TGP Security Consulting Inc- Public Investor Overview

Strategic IP Licensing · OEM Partnerships · Funded POC Development

Context-Aware Authorization Through DSSC and UACCA Connecting Trusted Identity, AI-Derived Context and Enterprise Qualifications

4 Pending U.S. Patent Applications

From Trusted Identity to Real-Time Authorization

Prepared by: TGP Security Consulting Inc.
For: Public Investor Overview
Document Type: Prepared for Prospective Investors
Status: Non-Confidential Overview
Date: October 2026

Technology Background & Objectives of TGP's Four U.S. Patent-Pending Applications

To enable heterogeneous Identity, AI, Sensor and Enterprise Systems to interoperate through a common, machine-readable authorization-context framework.

The architecture is designed to verify sources, bind current context to authenticated identity, and normalize that information for customer policy evaluation, while preserving existing security infrastructure.

Trusted identity establishes WHO. Verified context helps customer policy determine WHETHER NOW.

Background and Technology Objectives

TGP's DSSC/UACCA architecture originated from challenges encountered by founder Michael TG Park during more than 35 years of experience in access control, video management and security system integration.

Physical access control has evolved to support magnetic-stripe and barcode cards, contactless credentials, fingerprint and facial recognition, mobile credentials and QR codes. Communication technologies such as OSDP have also improved security and interoperability between readers and controllers. However, a valid identity and an existing access permission do not necessarily establish a person's **current qualification or the safety conditions surrounding an intended activity**. An expired work qualification, missing required PPE or an unsafe condition in an access zone may require a different authorization outcome for the same person.

AI video analytics and sensor systems observe conditions in the physical environment. Enterprise systems maintain training, certification, employment and permit information. Incorporating these inputs into access policy requires reliable association with authenticated identity, verification of source authenticity, assessment of freshness and consistent interpretation of information. Differences among vendor data formats, APIs, SDKs and communication methods can make these integrations complex and difficult to reuse.

Supported by **four pending U.S. patent applications**, TGP is pursuing the implementation and validation of a vendor-neutral authorization-context architecture connecting identity credentials, AI and sensor observations, and enterprise qualifications. DSSC represents dynamic secondary credential conditions associated with authenticated identity. UACCA provides a proposed framework for representing and communicating that information in a common, machine-readable form across heterogeneous systems.

Technology Objectives and Expected Benefits

TGP's objective is to use source adapters and mapping profiles to verify and normalize heterogeneous inputs into **standardized authorization context**. Each source system can retain its own interface and communication method. Customer authorization policy evaluates the resulting context and makes the final access decision, which existing PACS and controllers enforce. The architecture aims to preserve existing security infrastructure, improve integration reuse, reduce dependence on individual vendors and support authorization that reflects current qualifications and safety conditions. Potential applications include construction sites, critical infrastructure, semiconductor fabrication facilities, food manufacturing plants and hospitals. Actual benefits, supported integrations and deployment requirements will be established through partner POCs and operational validation.

INVESTMENT OPPORTUNITY

From Trusted Identity to Dynamic Authorization.

TGP Security Consulting Inc.

Strategic IP licensing | OEM partnerships | Funded POC development

Identity establishes WHO.
Trusted context helps policy determine WHETHER NOW.

TGP is developing a vendor-neutral architecture that connects authenticated identity with AI-derived observations, sensor information and enterprise qualifications. DSSC and UACCA are designed to translate those heterogeneous inputs into standardized authorization context for existing security platforms.



The proposition	The next proof point
Four pending U.S. patent applications underpin the proposed architecture.	A focused reference implementation with measurable technical and operational results.

Partner-led commercialization through funded POCs and negotiated licensing.	A defined engineering partner, acceptance plan and commercial pathway.

