publication are those of the authors and do not necessarily represent the views of their respective organizations or U4SSC members. In line with the U4SSC principles, this report does not promote the adoption and use of Smart City technology. It advocates for policies encouraging responsible use of information and communications technologies (ICTs) that contribute to the economic, environmental and social sustainability as well as the advancement of the 2030 Agenda for Sustainable Development and the Pact for the Future and its Global Digital Compact.

ISBN

978-92-61-43641-4 (Electronic version)
978-92-61-43651-3 (EPUB version)



This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 3.0 IGO license (CC BY-NC-SA 3.0 IGO).

For more information, please visit https://creativecommons.org/licenses/by-nc-sa/3.0/igo/

© CBD, ECLAC, FAO, ITU, UNDESA, UNDP, UNECA, UNECE, UNESCO, UNEP, UNEP-FI, UNFCCC, UNFPA, UN-Habitat, UNIDO, UNITAR, UNJSPF, UNOP, UNU-EGOV, WMO and UN Tourism.



Contents

Abbreviations and acronyms vii

Executive summary ix

1 Introduction 1

2 Scope 2

3 Definitions 2

4 Overview 2

4.1 Introduction of Digital Public Infrastructure 2

4.2 DPI in Smart Sustainable Cities 3

4.3 Components of DPI in SSC 5

5 Security threat and risk analysis for DPI in SSC 7

5.1 Threat landscape for DPI in SSC 7

5.2 Risk analysis for DPI in SSC 14

6 Security Framework for DPI in SSC 17

6.1 Lifecycle-embedded security framework for DPI in SSC 17

6.2 Security control classification across the DPI lifecycle 20

7 Security guidelines for DPI in SSC 22

7.1 Architectural & technical measures 23

7.2 Security operation & continuous monitoring 27

7.3 Data governance, protection & privacy 30

7.4 Countering emerging & future threats 34

Appendix I: Best Practices of Secure DPI Implementation 37

Bibliography 41

List of figures and tables

Figures

Figure 1: Ecosystem of DPI for SSC (Source: Author) 5
Figure 2: Lifecycle-embedded security framework for DPI in SSC (Source: Author) 18

Tables

Table 1: Common Cybersecurity Threats to city DPI 8
Table 2: Threats to Data Security and Privacy 9
Table 3: External AI-Enabled Threats to DPI 12
Table 4: Threats to AI-Integrated DPI Systems 13
Table 5: Cyber Threats Posed by Quantum Computing 14
Table 6: Strategic and High Impact Attack Vectors and Strategic Effects by DPI Target 16
Table 7: Security control dimensions mapping into DPI lifecycle phases 20
Table 8: A Layered Defense-In-Depth Model for DPI Architecture 23
Table 9: AI Security Governance Recommendations for DPI 34
Table I.1: Best Practices of Secure DPI Implementation Globally 37

Abbreviations and acronyms

Abbreviation	Full form
ABAC	Attribute-Based Access Control
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
BCP	Business Continuity Plan
CERT	Computer Emergency Response Team
CI/CD	Continuous Integration and Continuous Delivery
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CTO	Chief Technology Officer
DDoS	Distributed Denial of Service
DPI	Digital Public Infrastructure
ECC	Elliptic Curve Cryptography
EDR	Endpoint Detection and Response
FIDO2	Fast Identity Online 2
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
IAM	Identity and Access Management
ICT	Information and Communication Technology
IdP	Identity Provider
IDS	Intrusion Detection System
IOC	Indicator of Compromise
IoT	Internet of Things
IPsec	Internet Protocol Security
IPS	Intrusion Prevention System
JEA	Just-Enough Administration
JIT	Just-in-Time
LoRaWAN	Long Range Wide Area Network
M2M	Machine-to-Machine
MFA	Multi-Factor Authentication
ML	Machine Learning
MPC	Secure Multi-Party Computation
mTLS	Mutual Transport Layer Security
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond

Abbreviation	Full form
NDR	Network Detection and Response
NETCONF	Network Configuration Protocol
NIST	National Institute of Standards and Technology
OAuth	Open Authorization
OT	Operational Technology
PAM	Privileged Access Management
PETs	Privacy-Enhancing Technologies
PKI	Public Key Infrastructure
PoLP	Principle of Least Privilege
PQC	Post-Quantum Cryptography
PSIRT	Product Security Incident Response Team
RBAC	Role-Based Access Control
RPO	Recovery Point Objective
RSA	Rivest–Shamir–Adleman
RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SBOM	Software Bill of Materials
SIEM	Security Information and Event Management
SMS	Short Message Service
SSC	Smart Sustainable City
SSH	Secure Shell
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOTP	Time-Based One-Time Password
TTPs	Tactics, Techniques and Procedures
U4SSC	United for Smart Sustainable Cities
VPN	Virtual Private Network
XDR	Extended Detection and Response
YANG	Yet Another Next Generation
ZTA	Zero-Trust Architecture

Executive summary

Cities are quietly becoming dependent on a shared digital layer, digital identity, payments, data exchange, service portals, urban IoT, that now sits underneath transport, health, housing, energy and social protection. When that layer fails, it is not an IT incident. It is residents unable to prove who they are, benefits not paid, traffic signals unresponsive, a health record system offline. This framework is the first practical, city-scale security guide for that layer. It explains how urban Digital Public Infrastructure (DPI) differs from national DPI, maps the threats cities actually face, including AI-driven attacks and future quantum decryption, and sets out controls a city can embed from the first day of a project to the last day of operation.

Why this document matters now

DPI has moved from national systems into the street. DPI was designed and deployed at national scale: one identity system, one payment rail, centralised data centres. Cities are now building on top of it and around it, with tens or hundreds of thousands of edge devices, real-time control systems and dozens of operators. The security assumptions do not transfer cleanly.

The blast radius is different. The document makes a point city leaders will recognise immediately: severity is not determined by how sophisticated the attack was, but by how many people it locks out. A simple credential-stuffing attack on a commercial app is an incident. The same attack on the identity system residents use for benefits, voting registration and healthcare is a civic emergency. The framework calls this an impact-anchored view of risk, and it changes how cities should prioritise spending.

Cyber incidents in cities become physical incidents. Urban DPI touches water treatment control, district heating, building management and traffic signals. A compromise can contaminate a water supply, lock a building or gridlock a district. The framework treats city DPI as critical infrastructure, on the same footing as physical utilities.

A security failure can also be an exclusion event. This is the document's most distinctive contribution and its strongest message for city politics. Controls that assume a fixed address, a personal smartphone, a formal job or perfect connectivity will fail residents in informal settlements, migrant communities, shared housing and the informal economy, and will do so silently. The framework insists that security must protect systems from attack and protect residents from being shut out, profiled, coerced, or having service-delivery data repurposed for enforcement.

The clock on two emerging threats is already running. AI attacks are becoming autonomous and adaptive, and adversaries are already harvesting encrypted data today to decrypt once quantum computers mature. Both require decisions cities take now, in procurement and architecture, not later.

What makes this framework different

It is built specifically for the urban context, around seven features that separate city DPI from national DPI:

- **Edge density** – attack surface spread across the whole urban fabric, where physical proximity to a device is itself an attack vector.
- **Real-time dependencies** – traffic control and emergency dispatch operate in milliseconds, so some standard security controls are too slow to use.
- **Cyber-physical convergence** – digital compromise produces physical harm.
- **Multi-stakeholder complexity** – municipal agencies, utilities, private platforms, academia and residents share a system no single body fully controls.
- **Sustainability-driven data intensity** – energy, mobility, air quality and social service data collected at unprecedented volume.
- **Pilot-to-scale speed** – experimental deployments reaching production before full security review.
- **Socio-spatial heterogeneity** – formal and informal city conditions side by side.

What's inside

Section	What a city gets
Threat analysis	Six reference tables mapping each threat to the affected security attribute *and* the specific city services at risk – ransomware, DDoS, supply chain, insider risk, data breaches, profiling, AI-enabled attacks, model poisoning, deepfakes, quantum decryption.
Risk model	An impact-anchored method that ranks risk by population-scale consequence, plus explicit treatment of municipal reality: constrained budgets, weak procurement capacity, fragmented authority, public-private delivery.
Lifecycle framework	Security embedded across five phases – conception and scoping, strategy and design, development, deployment, operations and maintenance – with cross-cutting vulnerability management and incident response.
Control matrix	Every phase mapped across organisational, procedural and technical controls, so accountability, process and technology are all assigned. Usable directly as a checklist.
Technical guidance	Seven-layer defence-in-depth model, Zero-Trust architecture adapted to urban scale, secure integration and API protocols, resilience and continuity design.
Data protection	Encryption, HSMs, integrity verification, identity and access management, plus privacy-enhancing technologies: differential privacy, secure multi-party computation, homomorphic encryption, trusted execution environments, zero-knowledge proofs.
City-specific safeguards	Fallback and offline access channels, accountable assisted-access rules for intermediaries, grievance and redress mechanisms, inclusion monitoring, and community communication during incidents.

Section	What a city gets
Emerging threats	Ten AI security governance recommendations for DPI, and a structured post-quantum cryptography migration path starting with a crypto inventory.
Global practice	Eight case studies – Estonia X-Road, India Aadhaar/UPI, Brazil Pix, Singapore Singpass, Japan My Number, EU eIDAS/GDPR, US Login.gov, China eID – each assessed honestly for what transfers to a city and what does not.

How cities can use it

1. As a self-assessment baseline. Run the control matrix against an existing DPI programme to find which lifecycle phases have no assigned owner.
2. As procurement language. Convert the technical guidance into tender requirements: machine-readable SBOMs, phishing-resistant MFA, mTLS, PQC-readiness clauses in vendor contracts.
3. As a budget case. The impact-anchored risk model gives finance committees and councils a defensible basis for prioritising spend on the systems with the widest civic reach.
4. To assign accountability across a fragmented ecosystem. The stakeholder and control mapping helps a city write down who is responsible for what across agencies, utilities and private operators – before an incident, not during one.
5. To stand up response capability. The framework recommends city-level CERT/CSIRT structures, coordinated vulnerability disclosure, tabletop exercises and cross-city collaboration.
6. To design for inclusion from the start. The safeguards section gives concrete requirements: alternative identity proofing, non-address-based access, low-bandwidth channels, audited assisted enrolment, and monitoring of authentication failures and service-denial complaints by neighbourhood.
7. To start the quantum transition. Crypto inventory, data classification by confidentiality shelf-life, infrastructure assessment, vendor roadmaps, workforce training.
8. To align city and national policy. The framework maps onto national and international regimes, helping cities integrate with sovereign identity infrastructure without duplicating or contradicting it.

Who it's for

- Mayors, deputy mayors and city councils – strategic framing, risk prioritisation, public accountability.
- City CIOs, CTOs, CISOs and IT teams – architecture, controls, operations.
- Procurement and contracting officers – vendor requirements and third-party risk.
- National regulators and ministries – city-level implementation of national DPI and cybersecurity policy.

- Utilities, transport authorities and PPP operators – shared responsibility in multi-operator environments.
- Technology providers and system integrators – the security expectations cities will bring to market.
- Civil society, academia and community organisations – oversight, grievance handling, and inclusion assessment.
- Media and public communicators – a plain account of why urban digital infrastructure security is a public interest issue.

Key messages

- Urban DPI is critical infrastructure. It deserves the same security posture as water and power.
- Severity is measured in people, not packets. A modest attack on a foundational city system is a civic crisis.
- Security is inseparable from inclusion. A control that locks out a resident without a fixed address has failed, even if no attacker was involved.
- Trust also depends on how DPI is governed. Residents need transparency about how systems work, clear accountability when they fail, a say in how they are designed and run, and protection of their digital rights.
- Security cannot be added at launch. It has to be designed in at conception and maintained for the life of the system.
- Two clocks are already running – autonomous AI attacks, and encrypted data being harvested today for decryption tomorrow.

