



CityBioAuth

Syberkey
— Patented Tech —

SyberKey SmartCity Trust Fabric

Human-Verified Identity, Access and Action Control for Connected Cities

Executive Summary

Smart cities are rapidly becoming connected operating environments where citizens, workers, contractors, vehicles, sensors, payments, permits, utilities, surveillance systems and AI agents interact continuously. This connectivity improves efficiency and service delivery, but it also creates a major trust problem: cities must know that the right person, system or AI agent is authorised before any sensitive action takes place.

SyberKey addresses this problem by providing a human-authenticity and continuous-trust layer for smart-city environments. Its patented technology enables secure, biometric-linked digital identity, passwordless authentication, optional live biometric verification, continuous pathway enforcement, verified digital documents, verified communications, privileged-action control and AI-agent governance.

Rather than replacing existing smart-city systems, SyberKey is designed to sit above and across them. It can integrate with city portals, transport systems, parking platforms, CCTV systems, utility infrastructure, Microsoft environments, PAM platforms, procurement systems, emergency-response platforms, digital-permit systems and AI automation layers.

The result is a smart-city trust fabric that verifies not only login, but also high-risk actions: who accessed a system, who approved a transaction, who entered a secure facility, who exported sensitive data, who changed infrastructure settings, who signed a document, who issued a permit, and which AI agent acted under whose authority.

SyberKey's strategic value for smart cities is simple: connected cities require connected trust.

1. The Smart City Trust Problem

Smart cities rely on extensive digital and physical infrastructure, including:

- Digital citizen portals
- Public transport systems
- Smart parking and mobility platforms
- CCTV and public-safety networks
- Water, energy, waste and environmental systems
- IoT sensors and operational technology
- Emergency-response systems
- Contractor and workforce platforms
- Digital permits and licences
- Procurement and payment systems
- AI agents and automated decision systems

Each of these systems creates a different form of access, identity or authorisation risk. A city may know that an account has logged in, a card has been tapped, a QR code has been scanned, or a device has connected, but that does not always prove that the correct authorised human is performing the action.

This creates several weaknesses:

1. Passwords, OTPs and access cards can be shared, stolen or bypassed.
2. Contractor access is often fragmented across multiple systems.
3. Digital permits and entitlements can be misused or transferred.
4. CCTV and surveillance systems require stronger accountability.
5. Smart utility systems need privileged-action control, not just login control.
6. Citizens are exposed to phishing and fake government communications.
7. AI agents may act without sufficient identity, authority and auditability.
8. Existing identity systems often stop at authentication, while risk continues after login.

SyberKey solves this by providing a verified human and AI action layer across the smart-city ecosystem.

2. SyberKey SmartCity Trust Fabric

SyberKey SmartCity Trust Fabric is a modular platform that can be deployed across city services, infrastructure, agencies and private-sector partners. It provides verified identity, access control, continuous enforcement and trusted action records.

The platform is built around SyberKey / OneBioID's core technology capabilities:

- QR-based digital bio-ID
- Passwordless authentication
- OTP-free user verification
- Optional live biometric step-up
- Device-agnostic verification
- No specialised biometric scanner required after enrolment
- Continuous Pathway Enforcement
- Privileged-action verification
- Verified digital signatures
- Verified communications
- AI-agent identity
- AI Airlock governance
- Audit logs and Human Action Certificates
- Integration with existing identity, cybersecurity and smart-city platforms

The key difference is that SyberKey does not merely verify that a user logged in. It can verify the human or AI action at the moment of risk.

3. Core Smart City Platform Modules

3.1 Citizen BioID

Citizen BioID provides residents with a verified digital identity for accessing city services.

It can be used for:

- Council portals
- Parking permits
- Public transport concessions

- Library access
- Utility accounts
- Resident rebates
- City benefits
- Community services
- Digital complaints and requests
- Permit applications

Example: A resident applies for a disabled parking permit. The city verifies the person once and links the entitlement to a secure digital identity. The permit can then be checked digitally without repeated manual ID verification.

3.2 SmartCity Workforce Pass

SmartCity Workforce Pass verifies city employees, contractors, emergency workers, maintenance workers, vendors and field staff.

It can be used for:

- City building access
- Smart utility maintenance
- Transport infrastructure access
- Contractor site entry
- Work-order verification
- Depot access
- Emergency worker credentials
- Temporary access passes
- Third-party service providers

Example: A contractor attending a water-treatment site must verify identity, location, work order and access approval before entering or operating connected systems.