Investment thesis

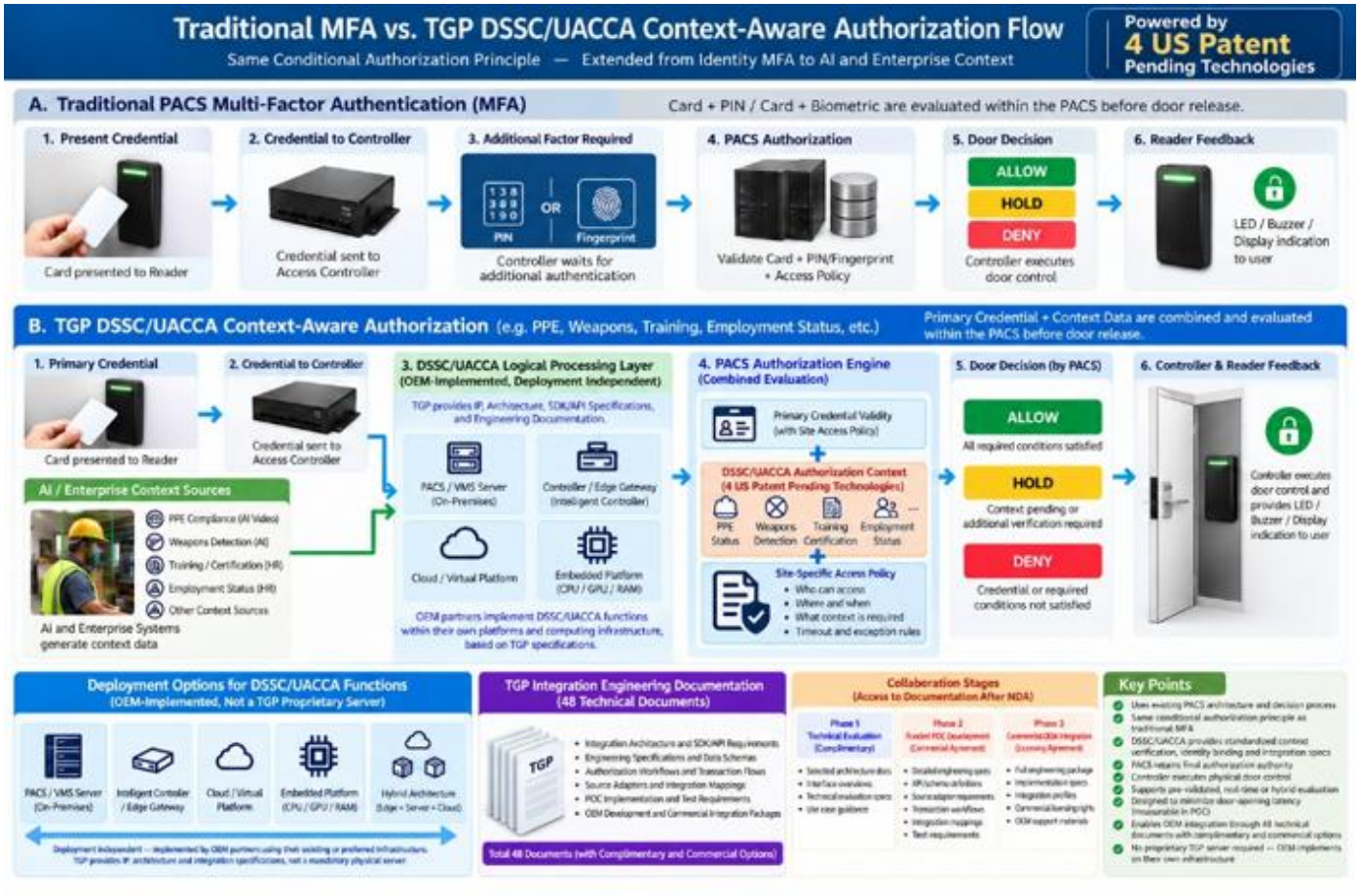
A reusable context interface could reduce repeated integration work as security platforms incorporate changing safety and workforce conditions into authorization. That opportunity must be demonstrated through practical integration and partner willingness to pay.

Current stage: Architecture and requirements development, technical evaluation and partner engagement. POC execution and commercial conversion remain milestones.

PROBLEM & OPPORTUNITY

The Gap between Observation and Authorization.

Security and enterprise systems hold useful information in different formats, with different meanings and update cycles. A valid credential confirms identity. It does not, by itself, establish that the person has current training, an active permit or the required protective equipment for a particular activity. Connecting these conditions to access policy requires reliable identity association, source interpretation and lifecycle handling.



Input domain	Information relevant to authorization
Identity and credentials	Authenticated person and credential reference.
AI, video and sensors	Observed PPE, behavior, environmental or operational conditions.
Enterprise systems	Training, certification, employment, contractor and permit status.
Customer policy / PACS	Rules for the person, zone, resource and time; final decision and enforcement.

Initial market entry

TGP proposes starting with an industrial or warehouse use case in which workforce qualifications and selected PPE observations can be evaluated against a clearly defined site policy.