1 Introduction

The High-Level Framework of Digital Public Infrastructure (DPI) Security has been developed under the United for Smart Sustainable Cities (U4SSC) initiative to address the pressing need to secure the digital systems underpinning essential public services and societal functions. As DPI becomes a foundational digital layer supporting smart sustainable cities – facilitating digital identity, payments, healthcare and citizen engagement – its security, resilience and trustworthiness are paramount.

While DPI has traditionally been implemented at national scale, its deployment in smart sustainable cities (SSCs) environments introduces distinct characteristics, including highly distributed edge infrastructures, real-time operational dependencies, deep cyber-physical convergence, multistakeholder governance, sustainability-driven data intensity, and rapid innovation cycles. These characteristics significantly expand the attack surface and increase the systemic impact of potential security failures.

This document provides a comprehensive, risk-based and actionable security framework to help smart cities and communities stakeholders fortify DPI against evolving cyberthreats and AI-driven attacks in SSCs. It integrates governance, technology and operational practices throughout the DPI lifecycle from conception and design to deployment, operations, and maintenance in smart cities and community systems applications and services. The framework follows a human rights-based approach, in line with UN-Habitat's people-centred smart cities approach. Privacy, non-discrimination, accessibility and equitable access to public services are principles that security measures must reinforce, rather than a separate set of concerns to be handled elsewhere.

Key features of the framework include:

- A structured threat analysis covering common, data-specific, and emerging threats such as AI-driven attacks and quantum computing risks for DPI in SSC.
- A security-embedded DPI lifecycle approach for SSC, with controls mapped to organizational, procedural, and technical dimensions across all lifecycle phases.
- A layered defense-in-depth architectural model, Zero-Trust principles for DPI in SSCs, practical measures for data protection, continuous monitoring and incident response, and explicit guidance on securing AI systems and transitioning to post-quantum cryptography.

Designed for policymakers, technology providers, regulators and civil society, this framework provides the foundational guidance for building secure and resilient DPI for SSCs. It enables stakeholders to systematically manage cyber-risks, implement robust technical and governance controls, and foster collaboration thereby ensuring that DPI systems remain trustworthy and capable of withstanding current and future security challenges.

2 Scope

This document provides a security framework and technical guidance to secure Digital Public Infrastructure (DPI) deployed in smart sustainable cities (SSC).

The scope of this document includes:

- Security threat and risk analysis relevant to DPI in SSC environments
- Security framework applicable to DPI for SSC
- Technical security guidelines for protecting DPI systems for SSC

3 Definitions

This document uses the following terms defined elsewhere:

- **Artificial intelligence (Recommendation ITU-T F.749.13)**: An interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence such as reasoning and learning.
- **Digital Public Infrastructure (OECD)**: Shared digital systems that are secure and interoperable and capable of supporting the inclusive delivery of, and access to, public and private services across society.
- **Smart Sustainable City (Recommendation ITU-T Y.4900)**: A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, efficiency of urban operation and services and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social, environmental and cultural aspects.

4 Overview

4.1 Introduction of Digital Public Infrastructure

Digital Public Infrastructure (DPI) refers to a set of shared, secure and interoperable digital systems designed to support broad access to public and private services [U4SSC–DPI–Framework]. It forms a shared digital layer that enables interoperability, secure data exchange, identity verification, payment processing, and trusted interactions across sectors.

DPI is characterized by its openness, modularity, and focus on enabling ecosystem innovation rather than providing end-to-end solutions. Unlike traditional digitization efforts that often result

in siloed, proprietary systems, DPI emphasizes the creation of shared, reusable infrastructure that can support multiple use cases across different sectors and jurisdictions. The global significance of DPI has been recognized across multiple international forums, including the United Nations Global Digital Compact (2024), which acknowledges DPI's potential to deliver services at scale and increase social and economic opportunities for all.

4.2 DPI in Smart Sustainable Cities

While DPI has traditionally been conceptualized and implemented at the national level, its deployment in SSC introduces distinct characteristics that fundamentally alter its technical architecture, operational requirements, and risk profile. These urban-scale systems exhibit seven defining features that differentiate them from generic national DPI implementations:

- **Urban density and edge distribution**: Cities concentrate large populations within geographically bounded areas, necessitating highly distributed, edge-heavy infrastructure. Unlike national DPI systems that rely primarily on centralized cloud data centers, DPI for SSC deploys tens or hundreds of thousands of edge nodes, including IoT sensors, smart cameras, autonomous vehicle roadside units, and building automation systems across the urban fabric. This density creates a massively distributed attack surface where physical proximity to devices becomes a viable attack vector, and the sheer scale of endpoints makes uniform security enforcement technically challenging.
- **Real-time operational dependencies**: Urban DPI systems must support time-critical functions that directly affect public safety and city operations. Traffic signal control, emergency response coordination, smart grid frequency regulation, and autonomous public transport systems operate at millisecond-to-second latencies. This real-time imperative contrasts sharply with national DPI systems and traditional security controls–such as deep packet inspection, behavioural analysis, or multihop authentication may not be applicable due to the latency they introduce.
- **Deep physical-digital convergence**: DPI for SSC directly interfaces with physical infrastructure: supervisory control and data acquisition systems controlling water treatment and distribution, industrial control systems managing district heating and cooling, building management systems regulating energy consumption, and automated environmental monitoring networks. This convergence transforms DPI from a purely information system into a cyber-physical system where cybersecurity incidents can cause physical impacts such as contaminated water supplies, building lockdowns, transportation gridlock or environmental hazards.
- **Multistakeholder complexity**: National DPI is characterized by relatively simple stakeholder topology–government providers and citizen users–with security responsibilities concentrated in sovereign institutions. Urban DPI, by contrast, functions within a complex ecosystem of municipal agencies, regulated utilities, private platform operators, academic research institutions, and citizens themselves. A single urban data exchange may involve data flows between city transportation departments, ride-sharing platforms, electric grid operators, weather services, and navigation applications. This multiplicity complicates trust establishment, liability allocation,

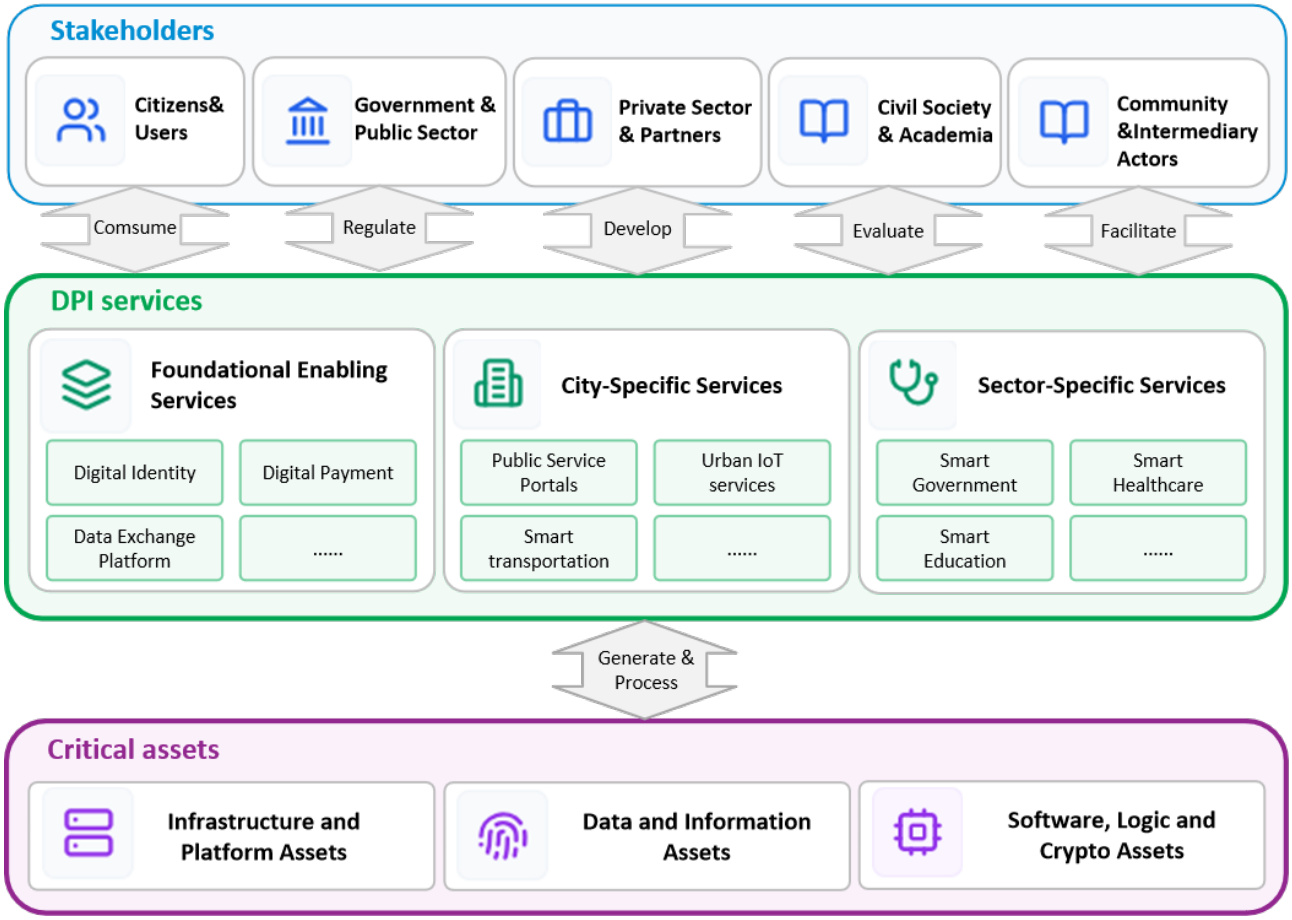
and security governance, as no single entity maintains comprehensive visibility or control over the entire data lifecycle. Within this ecosystem, local governments have a leadership role that sets them apart from other stakeholders. They may operate DPI directly, through municipal agencies or municipally owned companies, but they are also its stewards and coordinators: they set the terms on which other actors take part, allocate security and data-protection responsibilities among them, and remain accountable to residents for the services that DPI delivers. Making these responsibilities and accountability arrangements explicit is a precondition for effective security governance at city scale.

- **Sustainability-driven data intensity**: DPI for SSC is explicitly designed to measure, optimize and verify progress toward environmental and social sustainability goals. This purpose drives the collection of unprecedented volumes and varieties of data: real-time energy consumption at building and district levels, multimodal transportation patterns, air quality and noise pollution measurements, waste generation and recycling flows, and social service access patterns. Ensuring robust data security and privacy protection is essential to safeguard sensitive urban data, maintain public trust, and enable the responsible use of large-scale data for sustainable decision-making and long-term city resilience.
- **Rapid innovation and pilot-to-scale dynamics**: Cities increasingly function as innovation testbeds for emerging technologies. DPI for SSC frequently incorporates experimental deployments–autonomous delivery robots, AI-driven predictive maintenance, digital twins for urban planning, blockchain-based energy trading–that transition from pilot to production scale within compressed timelines. These technical innovations may create security issues since systems may achieve functional deployment before comprehensive security architecture review, and the experimental nature of components may preclude mature security validation.
- **Socio-spatial heterogeneity and urban informality**: DPI deployed in SSC operates across highly uneven urban environments, including formal and informal settlements, mixed land-tenure arrangements, formal and informal labour markets, formal and informal transport systems, unregistered micro-enterprises, shared housing, migrant populations, and residents without stable addresses or consistent access to formal documentation. These conditions affect how users authenticate themselves, access services, generate data, interact with intermediaries, and experience security and privacy risks. In such contexts, DPI security should not only protect digital systems from cyberattacks, but also prevent exclusion, coercion, misuse of service-delivery data, discriminatory profiling, and the repurposing of data for punitive or non-consensual enforcement purposes. The groups most exposed to these risks include residents of informal settlements, displaced populations and migrants, informal workers, women-led households, older persons, and persons with disabilities. Exclusion can arise, for example, when enrolment requires a formal address or tenure document, when service data on housing or livelihoods is shared with enforcement agencies, or when digital interfaces are not accessible to people with visual, hearing or cognitive impairments.

