

Smart City Cyber Security, Privacy

Rama Vedashree
CEO, DSCI

LEVERS OF SMART CITY CYBER SECURITY FRAMEWORK

- 
- **Multi- Dimensional, comprehensive and holistic cyber security plan**
 - **Cyber Response and Resilience**
 - **Cyber Threat Intelligence and Analysis**
 - **Digital Trust**
 - **Privacy by Design**
 - **Cyber competencies , Training, Awareness program**

Cyber security framework for smart cities

Governance layer

Design and governance
Cyber security framework, strategy, responsibilities and accountability

Security requirements implementation and operations

Implementation and operation layer

Design security and privacy policy	Design and implement secure network architecture	Implement and configure security solutions
Security assessment before Go-live	Set up and operate security operations centre	Compliance with regulatory requirements and guidelines

Application layer

Authentication	WAF	SIEM
Authorisation	Secure APIs	Antivirus

Data layer

Data classification	DLP	IDAM	HSM
Database activity monitoring	Encryption	Public key infrastructure	

Communication layer

Authentication	Authorisation	IPS/IDS	SIEM	Anomaly detection
Firewall	Network access control	DDOS protection	Anti-APT	

Sensor layer

Authentication	Remote administration	Device discovery
----------------	-----------------------	------------------

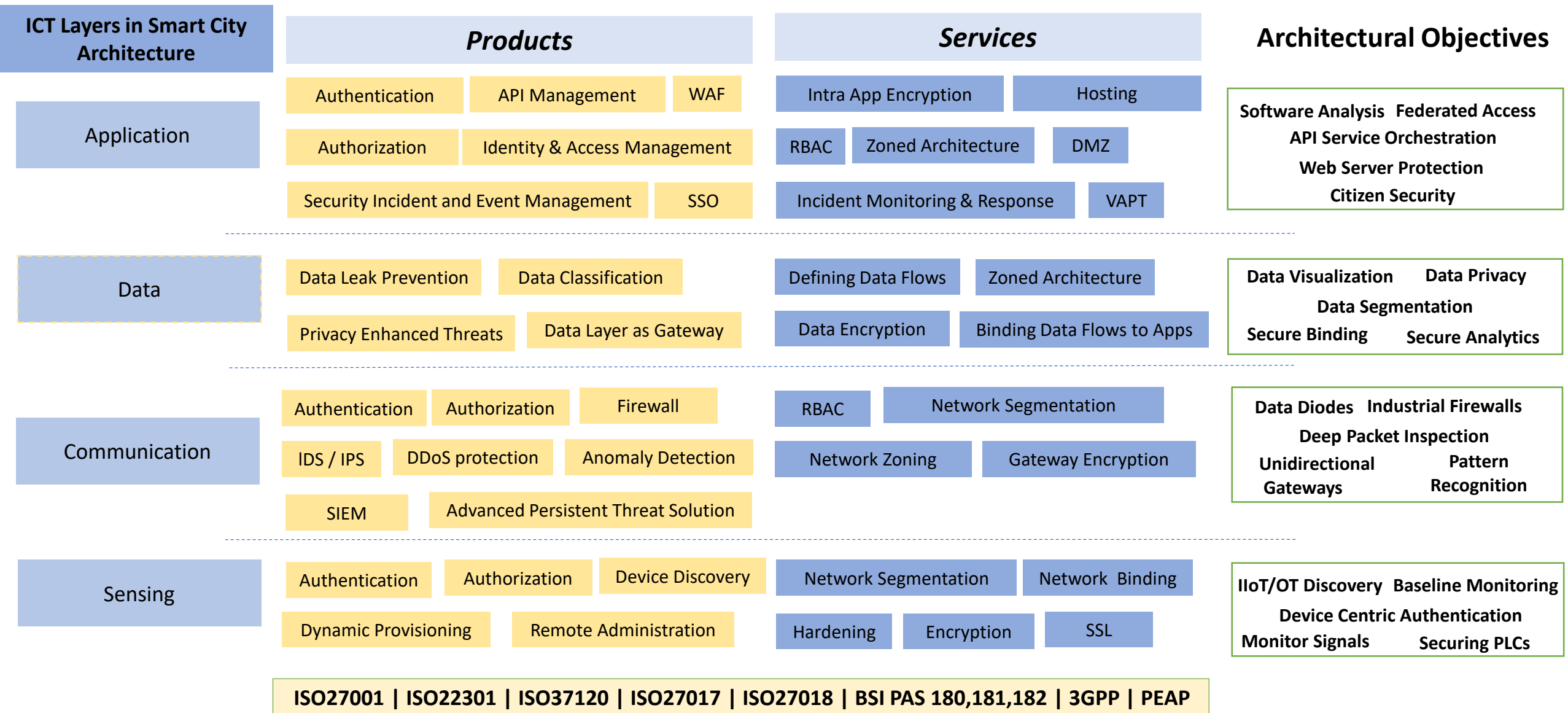
Assurance layer

Security assurance
Secure and uninterrupted operations with periodic audits, assessments, reviews and updates

Source: DSCI- PWC Report “ Creating Cyber Secure Smart Cities”

Cyber Security Requirements of a Smart City – Products and Services

Based on MoUHA Guidelines



Minimum Cyber Security Requirements of a Smart City – Products and Services

Based on MoUHA Guidelines

ICT Layers in Smart City Architecture

Products

Services

Architectural Objectives

Application

Authentication | API Management | WAF

Authorization | Identity & Access Management

Security Incident and Event Management | SSO

Intra App Encryption | Hosting in India

RBAC | Zoned Architecture | DMZ

Incident Monitoring & Response | VAPT

Software Analysis | Federated Access

API Service Orchestration

Web Server Protection

Citizen Security

Data

Data Leak Prevention | Data Classification

Privacy Enhanced Threats | Data Layer as Gateway

Defining Data Flows | Zoned Architecture

Data Encryption | Binding Data Flows to Apps