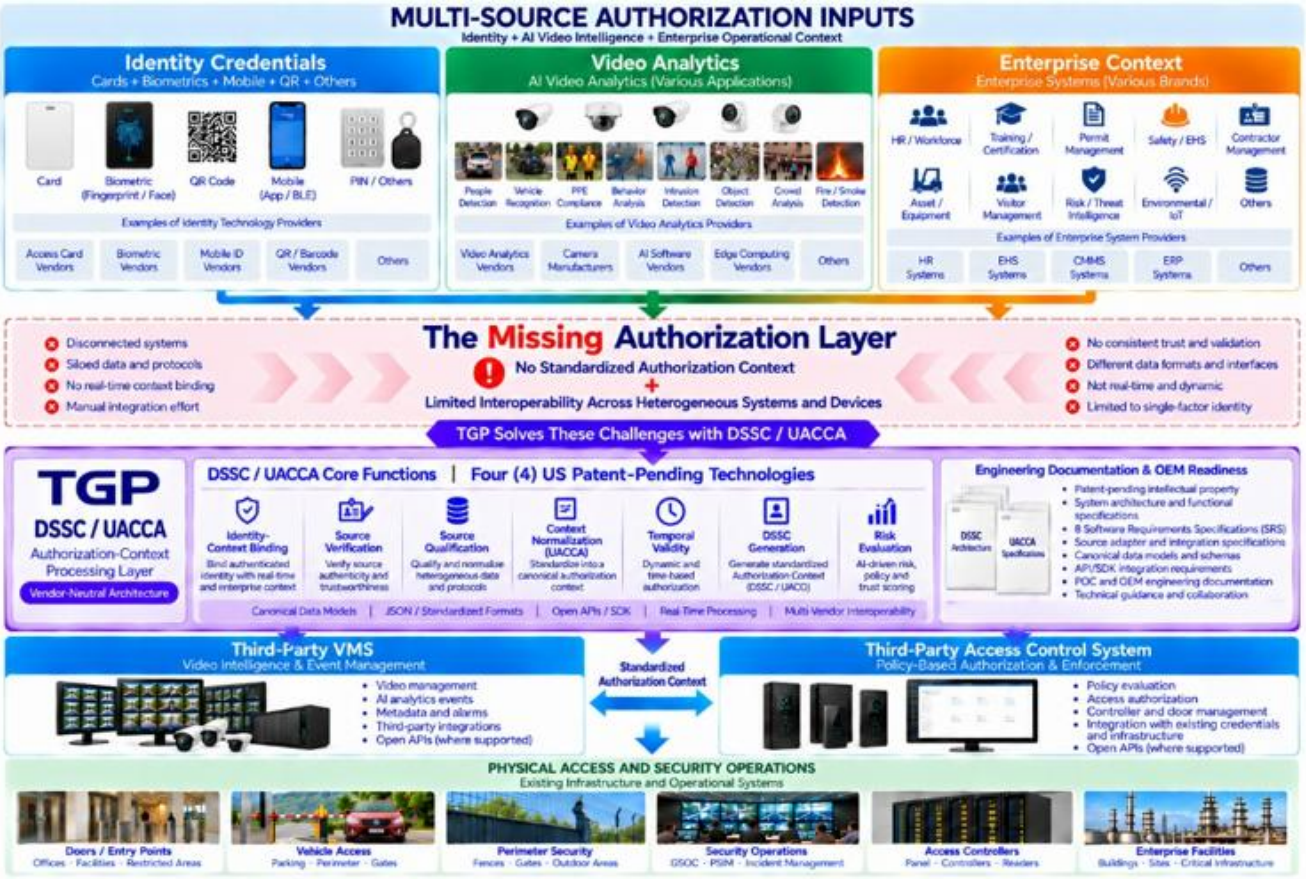
Expansion opportunity

After validation, the same integration approach could be evaluated for other sources, receiving platforms and facilities. Commercial potential depends on repeatable integrations and paid adoption; Initial commercialization will focus on industrial and warehouse environments, with expansion guided by validated integrations and customer demand.

SOLUTION & RESPONSIBILITIES

A common language for authorization context.

DSSC and UACCA connect heterogeneous sources to the customer's existing authorization environment.



Architecture stage	Proposed responsibility
1. Trusted inputs	Identity sources, AI / sensors and enterprise systems provide assertions.
2. TGP context processing	Verify and qualify sources; assess freshness; associate identity; normalize and reconcile relevant context.
3. DSSC / UACCA representation	Represent dynamic secondary context and communicate a machine-readable authorization context.
4. Customer authorization	The receiving platform evaluates context against customer policy and produces the final decision.
5. Existing infrastructure	PACS / controllers enforce the result; readers may indicate status.