4.3 Components of DPI in SSC

DPI in SSC comprises a complex ecosystem of services, stakeholders and assets that together enable the delivery of digital services on an urban scale. Figure 1 illustrates this ecosystem, showing the three components and their interrelationship.

Figure 1: Ecosystem of DPI for SSC (Source: Author)



- **Involved stakeholders**

Stakeholders form the governance and participation dimension of DPI for SSC. Typical stakeholders include:

- **Citizens & users**: Citizens and users are the ultimate beneficiaries and primary service objects of city DPI. They are consumers of public services, generators of data, and participants in urban life.
- **Government & public sector**: The government and public sector are the primary stewards, regulators, and service providers of city DPI. They are responsible for policy formulation, infrastructure investment, service delivery, and ensuring that DPI serves the public interest.

Governments at both national and local levels are custodians of the public-interest data that DPI generates. This makes them responsible for its stewardship: ensuring that the data is used transparently and equitably to create public value, and being answerable to residents for how it is used.

- **Private sector & partners**: The private sector and partners are essential collaborators in building, operating, and innovating upon DPI. They bring technical expertise, investment capital, operational efficiency, and market-driven innovation.
- **Civil society & academia**: Civil society and academia provide independent expertise, ensuring that DPI development remains responsive to societal needs and values. They can also support outreach, assisted enrolment, grievance handling, public communication, and assessment of DPI security impacts in local contexts. Their role should go further than outreach and assessment, to include co-designing DPI services, monitoring their performance and impacts, providing independent oversight, and taking part in governance processes. Residents are more likely to trust systems they have helped to shape than systems they only receive services from.
- **Community & intermediary actors**: Community leaders, local associations, digital access points, service agents, informal transport operators, utility intermediaries, and civil society partners may mediate access to DPI-enabled services. They can support inclusion and last-mile delivery, but may also introduce risks of fraud, unauthorized data access, or accountability gaps. Like civil society, they should be involved in co-design and feedback processes, since they often know best where residents face barriers to access.

- **Key DPI services in SSC**

DPI services form the functional layer of DPI, supporting the daily lives of residents, the operations of businesses, and the functioning of government. Key DPI services in SSC can be categorized into 3 types:

- **Foundational enabling service**s: Foundational enabling services provide common, reusable capabilities that underpin all other digital services. Key services include but are not limited to: Digital Identity, Digital Payments, and data exchange platform.
- **City-specific services**: City-specific services are the application-layer DPI services directly for urban management and the daily life scenarios of citizens. Key services include but are not limited to: Public Service Portals, Urban IoT Services, and Smart transportation.
- **Sector-specific services**: Sector-specific services are the specialized DPI services designed for particular vertical domains. Key services include but are not limited to: Smart Government, Smart Health care, and Smart Education.

- **Critical assets**

Assets are the digital resources that DPI systems depend on to function, which need to be protected and managed effectively. Critical assets for DPI in SSC are categorized into three primary classes:

- **Infrastructure and platform assets**: Consolidating infrastructure and operational assets. This refers to the foundational digital platforms (e.g., core identity systems, data exchange platforms) and the cyber-physical systems they control (e.g., traffic signal control, smart grid regulation). The primary protection goal is **availability and service continuity**.
- **Data and information assets:** Consolidating identity, personal, financial, and geospatial data. This includes citizen identity records, biometric data, health information, transaction histories, **urban development and geospatial data**. These assets may require enhanced protection where their misuse could expose residents or communities to exclusion, profiling, coercion, or commercial exploitation. The primary protection goal is **confidentiality and privacy.**
- **Software, logic and crypto assets**: Refining the definition of specialized digital components. This refers to the logic layer enabling security and functionality, including encryption keys, AI models, API specifications, source code, and core algorithms. The primary protection goal is **integrity and technical robustness**.

5 Security threat and risk analysis for DPI in SSC

5.1 Threat landscape for DPI in SSC

The threat landscape for DPI in SSC is analysed based on the specific vulnerabilities of the three asset categories defined in Section 4.3. This section:

- Section 5.1.1 focuses on common cybersecurity threats mainly targeting infrastructure and platform assets, such as DDoS and ransomware.
- Section 5.1.2 focuses on data-oriented threats targeting data and information assets, including unauthorized access and privacy breaches.
- Section 5.1.3 focuses on technology-driven threats targeting software, logic and crypto assets, such as AI model poisoning and quantum-enabled decryption.

5.1.1 Common cybersecurity threats

Cybersecurity threats pose a persistent challenge to the stability and trustworthiness of DPI deployed in SSCs. While many of these threats such as ransomware, phishing, supply chain attacks and insider risks – are common across digital ecosystems, their impacts on city DPI are particularly critical as these urban-scale systems underpin the delivery of essential services to millions of

citizens. The interconnected nature of city DPI, spanning multiple administrative domains, physical infrastructure, and citizen-facing services, increases exposure and amplifies the consequences of even routine cyberincidents.

To provide a clear mapping to the asset categories defined in Section 4.3, this section analyses these common threats with a focus on the operational resilience of the DPI infrastructure. While these threats primarily exploit vulnerabilities in infrastructure and platform assets to disrupt urban service availability (e.g., DDoS, legacy system vulnerabilities), they also pose systemic risks to the integrity and confidentiality of the data and information assets residing within or managed by those systems (e.g., ransomware, insider threats).

The commonly seen cybersecurity threats within city DPI contexts and examples of the city DPI services that may be affected are summarized in Table 1.

Table 1: Common Cybersecurity Threats to city DPI

Threat	Description	Affected security attribute	Affected city DPI services
Ransomware attacks	Attackers encrypt critical DPI data and demand ransom, disrupting essential public services and operations.	Availability	– Public service portals – Digital identity systems – Payment platforms – Smart healthcare systems
Supply chain vulnerabilities	Insecure third-party vendors or providers can compromise core DPI components due to interdependencies.	Confidentiality Integrity Availability	– All city DPI services (systemic risk across the ecosystem)
DDoS attacks	Large-scale botnet attacks overwhelming DPI resources, causing service disruptions or complete outages.	Availability	– Public service portals – Identity authentication services – Payment gateways – Emergency response systems
Espionage and privileged access compromise	Attackers intercept communications or target privileged individuals to gain unauthorized access.	Confidentiality Integrity	– All city DPI services (compromised privileges enable access across the ecosystem)
Legacy system vulnerabilities	Outdated infrastructure components lacking modern security are more susceptible to exploitation.	Confidentiality Integrity Availability	– Legacy city service platforms – Legacy databases – Old IoT devices – Legacy industrial control systems

Threat	Description	Affected security attribute	Affected city DPI services
Insider threats	Negligent or malicious insiders can damage or expose DPI systems and data.	Confidentiality Integrity Availability	– All city DPI services (insiders with sufficient privileges can access any system within their authorized scope)
Complexity & interdependency	The interconnected, layered nature of DPI can obscure vulnerabilities and make systems harder to secure.	Availability	– Cross-agency integrated services – Multivendor service ecosystems – City data sharing platforms

5.1.2 Data security and privacy-oriented threats

Data security and privacy are foundational to DPI deployed in SSCs, focusing on the protection of data and information assets as defined in Section 4.3. These assets, which encompass vast amounts of sensitive identity records, financial transactions and urban development data, represent the "digital lifeblood" of the city. Threats such as unauthorized access, data breaches and discriminatory profiling not only compromise individual privacy but also undermine the public trust essential for sustainable urban development. While infrastructure and platform assets focus on operational uptime, the threats analysed in this section primarily target the confidentiality and privacy of the information residing within DPI systems. As city DPI serves as the backbone for identity, health care and financial services, preventing the exposure or manipulation of these data and information assets is critical to their reliability and resilience, as well as the public trust essential for sustainable urban development.

The main security threats specifically targeting data and information assets and the privacy within city DPI contexts, along with examples of the city DPI services that may be affected are summarized in Table 2.

Table 2: Threats to Data Security and Privacy

Threat	Description	Affected security attribute	Affected city DPI services
Unauthorized access & credential compromise	Exploiting weak authentication, misconfigured access controls, or stolen credentials to gain unauthorized access to DPI data.	Confidentiality	– Digital identity services – Administrative portals – Healthcare systems – Social service databases

Threat	Description	Affected security attribute	Affected city DPI services
Data breaches & exfiltration	Unpatched vulnerabilities, legacy system exploits, or advanced persistent threats leading to large-scale breaches, exposing sensitive information.	Confidentiality	– City data platforms – Health record systems – Social service databases – Financial transaction systems – Identity registries
Sophisticated phishing & social engineering	Using advanced phishing techniques and social engineering to deceive users into revealing credentials, installing malware, or granting unauthorized access.	Confidentiality	– Citizen-facing service portals – Administrative dashboards – Vendor access interfaces – Help desk systems
Excessive data aggregation & profiling	Over-collection of personal data from multiple sources leading to privacy breaches and unauthorized surveillance. Combining datasets across services can also lead to algorithmic discrimination and unequal impacts on marginalized urban communities. The risk is higher in cities that have not yet assessed their spatial digital divide, i.e., where connected, less connected and unconnected residents live, because gaps and biases in the combined data then go unnoticed.	Confidentiality	– Urban IoT systems – Mobility tracking platforms – Public Wi-Fi systems – Video surveillance systems
Data tampering & injection attacks	Injecting malicious code or altering data streams to manipulate DPI data and undermine the reliability and accuracy.	Integrity	– Financial transaction systems – Traffic management systems – Public records databases

Threat	Description	Affected security attribute	Affected city DPI services
Misuse of urban informality-related data	Unauthorized or inappropriate use of settlement, tenure, livelihood, mobility, or social-service data, creating exclusion, profiling, coercion, or surveillance risks. For example, residents of an informal settlement may stop using a health or social assistance service if they believe their address or tenure data will be passed to agencies responsible for evictions, and street vendors may avoid digital licensing or payment services if they fear the data will be used to fine them or confiscate their goods.	Confidentiality Integrity	– Public service portals – Social service databases – City data platforms – Mobility tracking platforms – Urban IoT systems

These data-centric risks may arise from traditional cyberattacks as well as from emerging technologies such as AI-driven analytics misuse or future quantum-enabled decryption capabilities, which are further elaborated in 5.1.3.

5.1.3 Technology-driven emerging threats

Emerging threats refer to novel or rapidly evolving cybersecurity risks driven by the development and integration of cutting-edge technologies such as AI, quantum computing and advanced automation. While these technologies enhance DPI efficiency, they introduce new attack vectors specifically targeting the software, logic and crypto assets defined in Section 4.3, including encryption keys, AI models, API specifications, and core algorithms. For DPI deployed in SSCs, these threats can undermine the foundational logic and cryptographic security of the entire ecosystem. As DPI increasingly adopts innovative tools to improve scale and efficiency, proactive risk assessment and adaptive defense mechanisms for these technical components become essential to prevent algorithmic manipulation, automated exploits, and the compromise of long-term data confidentiality through quantum-enabled decryption.

The following subsections analyse these emerging threats with a focus on protecting the integrity and robustness of the software, logic and crypto assets that underpin DPI intelligence and security functions.

5.1.3.1 Threats posed by AI to DPI for SSC

With the rapid development of Agentic AI systems, AI-driven attacks are becoming increasingly autonomous, coordinated and goal-oriented. Such systems can independently plan attack paths, coordinate multiple attack tools, and continuously adapt to defensive measures, posing unprecedented challenges to DPI in SSC. Additionally, the growing adoption of edge AI, hybrid AI architectures, and multimodal perception-reasoning-action pipelines within city DPI will introduce new attack surfaces. These threats are particularly relevant in smart cities, digital mobility, and public service scenarios, and must be incorporated into city DPI threat model.

5.1.3.1.1 External AI-enabled threats to DPI for SSC

AI technologies are now being exploited by malicious actors to enhance the sophistication, scale and effectiveness of cyberattacks targeting city DPI. These threats include AI-driven malware, deepfake-enabled social engineering, and automated data harvesting. AI significantly expands the cyberattack surface, enabling more convincing deception and accelerating attack cycles.