3.3 Continuous Pathway Enforcement for Smart Cities

Continuous Pathway Enforcement, or CPE, extends security beyond login. It verifies and enforces trust during the full user journey, especially before high-risk actions.

CPE can protect:

- CCTV access
- Utility control systems
- City cloud consoles
- Procurement approvals
- Payment release
- Data exports
- Permit approvals
- Emergency system overrides
- AI-triggered actions
- Admin privilege changes

Example: A city administrator can log into a platform, but before exporting citizen data or changing a surveillance-system setting, CPE requires a fresh verified approval and records the action.

This converts access control from a one-time login event into a continuous trust pathway.

3.4 BioPermit

BioPermit provides verified digital permits for city services and regulated activities.

It can be used for:

- Parking permits
- Construction permits
- Event permits
- Street-trading permits
- Resident access permits
- Loading zone permits
- Disabled access permits

- Waste disposal permits
- Market stall licences
- Short-term road closure approvals

Example: A food-truck operator receives a verified digital permit. A city inspector can confirm the permit, operator identity, location, time restriction and compliance status in seconds.

This helps reduce permit fraud, permit sharing, manual inspection cost and administrative burden.

3.5 VerifiedCCTV Access

VerifiedCCTV Access provides human-verified control over public-safety and surveillance systems.

It can govern:

- CCTV login
- Camera feed access
- Video export
- Facial-recognition system access, where legally permitted
- Public-safety data review
- Evidence handling
- Supervisor approval
- Audit logs

Example: A city officer wants to export CCTV footage. SyberKey requires verified identity, reason code, authority level and, where required, supervisor approval. The system records a Human Action Certificate showing who accessed what, when, and why.

This positions SyberKey as a privacy and accountability layer, not a surveillance vendor.

3.6 Smart Utility Access

Smart Utility Access protects water, energy, waste, environmental and operational technology systems.

It can be used for:

- Water-treatment controls
- Pump stations
- Flood-control systems
- Smart meters
- Energy substations
- Waste-management systems
- Environmental sensors
- Traffic control systems
- Building-management systems
- Remote maintenance access

Example: An operator attempts to change a water valve setting. SyberKey checks role, identity, work order, location, risk level and live biometric approval before allowing the action.

This is particularly valuable for cities where cyber risk intersects with physical infrastructure.

3.7 CityPay BioAuth

CityPay BioAuth adds biometric verification to high-risk city payments, refunds and financial transactions.

It can be used for:

- Permit payments
- Parking payments
- Utility payments
- Fine payments
- Refund approvals
- Supplier payments
- Bank account changes
- Vendor onboarding
- Grant disbursements

- Card-not-present payment approval

Example: A supplier changes bank account details in the procurement portal. SyberKey requires verified supplier identity and verified city officer approval before the change is accepted.

This directly addresses payment redirection fraud, vendor impersonation and internal approval risk.

3.8 Fingersign City

Fingersign City provides biometric-linked digital signing for city documents.

It can be used for:

- Permit approvals
- Citizen consent forms
- Contractor agreements
- Vendor declarations
- Building applications
- Community service forms
- Licence applications
- Internal approvals
- Procurement documents
- Public-sector declarations

Example: A citizen signs a permit declaration remotely. The signed document includes a verification record and QR-linked certificate confirming the signer, time and authenticity of the action.

This gives the city stronger evidentiary confidence than ordinary electronic signatures.

3.9 VerifiedBioMail for City Communications

VerifiedBioMail can help protect citizens and city agencies from phishing, impersonation and forged communications.

It can be used for:

- Verified city notices

- Fine notices
- Permit approvals
- Grant communications
- Procurement communications
- Emergency alerts
- Citizen account notifications
- Sensitive document delivery
- Payment instructions
- High-risk internal communications

Example: A citizen receives a payment or fine notice. VerifiedBioMail allows the citizen to confirm that the message genuinely came from the city, reducing the risk of fake council emails and payment scams.

This is highly relevant for public trust and cyber-resilience.

3.10 AgePass and Youth Protection

AgePass provides privacy-preserving age verification for youth safety and restricted services.

It can be used for:

- Social media age assurance
- Gaming access
- Library digital services
- Youth facilities
- Online community services
- Restricted-content access
- School-linked services
- Child-safety programs

Example: A digital service only receives confirmation that the user satisfies the required age threshold. The platform does not need to receive unnecessary personal identity data.