DSSC - Dynamic Secondary Security Credential: Dynamic, identity-associated authorization context that can change while the primary credential remains valid.

UACCA - Universal AI Credential Communication Architecture: A proposed vendor-neutral framework for representing and communicating authorization context across heterogeneous systems.

The initial POC uses TGP as a context provider. It requires neither AI-context processing in an ordinary reader nor replacement of the primary credential. Source adapters and receiving-platform integration remain engineering work.

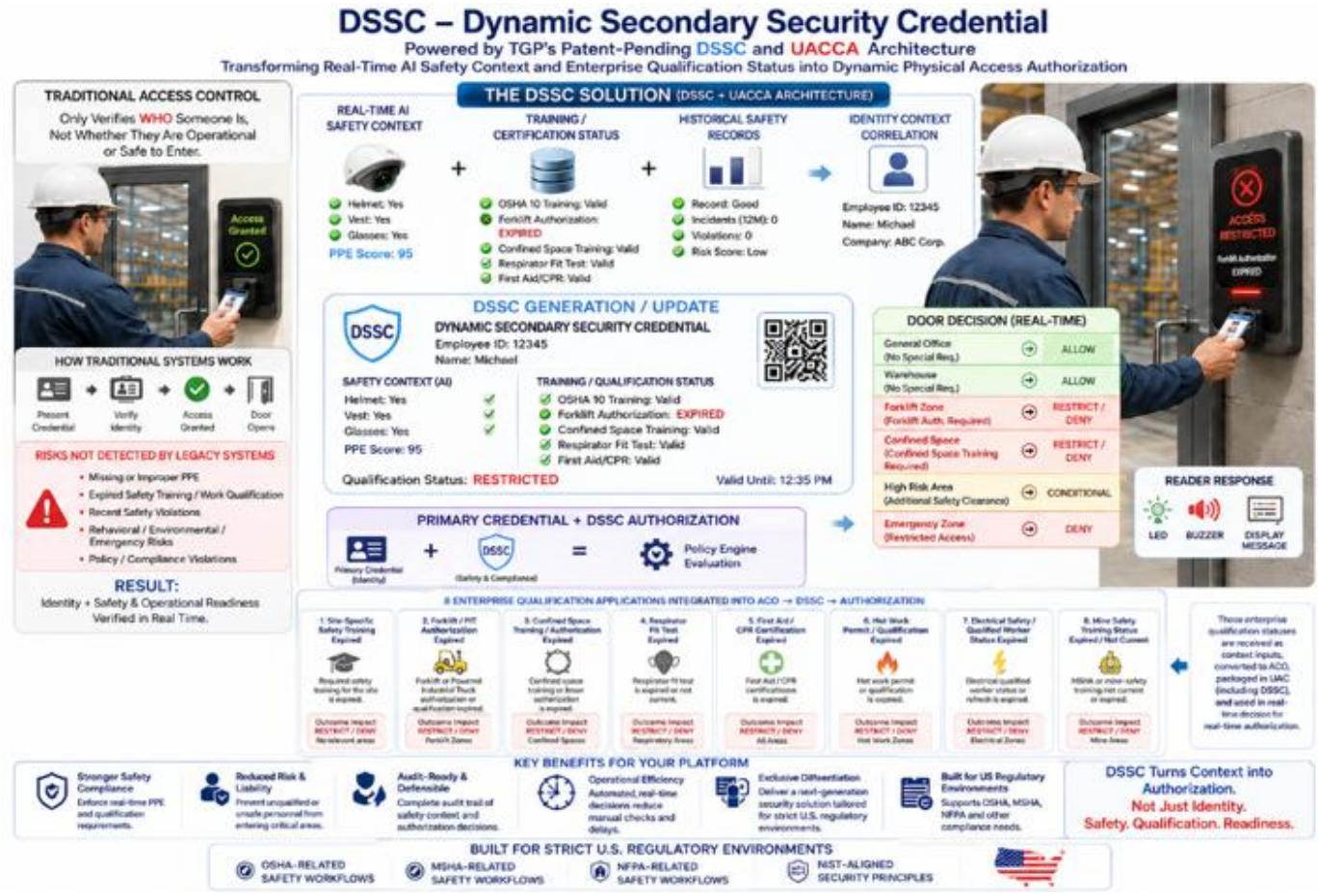
UACCA is a proposed architecture; references to interoperability do not establish an adopted industry standard or certification.