The main external AI-enabled security threats that endanger city DPI and examples of the city DPI services that may be affected are summarized in Table 3.

Table 3: External AI-Enabled Threats to DPI

Threat	Description	Affected security attribute	Affected city DPI services
AI-powered cyber attacks	AI-driven malware and automated attacks that can learn, adapt, and evade traditional security defences.	Confidentiality Integrity Availability	– Traffic management systems – Public service portals – City data platforms
Privacy invasion & data extraction	AI's ability to analyse vast datasets can be misused to extract sensitive information.	Confidentiality	– Urban IoT networks – City data platforms – Healthcare systems
Deepfake-based social engineering	Creation of realistic fake audio or video to impersonate trusted individuals and deceive targets.	Confidentiality	– Financial services – Digital identity systems

5.1.3.1.2 Threats to AI-integrated DPI systems

The deployment of AI within city DPI can inadvertently introduce security threats and vulnerabilities due to the complexity and opacity of AI models. In the urban context, these risks are magnified as AI systems increasingly underpin critical city functions, from predictive traffic management to AI-assisted emergency dispatch. These systems may be susceptible to data poisoning, adversarial attacks, and other forms of manipulation that compromise security.

The main threats to AI-integrated DPI systems in SSC and examples of the city DPI services that may be affected are summarized in Table 4.

Table 4: Threats to AI-Integrated DPI Systems

Threat	Description	Affected security attribute	Affected city DPI services
Data poisoning	Injection of malicious data into AI training sets, leading to corrupted model outputs.	Confidentiality Integrity	– Traffic management systems – Smart grid systems – City analytics platforms
Adversarial attacks	Input of specially crafted data designed to mislead AI models into making incorrect decisions.	Confidentiality Integrity	– Autonomous vehicle systems – Facial recognition systems – Smart surveillance systems – Traffic signal control systems
Model inversion	Extraction of sensitive information from AI models by analysing their outputs.	Confidentiality	– Healthcare AI systems – Digital identity systems – City data platforms
Model vulnerabilities in DPI systems	Inherent vulnerabilities in AI models used in DPI systems that can be exploited for malicious purposes.	Confidentiality Integrity Availability	– All AI-integrated city DPI services (systemic vulnerability across the ecosystem)
AI and unintended consequences in DPI decisions	AI-powered DPI decisions causing unintended impacts on data privacy, system fairness, or integrity.	Confidentiality Integrity	– Predictive policing systems – Smart city resource allocation – Traffic management systems
Unsafe content generation and propagation	AI systems generating, amplifying, or propagating false, manipulated or malicious content.	Integrity Availability	– Public information portals – Emergency alert systems

5.1.3.2 Threats Posed by quantum computing to DPI

Quantum computing holds immense promise for revolutionizing industries by solving complex problems at unprecedented speeds. However, this technology also poses unique challenges to the cybersecurity landscape for SSCs. As quantum computing advances, it could potentially undermine traditional cryptographic systems that are fundamental to the security of DPI. Cryptographically relevant quantum computers may be capable of breaking existing encryption protocols, putting sensitive data at risk and threatening the confidentiality, integrity and availability of critical city DPI systems. While practical quantum computing is still in its early stages, the potential for these risks necessitates forward-looking security strategies to ensure that city DPI can withstand the disruptive power of this emerging technology.

The main threats posed by quantum computing to DPI in SSC and examples of the city DPI services that may be affected are summarized in Table 5.

Table 5: Cyber Threats Posed by Quantum Computing

Threat	Description	Affected security attribute	Affected city DPI services
Compromise of asymmetric cryptography	Quantum computers can break RSA and ECC encryption, threatening data confidentiality and integrity.	Confidentiality Integrity	– Digital identity systems – Payment platforms – Data exchange platforms – Public key infrastructure (PKI) systems
Halving the security of symmetric cryptography	Quantum computing can reduce the complexity of exhaustive search by halving the security of a symmetric encryption algorithm.	Confidentiality Integrity	– Encrypted data storage systems – City databases – Backup systems
Undermining of digital signatures	Quantum computing could allow attackers to forge digital signatures, so bypassing authentication mechanisms.	Integrity	– Digital identity systems – Government authorization systems – Financial transaction systems
"Harvest now, decrypt later" attacks	Adversaries collect encrypted data today, planning to decrypt it once quantum computing advances.	Confidentiality	– Citizen identity records – Health information systems – Historical archives
Hybrid threat scenarios	AI-augmented quantum computing accelerates vulnerability discovery and cyber exploitation.	Confidentiality Integrity Availability	– All city DPI services (systemic risk acceleration)

5.2 Risk analysis for DPI in SSC

DPI for cities constitutes a foundational, interoperable digital layer enabling the delivery of public services, economic participation, and governance functions at urban scale. It typically encompasses digital identity systems, data exchange platforms, payment rails, registries, and AI-enabled orchestration components integrated across cloud, edge, and IoT environments. Within the context of smart sustainable cities, DPI acts as a critical infrastructure system, analogous to physical utilities, and therefore requires a security posture commensurate with its systemic importance.

Unlike traditional critical infrastructure sectors which are typically physically bounded and can be secured by a combination of multiple physical and digital controls (e.g., energy facilities, water distribution infrastructure, transport networks), DPI's attack surface is entirely digital and its harm radius, if compromised, extends to every citizen enrolled in its registers.

Building upon the threat identification in Section 5.1, this section evaluates the systemic risks posed to the three core DPI asset classes (data, system, and software, logic and crypto assets) defined

in Section 4.3. Unlike traditional IT systems, DPI risk is characterized by its systemic importance and population-scale exposure. Therefore, the risk analysis adopted in this document is "impact-anchored": severity is not primarily a function of technical complexity, but a measure of the systemic impact – specifically, how a compromise of data, system, or software, logic and crypto assets leads to widespread service exclusion, cascading infrastructure failure, or the erosion of societal trust.

DPI systems exhibit distinct risk characteristics that differentiate them from conventional IT systems:

- **High interdependency**: DPI components are tightly coupled with other city systems (transport, energy, health care), introducing systemic and cascading risk propagation primarily affecting the resilience of infrastructure and platform assets.
- **Population-scale exposure**: Failures or compromises affect large segments of the population and/or city residents, simultaneously, amplifying impact severity, often resulting from breaches in data and information assets.
- **Trust-centric operation**: DPI relies on sustained trust in identity, transactions, and data integrity. It equally relies on institutional trust: residents' confidence that decisions made through DPI are fair, transparent and accountable, and that they can challenge them. Trust erosion constitutes a primary risk vector. Software, logic and crypto assets (e.g., encryption and AI logic) provide the technical foundation of this trust; institutional trust depends on procedural fairness, transparency and accountability in how these assets are governed and used.
- **Cross-domain integration**: DPI spans administrative, economic, and social domains, increasing the attack surface and governance complexity, which expands the vulnerabilities of infrastructure and platform assets and requires robust software, logic and crypto assets for secure interoperability.
- **Long lifecycle and policy coupling**: DPI systems are embedded in regulatory and institutional frameworks, making remediation and evolution slower and more complex, often leading to the persistence of legacy vulnerabilities in infrastructure and platform assets and delays in updating software, logic and crypto assets (e.g., PQC migration).
- **Contextual and inclusion exposure**: DPI systems operate across uneven urban contexts, including informal settlements, underserved neighbourhoods, migrant communities, and users without stable addresses or documentation, which may create exclusion, data misuse, discriminatory profiling, or trust risks if security controls do not reflect local conditions, directly threatening the privacy of data and information assets and the equitable availability of infrastructure and platform assets.

Threat actors targeting DPI assets (data, system, and software, logic and crypto assets) and infrastructure, are typically motivated by financial gain, competitive intelligence, or even strategic impacts in case of state targeted attacks.

The threat taxonomy of DPI for smart cities departs from standard threat classification in one foundational respect: for DPI, threat severity is not primarily a function of technical complexity

or attacker capability, it is also a function of systemic impact across the population served or the specific asset class targeted DPI component affected.

A technically modest attack (e.g., a credential stuffing campaign exploiting a reused password) that compromises 50 000 citizen identity records in a voluntary commercial platform is a significant security incident. The same attack, targeting the infrastructure and platform asset (e.g., the national digital identity system) through which citizens access unemployment benefits, voter registration, and health care, is a national crisis. The taxonomy is therefore impact-anchored, in addition to its technical anchoring.

Table 6: Strategic and High Impact Attack Vectors and Strategic Effects by DPI Target

DPI Target (Asset category)	Attack vector	Strategic effect
Identity platform (Infrastructure and platform asset)	Mass credential revocation or fabrication.	Voter registration denial; electoral roll corruption; social benefit manipulation at city level or population scale.
Payment switch (Infrastructure and platform asset)	Transaction routing manipulation; bulk fraud injection.	Economic disruption; targeted financial exclusion; macroeconomic instability during crisis periods.
Data exchange platform (Data and information asset)	Integrity attack on eligibility data.	Mass false benefit determinations; confidentiality related attacks; profiling attacks.
Urban systems integration (Infrastructure and platform asset)	Sensor/actuator manipulation via DPI API abuse.	Physical infrastructure disruption: traffic control, utilities, emergency dispatch.
Cross-border interoperability layer (Software, logic and crypto asset)	Trust anchor compromise via third-country vendor.	Delegitimization of cross-border identity recognition; fraud.
Urban Inclusion Layer (Data and information asset)	Rigid identity, address, or eligibility checks; misuse of settlement or service data; insecure assisted access; accessibility barriers for persons with disabilities and older persons; limited digital literacy.	Service exclusion, discriminatory targeting, reduced uptake, and erosion of trust among vulnerable urban groups.

DPI security in SSC is also shaped by the local governance and socio-economic context in which DPI is deployed. Cities often operate through varied institutional mandates, multi-level governance arrangements, constrained municipal budgets, public-private service delivery models, and varying levels of administrative and cybersecurity capacity. These conditions can create security risks even

where the design of System and Software, Logic and Crypto Assets for the technical architecture is sound.

For example, weak procurement capacity may increase dependence on proprietary vendors or poorly governed third-party systems. Fiscal constraints may result in underinvestment in long-term maintenance, security monitoring, and incident response. Fragmented authority across municipal agencies, utilities, and private operators may produce unclear accountability for the protection of data and information assets, access control for infrastructure and platform assets, and breach response. In contexts of informality and unequal service access, DPI may also create exclusion risks if authentication for Infrastructure and Platform Assets or verification logic within software, logic and crypto assets do not reflect actual urban conditions.

Municipal capacities vary widely, and many cities have few dedicated cybersecurity staff and limited budgets and technical expertise. The guidance in this document should therefore be applied in proportion to local capacity. Cities with limited resources can start by identifying the few systems whose failure would most affect residents and protecting those first; adopting baseline controls before advanced ones; writing security requirements into procurement contracts; and drawing on shared capacity, such as national computer emergency response teams, inter-municipal cooperation, shared security operations services, and support from national governments and development partners.

Therefore, risk analysis for DPI in SSC should also consider institutional capacity, procurement incentives, data-sharing mandates, public-private accountability, service-delivery arrangements, and the potential impact of risks to data, system, and software, logic and crypto assets on vulnerable or underserved urban groups.