Data Visualization | Data Privacy

Data Segmentation

Secure Binding | Secure Analytics

Communication

Authentication | Authorization | Firewall

IDS / IPS | DDoS protection | Anomaly Detection

SIEM | Advanced Persistent Threat Solution

RBAC | Network Segmentation

Network Zoning | Gateway Encryption

Data Diodes | Industrial Firewalls

Deep Packet Inspection

Unidirectional Gateways | Pattern Recognition

Sensing

Authentication | Authorization | Device Discovery

Dynamic Provisioning | Remote Administration

Network Segmentation | Network Binding

Hardening | Encryption | SSL

IIoT/OT Discovery | Baseline Monitoring

Device Centric Authentication

Monitor Signals | Securing PLCs

ISO27001 | ISO22301 | ISO37120 | ISO27017 | ISO27018 | BSI PAS 180,181,182 | 3GPP | PEAP

Key features of the Smart City Cyber Security Policy

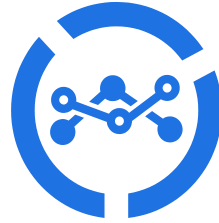
- 1.**Protect sensitive information stored with city, state government departments and agencies
- 2.**Protect the critical infrastructure
- 3.**Create risk assessment structure to manage risks in alignment with criticality of the information resource
- 4.**Continuously improve the cyber response capability
- 5.**Capacity building in cyber security of city administration, state government departments, agencies, commissions and Law Enforcement Agencies
- 6.**Facilitate cyber risk awareness to its operations and citizens on online safety and security

Highlights of the Smart City Cyber Security Policy



City Organization Structure

- The city shall appoint a **City Chief Information Security Officer**
- **Each city organisation** to have a cyber security management team that would be responsible for Identification of city's organisation security goals and integrate them into the appropriate processes



Security Implementation

- The Information Security Officer of each City Organisation to establish **standard operating procedures (SOPs)** as per industry standards and best practices.
- Every city organisation to establish a **cyber security response team** operating in conjunction with state IT Department Security Team and CERT-In



Governance

- **Annual audit** to measure the security posture in-line with the **city policies, procedures, cyber security framework and other regulatory requirements** and readiness assessment to be conducted
- Policy recommends that all **SMBs** operating in city to adopt fundamental Internet security practices,