WHY DSSC & UACCA FOR SECURITY INDUSTRIES?

Same Identity. Different Permission now.

A warehouse worker presents a valid credential while a task-specific qualification has expired.

For the proposed demonstration, an enterprise source reports that forklift authorization has expired. Selected AI observations report that required PPE is present. TGP associates the relevant context with the authenticated worker and supplies it to the receiving platform.



Resource / activity	Illustrative policy outcome	Reason
General office	ALLOW	Normal identity and access rules satisfied.
General warehouse	ALLOW	Warehouse requirements satisfied.
Forklift operation	RESTRICT / DENY	Task-specific authorization expired.
After qualification renewal	Re-evaluate	New verified qualification state received.

The proposed architecture is designed to support selected safety and security compliance workflows related to applicable OSHA and MSHA regulations, NFPA codes and standards, and relevant NIST guidance through context-aware authorization and traceable records. Specific requirements and mappings will be defined and

validated for each deployment. These references do not imply certification, regulatory approval or guaranteed compliance.

These are example policy outcomes, not automatic product behavior or a claim of regulatory compliance. Actual decisions depend on the site's rules and validated integrations.

What the POC must establish

Correct identity-context association; rejection or explicit handling of stale and conflicting inputs; reliable update propagation; and a traceable explanation of the context used by customer policy.

What success would mean

A working, auditable reference flow showing that one changing qualification can affect the intended resource without globally revoking a valid identity credential. Numerical targets must be agreed before testing.

CONTEXT-AWARE ACCESS USE CASES ACROSS INDUSTRIES



TGP's proposed DSSC/UACCA architecture connects authenticated identity, observed safety and environmental conditions, and current enterprise qualifications. It transforms these heterogeneous inputs into standardized authorization context for customer policy evaluation.

The following scenarios illustrate potential applications. Outcomes depend on site policy, available integrations and operational validation.

1. Industrial Manufacturing

Manufacturing facilities distinguish between permission to enter a facility and qualification to perform a particular task. An employee may hold a valid credential and retain warehouse access while no longer meeting the requirements to operate a forklift or specific production equipment.

2. Food Manufacturing

Food manufacturing facilities apply different entry requirements to offices, storage areas and food-production zones. Valid identity and completed training may need to be evaluated alongside current hygiene-entry conditions.

3. Semiconductor and Cleanroom Facilities

Semiconductor and cleanroom facilities may require current training, specific work permissions and defined entry conditions. Access requirements can vary by cleanroom, process area and maintenance activity.

4. Construction Sites

Construction sites experience changing work areas, contractor assignments and temporary hazards. Completion of site induction does not necessarily authorize entry into every work zone at every time.

5. Critical Infrastructure

Critical infrastructure facilities may require specific authorization for restricted areas, maintenance tasks and defined work periods. A technician's valid identity does not establish that every work permit remains active.

6. Healthcare and Memory Care Use Cases

Hospitals and memory care facilities require authorization that considers patient care needs, visitor permissions and changing conditions within the facility. A confirmed identity alone does not establish whether a person should enter a restricted area or leave a monitored care zone unaccompanied.

TGP's proposed DSSC/UACCA architecture connects authenticated identity with video and sensor observations, together with relevant enterprise and care information. It supplies standardized authorization context for evaluation by hospital policy and authorized personnel.

A. Unaccompanied Exit Risk

A patient approaches a monitored exit without an accompanying caregiver. An approved identification source, such as a patient wristband or RTLS system, establishes identity. Video or sensor observations indicate the patient's location and movement, while an authorized care-system source indicates that escorted movement is required. Hospital policy may notify care staff and request escort confirmation, supporting earlier intervention based on the patient's current care requirements.

B. Wandering and Prolonged Presence

Video intelligence observes repeated movement or prolonged presence near a monitored or restricted area. Available identity information and enterprise context help distinguish among a patient needing assistance, a visitor waiting for care, and a person whose access requires review. The receiving system may request staff assistance or authorization review, helping distinguish a person needing support from a situation requiring security attention.

C. Potential Imminent Threat

Video analytics, acoustic sensors or staff reports identify a potential urgent security event, such as threatening behavior, a suspected weapon or a distress signal. DSSC/UACCA associates available observations with identity, location, timestamps and relevant incident context. Authorized personnel evaluate the evidence and initiate the appropriate security response under hospital procedures.