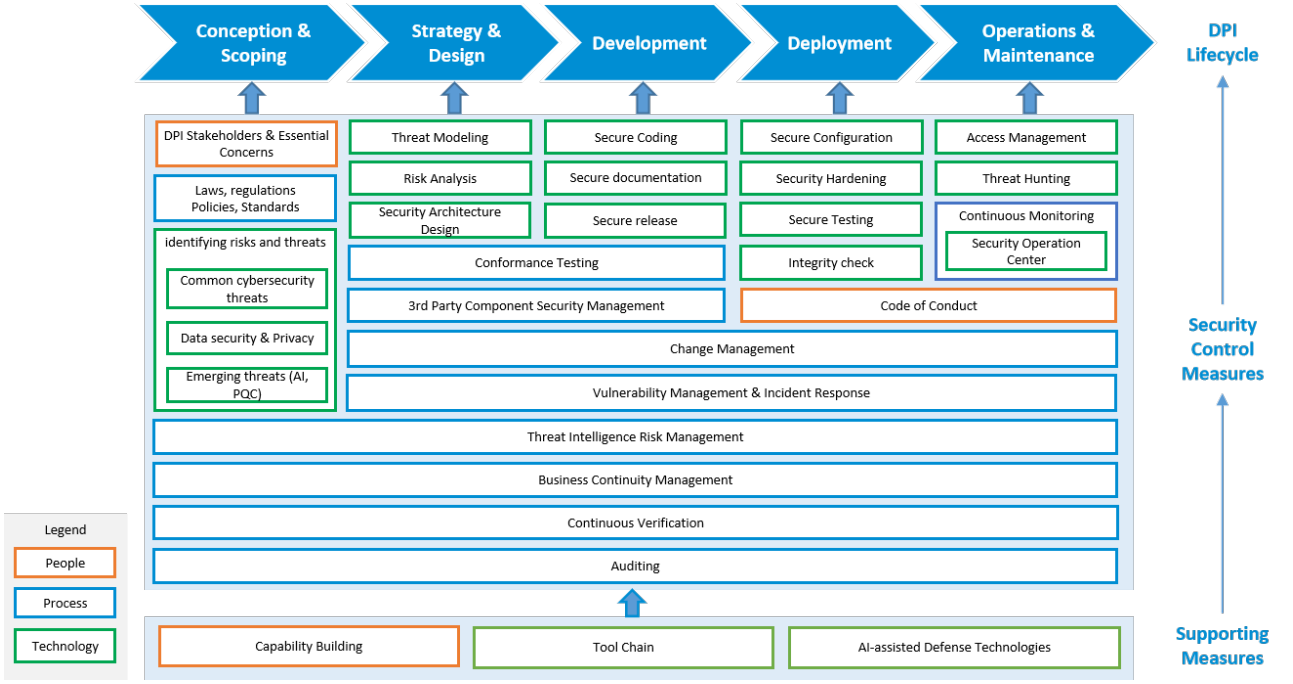
6 Security Framework for DPI in SSC

6.1 Lifecycle-embedded security framework for DPI in SSC

DPI deployed in SSC supports critical and large-scale systems such as digital identity services, payment platforms, urban IoT infrastructures, public service portals, and data exchange platforms. These systems are characterized by high interconnectivity across administrative and functional domains, real-time operational dependencies, large-scale aggregation and exchange of sensitive citizen data, and strong interdependencies between cyber and physical infrastructures. Given these characteristics, security considerations are required to be embedded across the entire DPI lifecycle.

Figure 2 illustrates the lifecycle-embedded security framework for DPI in SSC. Security mechanisms shall be integrated into each phase of a typical lifecycle of DPI – conception & scoping, strategy & design, development, deployment, and operations & maintenance to ensure resilience, integrity, availability, confidentiality, and traceability in SSC environments.

Figure 2: Lifecycle-embedded security framework for DPI in SSC (Source: Author)



- In the **conception and scoping phase**, the purpose, goals, constraints and boundaries of DPI must be established, guiding decisions and aligning with city strategic objectives and needs. Key security activities include setting security goals and objectives for city stakeholders; considering linkages to urban sustainability goals; analysing applicable legal, regulatory, and standards requirements for city DPI; identifying security risks and threats within the urban context while assessing potential impacts on city service continuity; and conducting participatory risk assessments with community organizations and service users, particularly groups likely to face barriers to access, so that risks to inclusion are identified alongside technical threats.
- In the **strategy and design phase**, a comprehensive plan is required to be developed to meet city DPI functional and performance objectives through actionable steps. Abiding by the principle of security-by-design, key security activities include conducting threat modelling and risk analysis tailored to urban service scenarios; conducting social impact, equity and inclusion assessments alongside threat modelling; performing security architecture design; setting out phase spanning activities such as conformance testing, third-party component management, change management, vulnerability management and incident handling process; and utilizing risk-based strategies to effectively mitigate design-related and architectural risks specific to city DPI.
- In the **development phase**, prototype systems conforming to city service specifications must be built, ensuring functionality, reliability and scalability. The main objective of the phase is to implement the secure design while preventing the introduction of additional engineering security risks. Therefore, key security activities include secure coding, secure verification including white-box, grey-box and black-box testing, documentation of the city DPI security specifications, and secure releasing.

- In the **deployment phase**, the implementation of DPI systems in the actual urban operational environment is required to ensure successful large-scale adoption while maintaining city service security and resilience. Key security activities include secure configuration, security hardening, security testing, and an integrity check of the release. The objective is to ensure the integrity of the delivered systems, and to make sure that the installed hardware, software and networking components are secure-by-default. A standardized code of conduct for system operators is essential because security responsibility is transferred during this phase.
- In the **operations and maintenance phase**, the ongoing performance, stability, and efficiency of city DPI must be ensured. Key security activities include access management, threat hunting, continuous monitoring, and incident response to ensure the security and resilience of the urban system. This phase typically triggers the continuous improvement of security capabilities to address emerging threats arising from ongoing urban digital transformation. Operations should also include a regular review of differential impacts across neighbourhoods and demographic groups, to identify exclusion or disparate outcomes caused by security controls such as authentication requirements, fraud rules or access restrictions. This review should be coordinated by a designated team within the local government.

In addition, the security activities for specific phase specified above, to address evolving security risks in smart sustainable cities, a set of security activities shall span the entire DPI lifecycle. Security activities such as threat intelligence risk management, incident response, vulnerability management, business continuity management, continuous verification and auditing should be included to stay aligned with the evolving security risks, protect the assets from the harm from cyberattack or physical disasters, and to inspect the effectiveness of the security control measures in each phase.

In particular, vulnerability management and incident response are essential as lifecycle-spanning security processes due to their critical role in maintaining continuous protection and resilience across all phases of city DPI lifecycle. Vulnerability management systematically identifies, assesses and remediates weaknesses from design through maintenance, reducing the attack surface proactively rather than reactively. Similarly, incident response ensures preparedness, rapid detection, containment, and recovery from security incidents throughout the lifecycle, thereby minimizing operational disruption and enabling the learning from incidents in order to strengthen urban defense capabilities.

To execute these functions effectively, it is recommended that cities establish dedicated security teams such as a city-level Computer Emergency Response Team, a Computer Security Incident Response Team or a Product Security Incident Response Team, which will provide centralized expertise, ensure consistent response coordination, and maintain oversight of ongoing security activities.

Furthermore, adopting collaborative approaches like coordinated vulnerability disclosure and collaborative incident response builds trust among city stakeholders, promotes transparency, and enhances collective ability to respond to evolving threats, strengthening the overall security posture of the DPI ecosystem in an interconnected urban operational environment.

Acting as supporting measures to the framework, capability building equips city administrators, operators, and citizens with essential cybersecurity competencies, while a digitized tool chain enhances operational consistency and traceability. Furthermore, the integration of state-of-the-art AI-assisted defense technologies significantly improves threat detection accuracy, accelerates response times, and reduces reliance on manual intervention, thereby strengthening overall resilience and minimizing human error across the DPI ecosystem.

6.2 Security control classification across the DPI lifecycle

To ensure completeness and traceability of security controls, the lifecycle-embedded framework shall classify security measures across three control dimensions:

- Organizational Controls: accountable stakeholders and responsibilities
- Procedural Controls: repeatable and auditable processes
- Technical Controls: enforceable technical mechanisms

Security controls defined in each lifecycle phase are required to be mapped to at least one of these dimensions to ensure balanced implementation. Table 7 illustrates the mapping of control dimensions to DPI lifecycle phases.

Table 7: Security control dimensions mapping into DPI lifecycle phases

DPI lifecycle phases	Organizational controls	Procedural controls	Technical controls
Conception & scoping	– Identify key stakeholders, e.g., city agencies, private sector, civil society. – Define security accountability across multiple city agencies and operators. – Assess local institutional capacity, fragmented authority, and public-private dependencies. – Plan stakeholder engagement processes, including how communities and civil society organizations will be involved throughout the lifecycle.	– Establish security objectives, risk appetite, and compliance frameworks. – Conduct risk assessments against urban threat landscape. – Conduct urban context assessment covering informal settlements, service gaps, and vulnerable groups. – Conduct a human rights impact assessment alongside the security risk assessment, drawing on UN-Habitat's people-centred smart cities approach.	– Define security architecture principles for city-scale systems, e.g., secure-by-design, privacy-by-design. – Plan for interoperability and resilience. – Identify access constraints affecting identity, connectivity, devices, and service channels.

DPI lifecycle phases	Organizational controls	Procedural controls	Technical controls
Strategy & design	– Conduct security awareness training for DPI architects and policymakers. – Build cross-sector collaboration for security best practices. – Define accountability mechanism for assisted access and intermediary-based service delivery. – Run participatory design processes with local communities, civil society organizations, and vulnerable groups to test usability, accessibility, and trust.	– Integrate secure development lifecycle principles. – Perform threat modelling and security validation. – Define data-use boundaries, grievance channels, and safeguards for vulnerable users.	– Design system architecture with encryption, IAM, and Zero-Trust models. – Implement access control and secure coding practices. – Design alternative identity-proofing, non-address-based access, and low-bandwidth service channels.
Development	– Train developers on secure coding and security testing. – Conduct regular security drills and simulations. – Include user groups from underserved areas in security and usability validation where appropriate.	– Establish change management and secure software development policies. – Require machine-readable Software Bill of Materials (SBOM) for all digital components. – Implement continuous risk assessments. – Test enrolment and access workflows under low-connectivity, shared-device, and multilingual conditions.	– Automate security testing, e.g., CI/CD security checks, vulnerability scanning. – Integrate automated vulnerability correlation against SBOM inventories. – Use container security and endpoint protection tools. – Validate assisted enrolment, community verification, and fallback access mechanisms.
Deployment	– Provide security awareness programmes for city operational staff across all agencies. – Conduct phishing and social engineering attack simulations. – Establish accountable arrangements for trusted local intermediaries and assisted access points.	– Implement compliance checks before go-live. – Conduct penetration testing and red teaming. – Provide community communication, grievance mechanisms, and anti-coercion safeguards.	– Enforce secure configuration baselines. – Deploy monitoring and logging solutions (SIEM, IDS/IPS). – Configure access controls and audit logs for assisted access and intermediary-operated interfaces.

DPI lifecycle phases	Organizational controls	Procedural controls	Technical controls
Operations & maintenance	– Maintain continuous cybersecurity training for city DPI operators. – Foster a security-first culture within organizations. – Maintain feedback channels with underserved communities and local service actors.	– Conduct periodic security audits and compliance reviews. – Implement an incident response and recovery framework. – Monitor exclusion errors, complaints, intermediary abuse, and differential service outcomes across neighbourhoods. – Publish periodic public reports on access, complaints, remediation actions, and service equity indicators.	– Deploy real-time threat intelligence and anomaly detection systems. – Use AI/ML for predictive cybersecurity threat management. – Audit abnormal access requests to sensitive settlement, welfare, mobility, and geospatial data.

7 Security guidelines for DPI in SSC

Addressing the cybersecurity challenges of DPI in SSC calls for several layers of protection that work together: technical controls, governance, risk management, and privacy measures. The guidelines below are intended for the governments, developers, operators and auditors who design, run and oversee city DPI. Their purpose goes beyond keeping systems confidential, intact and available. Secure DPI should also deliver public services that are equitable and accountable to the residents who depend on them, and this is where city-level DPI can add the most value.

To mitigate the systemic risks identified in Section 5.2 and to safeguard the core assets defined in Section 4.3, the following multilayered security guidelines are established:

- Sections 7.1 and 7.3 prioritize the resilience and uptime of Infrastructure and Platform Assets through a layered defence-in-depth architectural model and zero trust principles.
- Section 7.2 focuses on the confidentiality and privacy of data and information assets through encryption, secure storage, and privacy-enhancing technologies (PETs).
- Section 7.4 provides specialized governance for software, logic and crypto assets against emerging technology-driven threats, specifically those posed by AI and quantum computing.