This can support government-backed digital safety initiatives.

3.11 SafePickup SmartCity

SafePickup SmartCity protects child handover, student transport and school-related identity workflows.

It can be used for:

- School pickup
- Bus boarding
- Excursion management
- Guardian verification
- Emergency contact verification
- After-school care release
- Student concession transport
- Child-safety incident records

Example: A school confirms that the person collecting a child is a verified parent, guardian or authorised nominee. The action is recorded securely.

3.12 AI Agent Identity and SmartCity AI Airlock

Smart cities will increasingly use AI agents for citizen support, transport routing, traffic management, infrastructure monitoring, cybersecurity, permit triage and emergency response. These AI systems need identity, control and accountability.

SyberKey AI Agent Identity and AI Airlock can provide:

- Synthetic identity for AI agents
- Binding of AI agents to authorised human controllers
- Policy-based execution boundaries
- Verified approval for high-risk AI actions
- Continuous pathway enforcement
- Audit logs for AI decisions and actions

- Sovereign control over city AI systems

Example: A traffic-management AI agent recommends emergency rerouting. Before pushing control changes to connected traffic infrastructure, AI Airlock verifies the agent identity, authorised human authority, policy scope and action approval.

This allows smart cities to use AI while retaining human authority and sovereign control.

4. Integration Model

SyberKey is not dependent on replacing existing smart-city systems. It can operate as an overlay, integration layer or embedded identity service.

Potential integration points include:

- Microsoft Entra ID
- Microsoft Defender
- Microsoft Purview
- CyberArk
- BeyondTrust
- Okta
- SailPoint
- SIEM and SOC platforms
- City citizen portals
- Smart parking systems
- Transport platforms
- CCTV platforms
- Utility control systems
- Procurement platforms
- Payment gateways
- Work-order systems
- Visitor-management systems
- Digital permit systems
- AI orchestration platforms

This makes the platform attractive for system integrators, smart-city technology providers, infrastructure operators and government agencies because it strengthens existing systems rather than forcing wholesale replacement.

5. Deployment Pathway

A city does not need to deploy the entire platform at once. SyberKey can be introduced through practical high-value entry points.

Phase 1: Workforce and Contractor Identity

Deploy SmartCity Workforce Pass for city employees, contractors, emergency workers and critical-site access.

Phase 2: Privileged Action Control

Deploy CPE for city IT, procurement, CCTV, utilities and sensitive data access.

Phase 3: Digital Permits and Citizen Services

Deploy Citizen BioID, BioPermit and CityPay BioAuth for selected public-facing services.

Phase 4: Verified Communications and Documents

Deploy VerifiedBioMail and Fingersign City for official notices, permits, agreements and citizen communications.

Phase 5: AI Governance

Deploy AI Agent Identity and SmartCity AI Airlock for city AI systems and automated workflows.

This phased model reduces adoption friction and allows the city to begin with clear operational and cybersecurity benefits.

6. Priority First Products

Product 1: SmartCity Workforce Pass

A verified identity and access product for city employees, contractors, emergency workers and infrastructure-service providers.

Primary buyers:

- City councils

- State agencies
- Infrastructure operators
- Transport authorities
- Utilities
- System integrators
- Smart-building operators

Why it is attractive:

- Immediate operational need
- Clear access-control problem
- Lower privacy friction than broad citizen identity
- Strong cybersecurity value
- Easy to integrate with existing contractor and access systems

Product 2: CPE for Municipal Privileged Access

A continuous enforcement layer for high-risk city actions.

Primary buyers:

- City CISOs
- Cybersecurity teams
- SOC operators
- Critical infrastructure teams
- Public-sector technology departments
- Managed security providers

Why it is attractive:

- Fits cybersecurity budget categories
- Integrates with Microsoft, PAM and SOC stacks
- Protects critical systems after login
- Supports audit, compliance and incident investigation
- Differentiates SyberKey from ordinary MFA providers

Product 3: BioPermit

A verified digital permit and entitlement product for parking, construction, events, markets and resident services.

Primary buyers:

- Councils
- Parking authorities
- Event regulators
- Local business regulators
- Transport agencies
- Smart-city platform providers

Why it is attractive:

- Easy for city leaders to understand
- Visible citizen-service benefit
- Reduces fraud and manual checking
- Can expand into broader citizen identity

7. Commercial Value Proposition

SyberKey can create value for smart cities in five major ways.