D. Restricted Clinical Area Access

A staff member or visitor requests access to a restricted clinical area. Identity credentials establish who is requesting entry. Video or sensor inputs provide relevant observations, while enterprise systems supply role, assignment, training and access-permission information. Hospital policy may allow access, hold the request or seek authorized approval according to current role and area-specific requirements.

Patient-related responses remain subject to clinical oversight, privacy requirements and approved hospital procedures. Exit management must preserve emergency egress. Video observations do not establish a diagnosis or intent.

Common Architectural Value

Across these industries, TGP aims to provide a reusable authorization-context framework for heterogeneous systems. Source adapters and mapping profiles preserve existing interfaces while translating relevant inputs into a consistent, machine-readable representation.

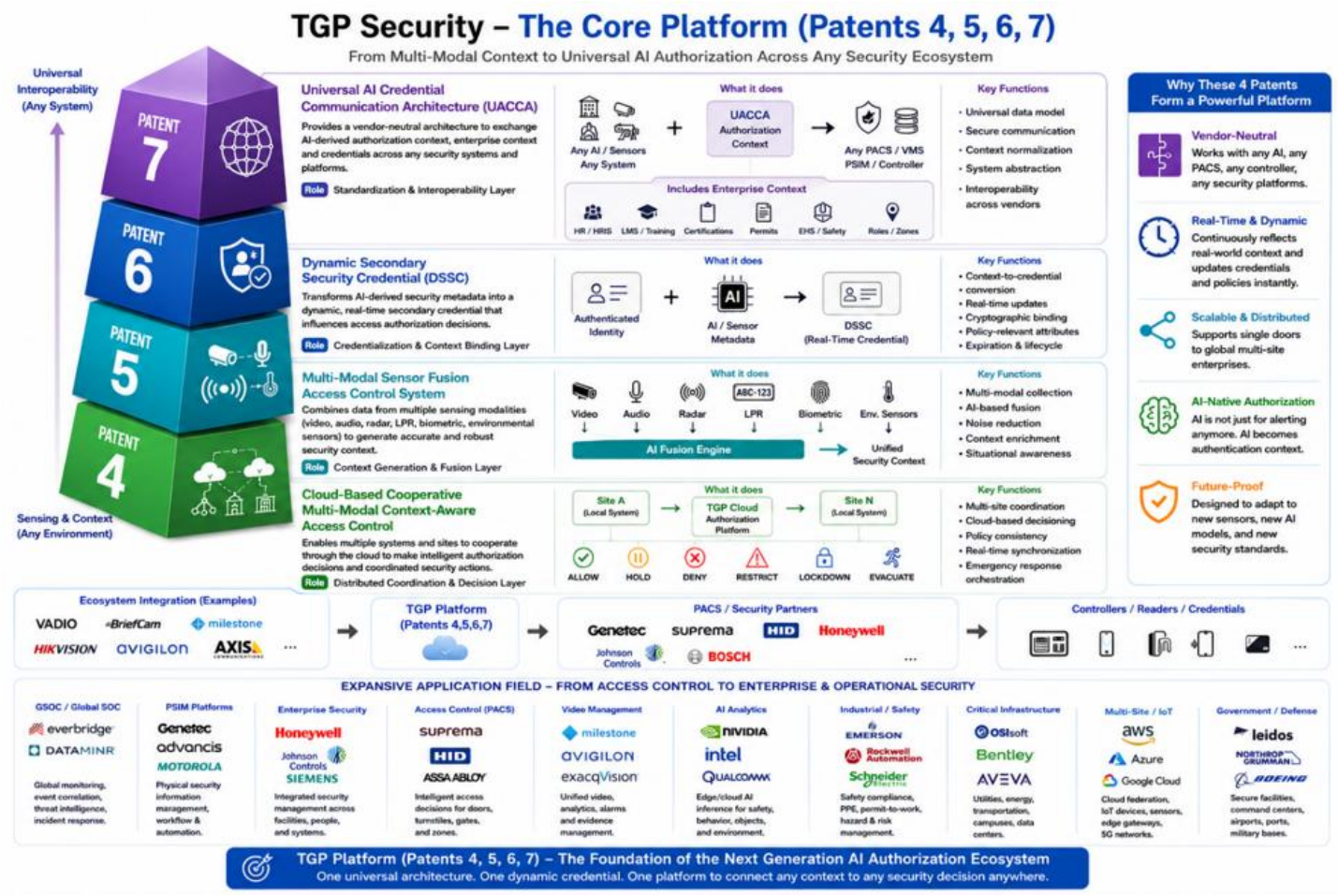
DSSC/UACCA supplies context. Customer policy determines the final authorization outcome. Existing PACS, controllers and other integrated systems execute the approved action.