In SSC contexts, security guidelines should be adapted to city-specific conditions, including urban density, uneven service coverage, informal settlements, shared devices, local institutional capacity, public-private service delivery, and dependency on cyber-physical infrastructure. Security measures should, therefore, protect DPI systems while ensuring that authentication, data access, monitoring,

incident response, and continuity arrangements remain usable, inclusive and accountable across diverse urban contexts.

7.1 Architectural & technical measures

DPI in SSC must be architected with security as a foundational principle, incorporating modern paradigms and layered defenses to protect against evolving threats. This involves a strategic combination of layered defenses, a fundamental shift in trust assumptions, secure interoperability, and inherent resilience to ensure the confidentiality, integrity and availability of critical services.

7.1.1 Defense-in-depth architectural model

To ensure the security and resilience of DPI, a layered defense-in-depth model offers a systematic and robust foundation to ensure that breaches in one layer do not compromise the entire system. The approach spans physical environment up through networks, identity controls, applications, data, operational monitoring and auditing. Each layer implements a unique set of security controls designed to address specific threat vectors, creating a synergistic barrier that significantly raises the cost and complexity for an attacker. The model enables DPI architects, integrators, auditors, and operators to address specific concerns such as intrusion detection, identity assurance, and regulatory compliance with precision.

Table 8: A Layered Defense-In-Depth Model for DPI Architecture

Layer	Security Concern	Controls / Technologies
Audit & compliance layer	Ensure traceability, non-repudiation, regulatory compliance with city, national, and sector-specific regulations; audit inclusion, accessibility, and fairness outcomes, particularly where DPI supports access to public services and benefits.	– Immutable logging systems – Automated compliance checking and reporting – Centralized audit trails – Periodic audits of inclusion, accessibility, and fairness outcomes
Operations, monitoring & orchestration layer	Detect, respond to, and autonomously contain incidents; monitor behaviour and automate security operations.	– Security information and event management (SIEM) with integrated threat intelligence – Security orchestration, automation, and response platforms – Cyber-physical threat intelligence – User and entity behaviour analytics – Endpoint detection and response – Network detection and response

Layer	Security Concern	Controls / Technologies
Data layer	Preserve confidentiality, integrity, privacy; ensure responsible data governance and stewardship, purpose limitation, and use of data for public value.	– Encryption (e.g., AES-256) for data at rest and in transit – Hardware security modules (HSMs) for key management – Data loss prevention with policies tailored to citizen data types – Privacy-enhancing technologies (PETs) like differential privacy and secure multiparty computation (MPC) – Compliance with data localization and cross-border data transfer regulations – Data stewardship arrangements, including purpose limitation and a documented public-value rationale for each data use
Application layer	Prevent exploits, injection, insecure code execution in city-facing applications, and ensure secure data exchange.	– Secure by design and privacy-by-design principles for urban applications – Web application firewalls – Static and dynamic application security testing – Machine-readable SBOM; runtime application self-protection – Secure coding practices
Access & identity layer	Enforce authentication, authorization, least privilege.	– Multi-factor authentication (MFA) with phishing-resistant methods (e.g., FIDO2) – Device identity and access management for IoT endpoints – Zero-trust network access – Role-Based and Attribute-Based Access Control (RBAC/ABAC) – Privileged access management (PAM) solutions
Network layer	Prevent eavesdropping, DDoS, lateral movement.	– Next-generation firewalls with deep packet inspection – Network segmentation and microsegmentation for OT and IoT – Secure protocols for IoT/M2M communications – DDoS mitigation services – Wireless network security (e.g., for public Wi-Fi and city-wide LoRaWAN)

Layer	Security Concern	Controls / Technologies
Physical layer	Prevent unauthorized physical access, tampering, sabotage, and environmental threats to distributed urban assets.	– Video surveillance with AI-powered analytics and anomaly detection in public spaces – Physical security monitoring for distributed assets – Hardware root of trust – Tamper-evident seals on critical infrastructure – Supply chain security and anti-counterfeiting measures for urban equipment

7.1.2 Zero-trust architecture (ZTA)

Zero-Trust Architecture (ZTA) operates on the core principle of "never trust, always verify," explicitly assuming that threats exist both inside and outside the traditional network perimeter. In the context of DPI for SSC, ZTA must extend beyond conventional IT environments to address the unique characteristics of urban-scale systems: massively distributed IoT endpoints, cross-sector data sharing, integration of physical and digital access controls, and the need to protect citizen privacy while enabling data-driven city services. Implementing ZTA involves a comprehensive approach beyond simple network changes:

- **Strong, phishing-resistant authentication**: Verifying every user, device and service identity attempting to access resources. This mandates the use of MFA, prioritizing phishing-resistant methods like FIDO2 security keys over weaker SMS-based codes. For urban DPI deployments, device authentication must scale to support millions of distributed sensors and edge nodes, requiring lightweight, hardware-anchored identities and automated certificate lifecycle management.
- **Explicit least privilege access**: Dynamically restricting access rights to only the data and applications necessary for a specific session or task, minimizing the attack surface. This is often enforced through "just-in-time" (JIT) and "just-enough-access" (JEA) policies. In the city DPI context, least privilege should be enforced at the data attribute level to support fine-grained data sharing across municipal departments.
- **Microsegmentation & software-defined perimeters**: Dividing the network into fine-grained, isolated segments based on workload identity to prevent lateral movement by malicious actors. This extends beyond the network layer to application and data layers. Segmentation policies should also reflect data classification levels to ensure that sensitive citizen data remains isolated from less critical city operations.
- **Continuous validation and authorization**: Re-evaluating trust based on changing context (user location, device health, behaviour analytics) for all access requests and connections, not just at initial login. For urban DPI, continuous validation must incorporate device telemetry from distributed edge nodes alongside user behaviour.

- **Comprehensive visibility and analytics**: Implementing robust logging and monitoring across all assets to feed the continuous validation engine and provide visibility into all access attempts. In city-wide DPI, this visibility must span both cyber and physical domains, correlating access logs from digital systems with physical access events and operational telemetry from city infrastructure.

Adopting ZTA enhances security by eliminating implicit trust and enforcing strict access controls based on identity and context, thereby drastically reducing the risk of unauthorized access and lateral movement.

7.1.3 Secure integration protocols

Ensuring secure and trusted communication between DPI systems and external platforms is essential for maintaining a coordinated security architecture. These protocols safeguard interoperability across distributed components such as cloud controllers, network policy engines, and threat intelligence platforms. Critical measures include:

- **Inter-system authentication and secure channels**: Implementing certificate-based mutual authentication (mTLS) and secure tunnelling protocols (e.g., IPsec, TLS 1.3) to ensure trusted connections between DPI systems and external management or orchestration services. All certificates must be managed through a robust Public Key Infrastructure (PKI).
- **API security controls**: Deploying authenticated and encrypted API communication using standards such as OAuth 2.0 with mTLS and OpenID Connect, especially for dynamic policy updates and telemetry sharing. API gateways should be employed to enforce rate limiting, schema validation, and threat detection at the API layer.
- **Orchestration and automation security**: Adopting secure automation protocols such as Network Configuration Protocol/ Yet Another Next Generation (NETCONF/YANG) with Secure Shell (SSH) or Transport Layer Security (TLS) for secure network configuration management and DPI policy distribution. All automation scripts and credentials must be securely stored and managed, ideally within a PAM solution.
- **Unified access control across domains**: Enforcing consistent access policies through federated identity systems (e.g., using SAML 2.0 or OpenID Connect) to prevent privilege escalation and lateral movement via integrated interfaces. A central identity provider (IdP) should serve as the single source of truth for authentication.

These protocols ensure that DPI systems interoperate securely within broader network and cloud environments, creating a seamless yet secure fabric that prevents threat actors from exploiting integration interfaces to bypass inspection, exfiltrate data, or disrupt traffic analysis. To ensure the long-term resilience of these protocols against evolving computational capabilities, including the potential threats posed by quantum computing, DPI architects should prioritize cryptographic agility and plan for a structured migration to Post-Quantum Cryptography (PQC) standards (see Section 7.4.2).

7.1.4 Resilient infrastructure models

Building reliable and fault-tolerant DPI systems requires foundational infrastructure practices that maintain operation during failures, attacks, or peak load. Resilience is measured by the ability to maintain availability and performance under stress. In the context of SSC, resilience must address not only digital system failures but also the physical realities of urban environments and physical damage to distributed edge assets. Essential methods include:

- **Redundant, geographically distributed deployment**: Using multiple, active-active instances of DPI systems across different availability zones or regions to ensure continuous traffic inspection if one node fails and to survive regional disasters.
- **Elastic load balancing and scalability**: Distributing network traffic evenly across DPI nodes and automatically scaling resources up or down to prevent overloading and maintain performance during high-volume periods, such as during a DDoS attack.
- **Regular backups and rapid, verified restoration**: Frequently backing up DPI configurations, policy sets, and critical state data. Backups must follow the 3-2-1 backup rule and be tested regularly via restoration drills to ensure they are uncorrupted and service can be quickly restored after an outage.
- **Failure testing and automated updates**: Periodically testing system response to failures through chaos engineering practices and applying security patches via automated, orchestrated rollout procedures with rollback capabilities to strengthen resilience against known vulnerabilities.
- **Stateless design where possible**: Designing DPI components to be stateless, pushing stateful sessions to an external, resilient data store. This simplifies failover and allows any node to handle any request, improving horizontal scalability.

These practices help DPI systems continue operating effectively under stress or partial failure, ensuring uninterrupted network monitoring and protection even in adverse conditions, which is critical for maintaining trust in public infrastructure.

7.2 Security operation & continuous monitoring

Proactive security operations and planning are essential to anticipate, withstand and recover from disruptions, as well as to detect, respond to and recover from the cybersecurity threats described in Section 5.1.1. This requires a shift from a reactive posture to a continuous, intelligence-driven security cycle, integrating people, processes, and technology.

7.2.1 Continuous monitoring & threat detection

Proactive monitoring is vital for early threat detection:

- **Security information and event management (SIEM)**: Aggregating and analysing logs from various sources (network traffic, endpoints, servers, applications) to identify anomalies. Modern SIEM platforms integrate with threat intelligence feeds to correlate internal events with known global attack indicators (IOCs), providing critical context for alerts and reducing false positives.
- **AI-driven security solutions**: Leveraging artificial intelligence and machine learning (ML) to detect subtle, evolving patterns indicative of advanced persistent threats (APTs) and zero-day attacks that traditional signature-based tools might miss. These systems continuously learn from new data, improving their detection capabilities over time.
- **Extended detection and response (XDR)**: Implementing XDR solutions provides a more unified view across multiple security layers (e-mail, endpoint, cloud, network). By automatically correlating data from these integrated sources, XDR enables faster threat hunting and more comprehensive investigation and response capabilities.
- **Threat intelligence integration**: Consuming and leveraging curated threat intelligence is crucial for contextualizing internal alerts. Understanding the tactics, techniques, and procedures (TTPs) of relevant threat actors allows security teams to proactively hunt for signs of these specific behaviours within their DPI environment.

Continuous monitoring enables organizations to detect and respond to security incidents in a timely manner, so drastically reducing mean time to detect (MTTD) and mean time to respond (MTTR).

7.2.2 Incident response & crisis management

Effective incident response and crisis management are vital for minimizing the impact of cyberincidents:

- **Develop comprehensive incident response plans**: Establish clear procedures for detecting, analysing, containing, eradicating, and recovering from security incidents. Plans should be aligned with established frameworks like NIST SP 800-61 and must include clear communication protocols for internal stakeholders, regulators, and law enforcement. Regularly update and test these plans through tabletop exercises and simulations to ensure effectiveness.
- **Crisis management & communication**: Developing strategies for managing large-scale cyberincidents with cross-organizational impact. This includes establishing a dedicated crisis command structure, preparing pre-approved communication templates for residents and the public, and managing public relations to protect the organization's reputation. Communication with affected communities should be accessible: multilingual, available through low-connectivity channels such as SMS, radio and community notice boards, and carried through trusted local networks such as community leaders and civil society organizations. In a crisis, visible and

coordinated leadership from the city, supported by streamlined digital processes, is central to keeping residents' trust.