7.1 Stronger Cybersecurity

SyberKey reduces reliance on passwords, OTPs, shared credentials and weak access cards. It adds verified-human controls to sensitive systems and privileged actions.

7.2 Reduced Fraud

Digital permits, payment approvals, vendor changes, staff access, concession entitlements and document signing can be tied to verified human identity.

7.3 Better Public Trust

Verified communications, accountable CCTV access, biometric-linked signatures and privacy-preserving identity can increase citizen confidence in digital city services.

7.4 Operational Efficiency

Cities can reduce manual ID checks, paper permits, repeated document verification, contractor onboarding delays and fragmented access-management processes.

7.5 Future-Ready AI Governance

AI Agent Identity and AI Airlock give cities a pathway to deploy AI while preserving human authority, auditability and sovereign control.

8. Partner Opportunity

SyberKey is particularly suitable for partnerships with:

- Smart-city technology providers
- Systems integrators
- Cybersecurity companies
- Microsoft ecosystem partners
- Identity and access management providers
- Public-sector consulting firms
- Infrastructure operators
- Transport technology companies
- CCTV and public-safety platform vendors
- Smart utility providers
- AI governance platforms

For partners, SyberKey provides a differentiated trust capability that can be embedded into existing offerings.

Potential partner models include:

1. Technology integration
2. OEM embedding
3. Joint smart-city bids
4. Public-sector pilots
5. Managed service deployment
6. Sector-specific modules
7. Co-branded city trust solutions

9. Why SyberKey Is Different

Most smart-city vendors provide infrastructure, software or data platforms. SyberKey provides the trust layer that governs who can use them, who can change them, who can approve actions, who can access sensitive data, and which AI agents are allowed to act.

Traditional smart-city system:

- Device connects
- User logs in
- System performs action
- Audit log records account activity

SyberKey-enhanced smart-city system:

- Human or AI identity is verified
- Risk is assessed
- Role, policy, location and authority are checked
- High-risk action triggers live verification or approval
- Action is enforced or blocked
- Human Action Certificate is recorded
- System remains under continuous trust control

This is a significant move from access management to action governance.

10. Overall

SyberKey SmartCity Trust Fabric is a human-authenticity and continuous-trust platform for connected cities. It verifies citizens, workers, contractors, vendors, privileged users, digital permits, documents, communications, payments and AI agents across smart-city infrastructure.

It enables cities to modernise securely without replacing existing platforms. By integrating with identity systems, cybersecurity platforms, city portals, CCTV networks, utility systems, transport platforms, payment systems and AI environments, SyberKey provides the verified trust layer needed for the next generation of urban infrastructure.

Smart cities connect everything. SyberKey makes sure that every important action is performed by the right authorised human, system or AI agent.

11. Recommended Pilot

The recommended first pilot is a combined SmartCity Workforce Pass and CPE deployment.

Pilot scope

- 100 to 500 city staff and contractors
- One critical facility or controlled environment
- One high-risk digital system
- Verified contractor access
- Privileged-action verification
- Admin dashboard
- Audit logs
- Human Action Certificates
- Optional live biometric step-up
- Integration with existing identity or access platform

Pilot objectives

- Prove verified human access
- Reduce credential-sharing risk
- Protect privileged actions
- Demonstrate auditability
- Validate integration pathway
- Build the business case for wider smart-city deployment

Expansion pathway

After pilot success, the platform can expand into:

- Digital permits
- CCTV access governance
- Procurement approvals

- Utility operations
- Citizen services
- Verified communications
- AI-agent governance

Conclusion

Smart cities are not only infrastructure projects. They are trust projects.

As cities connect citizens, workers, contractors, vehicles, buildings, sensors, cameras, utilities, payments, documents and AI systems, they need a new layer of identity and action governance. Traditional authentication is no longer enough. The city must know who is acting, what they are authorised to do, whether the action is high risk, and whether the action should be allowed at that moment.

SyberKey provides this layer.

Through its patented biometric-linked identity, passwordless verification, continuous pathway enforcement, verified signatures, verified communications, privileged-action controls and AI-agent governance, SyberKey can become the trust fabric for connected cities.

For partners, this creates a strong opportunity to deliver differentiated smart-city security, identity and governance solutions. For governments, it provides a practical path to safer, more accountable and more trusted digital city infrastructure.