A scoped POC will evaluate identity association, source verification, information freshness, conflicting inputs, update propagation and audit traceability. Operational benefits and integration repeatability will be measured before broader deployment.

INTELLECTUAL PROPERTY

Four (4) Pending U.S. Patent Applications.

Complementary architectural areas summarized using TGP's internal P4-P7 labels.



Internal label / area	Intended architectural role
P4 - Cloud-Based Cooperative Multi-Modal Context-Aware Access Control	Distributed coordination of context-aware access concepts across systems and locations.
P5 - Multi-Modal Sensor Fusion Access Control System	Combining multiple sensing modalities into policy-relevant context.
P6 - Dynamic Secondary Security Credential (DSSC)	Associating changing security or operational conditions with authenticated identity.
P7 - Universal AI Credential Communication Architecture (UACCA)	Representing and communicating context across heterogeneous security platforms.

Proposed commercial differentiation

A shared authorization-context contract is intended to preserve existing identity and security investments while enabling diverse sources to participate. Source trust, temporal validity, identity binding and interpretable output are central design requirements.

Investor diligence

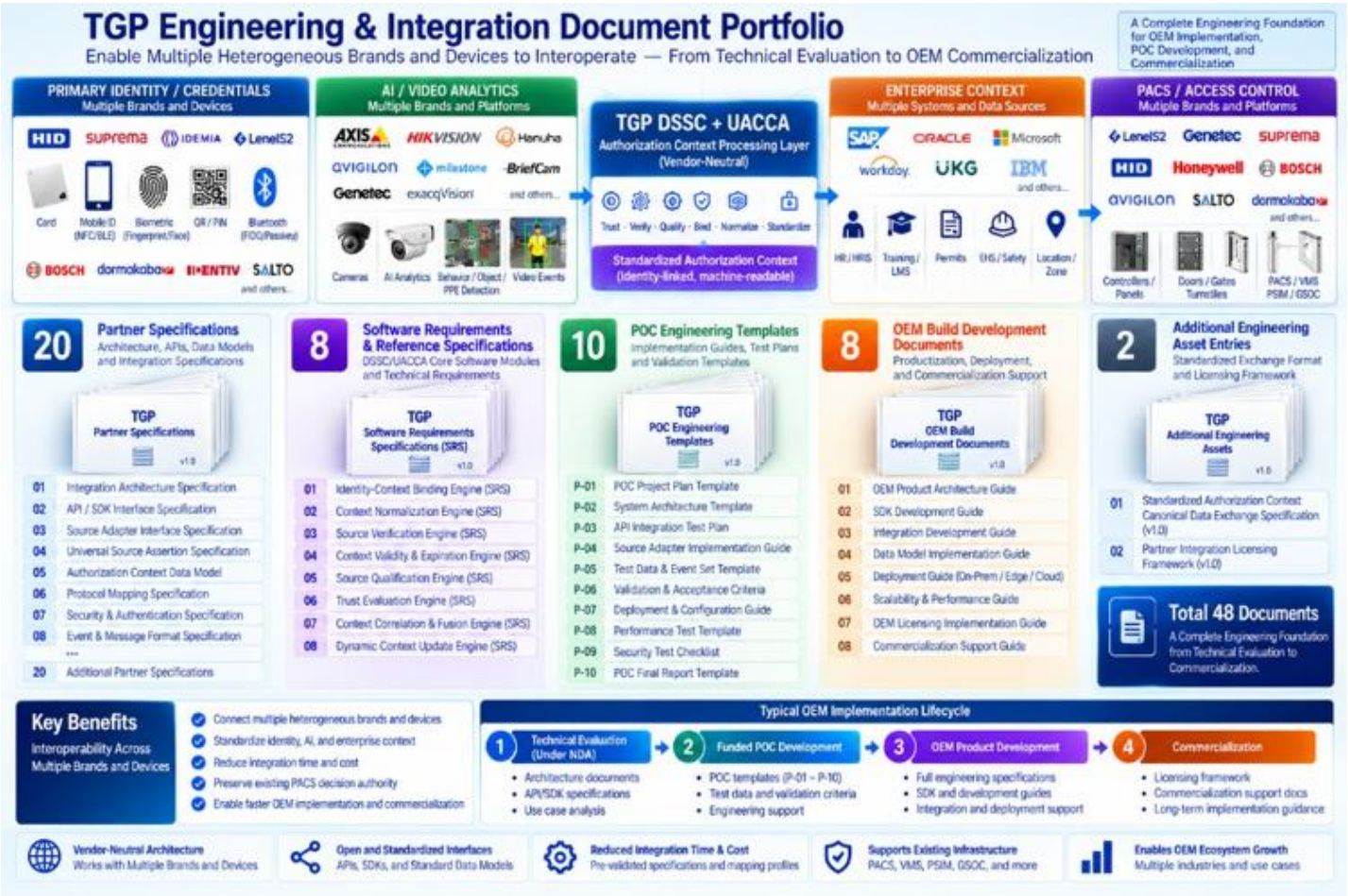
Selected filing records, claims and portfolio information can be reviewed within an agreed disclosure scope. Application identifiers and filing dates should be confirmed against authoritative records during diligence.