- **Conduct regular training and simulations**: Equip staff with the necessary skills and knowledge through continuous training and simulated cyberattack exercises to ensure preparedness. These exercises should test technical responses and decision-making under pressure, ensuring the entire team, from technical staff to executive management, understands their role during a crisis.
- **Staff training and awareness**: Equipping personnel with necessary skills through continuous training programmes. Beyond the security team, all employees should receive regular awareness training to recognize and report potential security threats, such as phishing attempts, which are a common initial attack vector.

7.2.3 Disaster recovery & business continuity planning

Preparing for potential disasters ensures that DPI systems can quickly recover and maintain essential functions:

- **Develop disaster recovery plans**: Create detailed strategies to restore hardware, applications, and data promptly after a disaster. This includes defining Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical systems, regular data backups, and establishing alternative data centers or cloud-based failover sites.
- **Establish business continuity plans**: Outline procedures to continue critical business operations during and after a disaster, ensuring that essential functions remain operational. BCPs focus on the people and processes, ensuring that even if primary technical systems are unavailable, the organization can continue to serve its users and meet its obligations through predefined manual or alternative workflows.
- **Resilience testing**: Regularly testing recovery and continuity capabilities through simulated outage scenarios. This includes conducting full-scale disaster recovery drills to fail over to backup systems and verifying that data can be restored from backups without corruption. The lessons learned from these tests must be used to continuously refine and improve the plans.
- **Multi-site hosting and climate-related continuity**: Critical DPI components and backups should be hosted in more than one physical location, such as separate data centres or cloud regions, so that a disaster or outage at one site does not take down the whole service. Continuity plans should explicitly account for climate-related disruptions that affect urban areas, including floods, heatwaves, storms, and extended power outages. They should consider cases where a single event hits both a hosting site and the communities that depend on the service, and set out how essential services will be maintained through offline or alternative channels.

Implementing these guidelines will strengthen the resilience of DPI systems, ensuring their ability to withstand and recover from various challenges and threats.

7.2.4 City-specific access continuity and trust safeguards

Ensuring secure and continuous access to DPI-enabled city services requires safeguards that account for uneven urban conditions, diverse user capabilities, and intermediary-based service delivery. Essential measures include:

- **Inclusive access continuity**: Establish fallback channels, assisted access points, offline procedures, and low-bandwidth service options to ensure that essential DPI-enabled services remain available during cyberincidents, infrastructure outages, public emergencies, or partial system failures. These measures help prevent security incidents from becoming service exclusion events.
- **Accountable assisted access**: Define clear roles, permissions, authentication requirements, and audit obligations for local service agents, community organizations, help desks, and other intermediaries supporting DPI access. Assisted access workflows should apply least-privilege access, session logging, and periodic review to reduce fraud, coercion, or unauthorized data access.
- **Grievance and redress mechanisms**: Establish accessible procedures for users to report service denial, authentication failure, identity mismatch, suspected misuse of personal data, or coercive intermediary behaviour. These procedures should include escalation paths, response timelines, and mechanisms for correcting inaccurate records or restoring access to essential services.
- **Urban inclusion monitoring**: Monitor indicators that may reveal unintended exclusion or misuse, including repeated authentication failures, service-denial complaints, abnormal access to sensitive welfare, mobility, settlement, or geospatial data, and uneven service disruptions across neighbourhoods. Such monitoring helps detect operational risks that may not appear in conventional cybersecurity dashboards.
- **Community communication and trust management**: Provide timely, clear, and accessible communication to affected communities during incidents, outages, or major changes to DPI-enabled services. Communication channels should be adapted to local languages, literacy levels, connectivity constraints, and trusted community networks.

Implementing these safeguards strengthens the operational resilience of DPI in SSC by ensuring that security controls remain effective, accountable, and usable across diverse urban contexts.

7.3 Data governance, protection & privacy

To address the data and privacy-oriented threats identified in Section 5.1.2, cities need data governance as well as data protection. Data governance covers stewardship of and accountability for data throughout its lifecycle, ethical use, and the public interest that justifies collecting the data in the first place. Because this data is about people, protection and privacy measures should be people-centred: designed around the rights, expectations and circumstances of the residents

concerned. Within this framework, fulfilling regulatory obligations and maintaining public trust requires both foundational security and advanced privacy techniques.

7.3.1 Data protection mechanisms

Implementing comprehensive measures that provide baseline protection for data confidentiality and integrity, and help prevent unauthorized access and potential misuse of resources.

7.3.1.1 Data encryption & secure storage

Protecting data confidentiality and integrity is paramount. Effective measures include:

- **Data encryption**: Utilizing robust encryption protocols (e.g., AES-256 for data at rest, TLS 1.3 for data in transit) to prevent unauthorized access. A well-defined encryption strategy, including regular key rotation and cryptographically secure random number generation, is essential for maintaining long-term security.
- **Secure storage solutions**: Implementing storage systems with built-in security features, such as automatic encryption, immutable backups, and fine-grained access controls, to safeguard sensitive information. Solutions should be evaluated against industry standards (e.g., FIPS 140-3) to ensure they meet stringent security requirements.
- **Hardware security modules (HSMs)**: Deploying certified hardware security modules to provide a hardened, tamper-resistant environment for cryptographic key storage and operations. HSMs ensure that encryption keys are generated, stored, and used never leaving the protected hardware boundary, significantly raising the security bar against key extraction and misuse. They are fundamental for protecting root encryption keys and managing the entire cryptographic key lifecycle in a secure and compliant manner.

These practices ensure that even if data is intercepted or accessed without authorization, it remains unintelligible and secure. To maintain this assurance against future computational capabilities, cryptographic agility shall be embedded in encryption strategies, with a structured migration path to PQC algorithms for data requiring long-term confidentiality (see Section 7.4.2).

7.3.1.2 Data integrity & cryptographic verification

Maintaining the accuracy and trustworthiness of data is a critical security objective. This is achieved through:

- **Cryptographic hashing**: Employing secure hash algorithms (e.g., SHA-256, SHA-3) to generate unique digital fingerprints (cryptographic digests) for datasets. These digests are stored separately from the data itself. Any alteration to the data, however minor, will result in a completely different hash value upon re-calculation, immediately indicating tampering. This is critical for verifying the integrity of software updates, configuration files, and evidence logs.

- **Digital signatures**: Implementing asymmetric cryptography (e.g., using ECDSA or RSA-based digital certificates) to sign critical data. This not only verifies integrity but also provides non-repudiation, confirming the data's origin and authenticity. The private keys used for signing must be protected to the highest standard, ideally using an HSM (as outlined in Section 8.2.1.1), to prevent forgery in the verification process.
- **Cryptographic data lineage**: For federated data exchange platforms, incorporating tamper-evident provenance mechanisms (e.g., hash chaining, Merkle-tree-based attestations, or signed metadata) to ensure verifiable data lineage across distributed systems. Such mechanisms strengthen integrity guarantees and reduce the risk of undetected data tampering or malicious dataset manipulation.

These measures guarantee that data has not been modified in an unauthorized manner, ensuring its reliability throughout its lifecycle. To maintain this assurance against future computational capabilities, cryptographic agility shall be embedded in integrity protection strategies, with a structured migration path to PQC algorithms for data requiring long-term confidentiality (see Section 7.4.2).

7.3.1.3 Identity & access management (IAM)

Effective IAM is crucial for controlling user access within DPI systems:

- **Multi-factor authentication**: Requiring multiple independent forms of verification (e.g., a password combined with a time-based one-time token (TOTP) or a hardware security key) to authenticate users, thereby drastically reducing the risk of account compromise due to credential theft.
- **Role-based access control (RBAC)**: Assigning permissions strictly based on user roles and responsibilities to enforce the principle of least privilege (PoLP). Access policies should be clearly defined, regularly reviewed, and automatically enforced across all system components to minimize the attack surface.
- **Continuous monitoring & auditing**: Implementing a comprehensive logging and monitoring solution that records all access attempts, privilege changes, and data transactions. Regularly auditing and updating access rights is essential to adapt to organizational changes and emerging threats. This audit trail is vital for forensic analysis and demonstrating compliance.

Implementing robust IAM policies helps prevent unauthorized access and potential misuse of resources, creating a secure and accountable operational environment.

7.3.2 Privacy-preserving mechanisms

Safeguarding user privacy is paramount for DPI. Key privacy-preserving mechanisms include:

7.3.2.1 Data anonymization & pseudonymization techniques

- **Data anonymization**: This process involves removing or modifying personal identifiers to prevent the association of data with specific individuals. Common techniques include data generalization and data permutation. The goal is to irreversibly prevent re-identification, though this can sometimes reduce the data's usefulness for analysis. Advanced methods exist to better balance privacy protection with data utility.
- **Pseudonymization**: This technique replaces real identifiers with artificial ones, or pseudonyms, reducing the linkability of a dataset with the original identity of an individual. Unlike anonymization, pseudonymization does not remove all identifying information but makes it more challenging to identify individuals without additional information. It is a vital tool for secure data processing and analytics. The "key" that can re-identify individuals must be stored separately and guarded with strong security controls, such as encryption and strict access limits.

7.3.2.2 Secure multiparty computation & homomorphic encryption

- **Secure multiparty computation (MPC)**: MPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. This ensures that no individual party can see the other parties' data, maintaining data privacy during collaborative computations. This enables valuable collaborations – like multiple banks jointly detecting fraud patterns or research institutions conducting combined health studies – without any participant having to expose their raw, sensitive data to the others.
- **Homomorphic encryption**: This form of encryption permits computations to be performed directly on encrypted data without the need for decryption. The result, when decrypted, matches the outcome as if the operations had been performed on the original data, thereby preserving data confidentiality during processing. This powerful technology allows data to be processed securely in untrusted environments, like a public cloud, without ever decrypting it. While performance is improving, it is often used for specific, targeted operations.

7.3.2.3 Privacy-enhancing technologies (PETs)

Implementing privacy-preserving mechanisms in DPI helps ensure data protection and privacy by design, facilitating efficient integration and delivery of digital services while addressing ethical considerations associated with emerging technologies.

- **Differential privacy**: By introducing controlled random noise to data queries, differential privacy ensures that the presence or absence of a single individual's data does not significantly affect the outcome, thus protecting individual privacy. It is a robust standard for releasing public

aggregate data (e.g., traffic patterns, health statistics) while mathematically guaranteeing that no individual's information can be learned from the results.

- **Trusted execution environments (TEE)**: TEEs provide isolated environments within hardware where sensitive data can be processed securely, preventing unauthorized access or tampering during execution. TEEs are ideal for securing data while it is being used, enabling "confidential computing" where even the cloud provider cannot see the data.
- **Zero-knowledge proofs**: These cryptographic methods allow one party to prove to another that a statement is true without revealing any information beyond the validity of the statement itself. This is particularly useful in scenarios requiring verification without data exposure. This is revolutionary for enabling trust and verification without compromising privacy. For example, users can prove they are over 18 without revealing their exact birthdate, or prove a transaction is valid without revealing any details about it.

7.4 Countering emerging & future threats

To address the technology-driven emerging threats identified in Section 5.1.3, DPI systems should be designed to adapt to and mitigate evolving threat landscapes, including those posed by emerging technologies like AI and quantum computing.

7.4.1 AI-posed security threats & mitigations

As AI becomes deeply integrated into DPI, including digital ID systems, public service delivery, health platforms, and financial services, there is a growing need to mitigate the security and safety risks that AI may pose. Global efforts like the EU AI Act, U.S. Executive Order on Safe, Secure, and Trustworthy AI, NIST AI Risk Management Framework, and China's Generative and Synthetic Content Labeling Measures offer valuable models for governance.