Patent-pending status is not a granted patent or proof of claim coverage. This overview describes intended architectural roles and does not assert exclusivity, freedom to operate or a legal conclusion about competing systems.

COMMERCIAL MODEL

Partner-led deployment. Negotiated licensing.

The proposed first paid engagement is a scoped POC program with an OEM, platform provider or integrator.



Vendor examples are illustrative. No partnership, endorsement or completed integration is implied.

Revenue pathway	Commercial deliverable
Funded POC	Agreed requirements, interface work, implementation support and validation package.
OEM technology license	Negotiated rights to use architecture materials, implementation assets and applicable IP.
Integration enablement	Selected mapping profiles and API / SDK assets as actually developed and delivered.
Production license / royalty	Agreed platform, deployment, door or other usage basis; minimum commitments may be negotiated.

Engineering Specifications and POC Planning Assets
Implementation and validation proceed through the funded POC.

The commercial unit is an agreed program and rights package. Pricing, software ownership, production rights and support obligations are defined by contract. Current discussions do not establish committed revenue.

Go-to-market sequence

Select one use case and receiving platform; agree a funded POC; document results; negotiate production rights; then validate a second integration before expanding.

Role allocation

TGP contributes architecture, requirements and agreed technical support. Partner or contracted engineers build the processor, adapters and integration. The partner-led approach requires named technical owners and a sustainable support model.

READINESS & EXECUTION

Turn specifications into evidence.

Founder experience and documented architecture provide a foundation for a focused engineering program.

Michael Park - Founder and CEO

More than 35 years in access control, video management and security integration, including founding leadership at IDTECK and RF Logics. This experience informs TGP’s interoperability focus.

TGP reports technical discussions, selected NDA relationships and sharing of evaluation materials with ecosystem participants. These activities represent engagement; funded implementation and commercial conversion remain outcomes to achieve.

Available foundation	Work required for the POC
Partner specifications and module requirements	Reconcile selected interfaces; freeze fields, semantics and source profiles.
POC working templates and OEM build drafts	Assign owners; implement processor and adapters; create executable fixtures.
Referenced source-assertion / schema assets	Confirm current versions and consistency; run integration and acceptance tests.

Execution capacity

A named technical lead and agreed development allocation are prerequisites. The initial team must cover context processing, source integration, receiving-platform integration, security testing and operations.

The original register contains 46 specification, requirements and template entries plus two version or asset-bundle references. Document count is not evidence of completed software or validated deployment.

CAPITAL & INVITATION

Fund a defined path to validation.

TGP seeks investment and strategic implementation support for a focused POC and a potential OEM licensing pathway.

Funding priority	Reviewable milestone
Scope and engineering ownership	Partner, use case, work allocation, budget and acceptance criteria agreed.
Reference engineering and integration	Working identity-to-context-to-policy flow in the selected test environment.
Security and operational validation	Measured results, audit evidence, failure behavior and documented limitations.
IP diligence and commercialization	Portfolio review; implementation rights, support scope and production licensing package.

Investment amount, financing structure and runway will be developed against the scoped engineering budget. No fixed valuation, revenue forecast or financing amount is represented here.

Questions for the first investor meeting

Which POC would demonstrate value? Who will implement it? What evidence is needed to proceed? Can the integration become a repeatable, commercially viable licensing package?

Next step: an investor and technical review meeting to define the first funded proof of concept.

Michael TG Park | Founder and CEO

Email : michaelp@tgpsecurity.com
Website: www.tgpsecurity.com
LinkedIn

Introductory discussions can use this non-confidential brief. Selected unpublished patent, specification and implementation materials are available subject to NDA and an agreed disclosure scope.