Table 9: AI Security Governance Recommendations for DPI

Measure	Description
Risk-based categorization of AI systems	Classify AI systems used in DPI (e.g., biometric ID, predictive analytics, chatbots) into **risk tiers** (minimal, limited, high, and unacceptable), with stricter governance for high-risk applications.
Secure-by-design development	Enforce AI systems in DPI to be developed using **secure-by-design** and **privacy-by-design** principles. Mandate testing against adversarial attacks, model poisoning, and bias vulnerabilities.
Transparency and explainability standards	Require **model interpretability**, decision traceability, and audit logs for AI-enabled DPI services. Provide public disclosure for high-impact systems.

Measure	Description
Human oversight & accountability	Implement clear human-in-the-loop mechanisms and **accountability structures** for decision-making in critical DPI functions (e.g., public benefits adjudication or law enforcement applications). Assess automated decision-making systems for bias, equity, accessibility, and non-discrimination before deployment and at regular intervals, with particular attention to impacts on vulnerable groups.
Synthetic content & deepfake Governance	Apply **synthetic content identification** and watermarking in DPI media and communications to prevent misinformation and maintain public trust.
Cross-border regulatory alignment	Harmonize DPI AI governance with global best practices and support **international regulatory interoperability** through bilateral and multilateral frameworks.
AI auditing & certification	Mandate **regular independent audits**, red-teaming exercises, and certification of AI systems deployed in DPI environments. Create national registries for high-risk AI models.
Public engagement & redress mechanisms	Establish ongoing community engagement and participatory governance processes, rather than one-time consultations, together with grievance redress mechanisms for citizens affected by automated DPI decisions. Promote civic education on AI in public infrastructure.
Mitigation of agentic AI threats	Establish detection and response mechanisms for agentic AI-driven attacks, including behavioural analytics, anomaly detection, and dynamic policy adaptation.
Secure federated learning	Require robustness mechanisms (e.g., Byzantine-robust aggregation, gradient validation, secure parameter exchange) for distributed AI training.

7.4.2 Countermeasures for post-quantum cryptography threats

Proactive planning and early adoption of quantum-resistant measures are crucial to protect DPI from the evolving threats posed by quantum technologies. The "Harvest Now, Decrypt Later" attack model, where adversaries collect encrypted data today for decryption once a quantum computer is available, makes immediate action imperative. A structured migration plan is essential to future-proof critical digital public infrastructure.

- **Transition to post-quantum cryptography (PQC)**: Develop and implement a phased strategy for adopting cryptographic algorithms resistant to quantum attacks. This begins with conducting a crypto inventory to catalogue all systems using public-key cryptography (e.g., TLS, digital signatures, key exchange). Prioritize the migration of systems protecting highly sensitive data with long-term confidentiality requirements. Embrace cryptographic agility in system design – the ability to swiftly swap out cryptographic algorithms without overhauling entire systems – to facilitate smoother future transitions. Organizations should begin assessing their systems and

planning migrations to PQC standards as defined by leading bodies like the U.S. NIST, which is finalizing its PQC Standardization Project.

- **Data inventory and classification**: Identify and prioritize the protection of sensitive data that require long-term confidentiality, ensuring that critical information is safeguarded against future quantum threats. Data with a shelf-life extending beyond the anticipated advent of cryptographically relevant quantum computers are at greatest risk. This includes national identification data, health records, long-term legal documents, and classified government information. Encryption of this data must be upgraded to PQC standards at the earliest opportunity.
- **Infrastructure Assessment**: Evaluate existing DPI components (e.g., HSMs, root CA certificates, VPN concentrators, key management systems) to determine their vulnerabilities to quantum attacks and upgrade systems accordingly to support quantum-resistant protocols. Assessment must include evaluating dependencies on third-party vendors and service providers for their PQC migration roadmaps. Procuring new hardware and software should include contractual requirements for PQC readiness and support.
- **Collaboration and standardization**: Engage with international cybersecurity bodies (e.g., ENISA, NIST), governmental agencies, and industry partners to stay informed about emerging PQC standards and best practices. Participation in industry consortia and information-sharing forums is critical for aligning national DPI strategy with global developments. This collaborative approach helps avoid fragmented solutions and ensures interoperability across borders and systems.
- **Workforce training**: Invest in training programmes to equip cybersecurity professionals, developers, and system architects with the knowledge and skills necessary to implement and manage quantum-resistant technologies. Building internal expertise on PQC concepts, migration challenges, and new API integrations is vital for a successful long-term strategy. Furthermore, supporting academic and industry initiatives to develop and vet PQC solutions will strengthen the overall security ecosystem.

Implementing a quantum-resistant strategy is not a one-time project but a long-term, ongoing process that must be integrated into the organization's overall cybersecurity and risk management lifecycle.

Appendix I: Best Practices of Secure DPI Implementation

(This appendix lists some leading global cases of securing DPI implementations in smart cities.)

Governments and organizations worldwide have implemented best-in-class security frameworks to protect their DPI. Table I.1 shows a summary of some leading global cases showcasing secure, resilient, and scalable DPI implementations for smart cities:

Table I.1: Best Practices of Secure DPI Implementation Globally

DPI Initiative	DPI Architecture Model	Best practices	Relevance to city DPI
Estonia – X-Road	National secure **data exchange platform** enabling interoperability among government agencies, healthcare systems, financial institutions, and municipal services.	– Architecture: Decentralized, federated model; each organization controls its own data, exposing services via standardized interfaces. – Authentication: PKI-based mutual authentication. – Integrity: KSI blockchain for tamper-proof logging. – Management: National-level monitoring with distributed governance.	Demonstrates how cities can interconnect municipal systems without building centralized data lakes, reducing breach impact and improving resilience.
India – Aadhaar & UPI [b-UIDAI 2024]	Biometric-based national **identity system** integrated with real-time interoperable **digital payment** system supporting public service delivery and financial inclusion.	– Authentication: Biometric (fingerprint/iris), and OTP-based; central Identity Repository with real-time de-duplication. – Privacy: Virtual IDs replace Aadhaar numbers. – Regulatory frameworks: Strong legal backing (Aadhaar Act, Personal Data Protection Bill) for data privacy and security compliance. – Fraud detection: ML-based real-time risk scoring. – Infrastructure: Secure and real-time interoperable digital payment system with fraud detection mechanisms.	Illustrates secure identity-as-a-service integration and scalable real-time transaction security. Centralized biometric architectures may not be fully replicable at city level but integration patterns are applicable.

DPI Initiative	DPI Architecture Model	Best practices	Relevance to city DPI
Brazil – Pix **[b-BCB 2024]**	Real-time national **payment system** interoperable across banks, fintechs, and public services.	– Architecture: Mandates ISO 27001 certification for all participants; institution authentication via client certificates. – API Security: RESTful APIs with OAuth 2.0 + client certificate authentication; payload signing. – Fraud prevention: Uses behavioural biometrics and AI-driven fraud detection.	Provides a model for city-operated real-time payment or mobility platforms where centralized governance is combined with distributed security accountability.
Singapore – Singpass **[b-Singapore 2021]**	National **digital identity platform** integrated with municipal, health care, housing, and transport services.	– Authentication: Uses FIDO2-based biometric authentication for secure logins. – Data architecture: Attribute-based storage with data sharded across encrypted stores – no single repository contains all attributes. – Privacy: Users control what data is shared with government and third parties. – API security: OAuth 2.0 + OpenID Connect with mTLS; national Security Operations Center with 24/7 threat intelligence.	Highly relevant to SSC digital identity for urban services (transport, housing, health care). Demonstrates secure federation between city agencies and national identity infrastructure.
Japan – My Number System **[b-WorldBank]**	Centralized **digital ID** integrated across taxation, health care, and social services.	– Authentication: IC chip with PINs; PKI-issued certificates for digital signing and authentication – Data protection: Consent-based data sharing across agencies; oversight by Personal Information Protection Commission. – Network security: Dedicated government intranet for inter-agency exchange; external access via secure VPN with certified gateways. – Monitoring: National threat intelligence coordination.	Shows how cities can integrate with centralized identity systems while enforcing segmented access and strong cryptographic authentication. Direct replication of central registry model may not suit all SSC contexts.

DPI Initiative	DPI Architecture Model	Best practices	Relevance to city DPI
European Union – eIDAS [b-eIDAS]& GDPR Compliance [b-GDPR]	**Regulatory framework** for cross-border digital identity and trust services across all 27 EU member states.	– Interoperability: Secure mutual recognition of national digital identities. – Data protection: Uses PKI-based cryptography to ensure data security. – Compliance: Mandatory DPIAs and DPOs for all DPI services; biennial cybersecurity stress testing. – Privacy: GDPR – data minimization, purpose limitation, and citizen rights.	Demonstrates how SSC platforms can interoperate across administrative boundaries using standardized trust frameworks.
United States – Login.gov	Federated **single sign-on platform** for federal and state digital services.	– Authentication: A unified, secure login for accessing federal services using MFA, including biometrics and security keys. – Privacy: Adheres to NIST 800-63-3 guidelines, ensuring user data is not centralized and is only shared with explicit consent. – Data protection: Secures data transmission between users and government systems. – Interoperability: Built on open protocols (e.g., SAML, OpenID Connect) to ensure compatibility across federal agencies. – Audit: Leverages CISA's cybersecurity guidance and regular audits to maintain system integrity.	Applicable for SSC unified access portals where multiple municipal services are accessed through a common authentication layer without centralizing service data.

DPI Initiative	DPI Architecture Model	Best practices	Relevance to city DPI
China -eID & WeChat Pay/ Alipay	**Digital identity** integrated with large-scale **digital payment** and **public service platforms**.	– eID Stack: Secure chip on Resident Identity Card with cryptographic signatures; backend verification against National Identity Repository. – Authentication: Uses biometric authentication (facial recognition & fingerprint scanning) for transactions. – Privacy & data encryption: Implements homomorphic encryption and zero-knowledge proof (ZKP) to enhance user data privacy. – Compliance: Strict legal mandates under the China Cybersecurity Law and Personal Information Protection Law (PIPL) enforce DPI security. – Testing: Annual mandatory penetration testing; bug bounty programmes.	Illustrates how SSC platforms may integrate identity with mobility, utilities, and service payments. Highly centralized super-app models may not align with all governance models but provide lessons in scalability and real-time risk control.

To conclude, the world's best practices of secure DPI implementations focus on privacy, encryption, multifactor authentication, fraud prevention, and resilience. Countries that adopt a multilayered cybersecurity approach, AI-driven threat detection, and regulatory enforcement are better positioned to protect their DPI against cyberthreats, fraud, and privacy risks.

Bibliography

Banco Central do Brasil. (2024). Annual report 2024. https://www.bcb.gov.br/content/publications/Annual_Report_docs/AR-2024.pdf

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union. https://gdpr-info.eu/

International Telecommunication Union. (2021). Framework and requirements for civilian unmanned aerial vehicle flight control using artificial intelligence (Recommendation ITU-T F.749.13).

International Telecommunication Union. (2016). Overview of key performance indicators in smart sustainable cities (Recommendation ITU-T Y.4900/L.1600).

Organisation for Economic Co-operation and Development. (2024). Digital public infrastructure for digital governments.

Cyber Security Agency of Singapore. (2021). The Singapore cybersecurity strategy 2021. https://isomer-user-content.by.gov.sg/36/6318c1f5-3257-4c99-80e5-27339cf41883/The-Singapore-Cybersecurity-Strategy-2021.pdf

United for Smart Sustainable Cities. (2025). Building digital public infrastructure for cities and communities: A strategic framework for city leaders, officials, ministers, and policymakers. https://www.itu.int/net/epub/TSB/2025-Building-digital-public-infrastructure-for-cities-and-communities/index.html

Unique Identification Authority of India. (2024). UIDAI annual report 2023–2024. https://www.uidai.gov.in/en/2024-report-uidai-annual

World Bank Group. (n.d.). Riding the wave of digital transformation: Insights from Japan's journey. https://documents1.worldbank.org/curated/en/099352305232428567/pdf/P177977145b03308b19ef61f321c4e404f4.pdf



For more information,
please contact: u4ssc@itu.int
Website: https://u4ssc.itu.int/

ISBN 978-92-61-43641-4

Published in Switzerland
Geneva, 2026

Photo credits: @AdobeStock