ENTERPRISE SYSTEM BLUEPRINT

STRICTLY CONFIDENTIAL — ENTERPRISE ARCHITECTURE REVIEW

UNIVERSAL ACCESS GATEWAY (UAG)

Technical Architecture, Cryptographic Infrastructure & Blueprint Suite

An exhaustive engineering analysis of Zero-Trust remote access, TLS 1.3 WebSocket Secure (WSS) encapsulation, elliptic curve key exchange (ECDHE & ECDSA), and enterprise identity federation.

Zero-Trust Edge
Port 443 termination with zero backend exposure

TLS 1.3 & WSS
Bi-directional tunnel with forward secrecy

ECDHE / ECDSA
Elliptic curve cryptography on NIST P-256

Enterprise IAM
Active Directory, MFA, and Bearer JWT tokens

SYNCHRONIZED VOICE PRESENTATION INCLUDED (en-IN-NeerjaNeural • 11:02)
Complete professional female narration is embedded in this PDF and accessible via one-click controls.

Play Page 1 (37s) | Full 11m Audio | Voice Viewer

AUTHOR & GOVERNANCE
Technical Architecture & Security Committee

RELEASE VERSION
1.0 Final Release

DATE OF PUBLICATION
September 2026

DOCUMENT SECURITY
SEC-UAG-2026-ARCH-V1

DOCUMENT STRUCTURE

Executive Summary & Table of Contents

Play Voice (46s) | Full 11m | Voice Viewer | UAGSERVER

TIER 1: FOUNDATIONS

01 Executive Overview & System Fundamentals — 46s — Page 03
02 Architectural Foundation & Network Topology — 47s — Page 04
03 Project Roadmap, Milestones & Lifecycle Timeline — 45s — Page 05
04 Enterprise Security Framework & Strategic Pillars — 45s — Page 06

TIER 2: SYSTEM BLUEPRINT

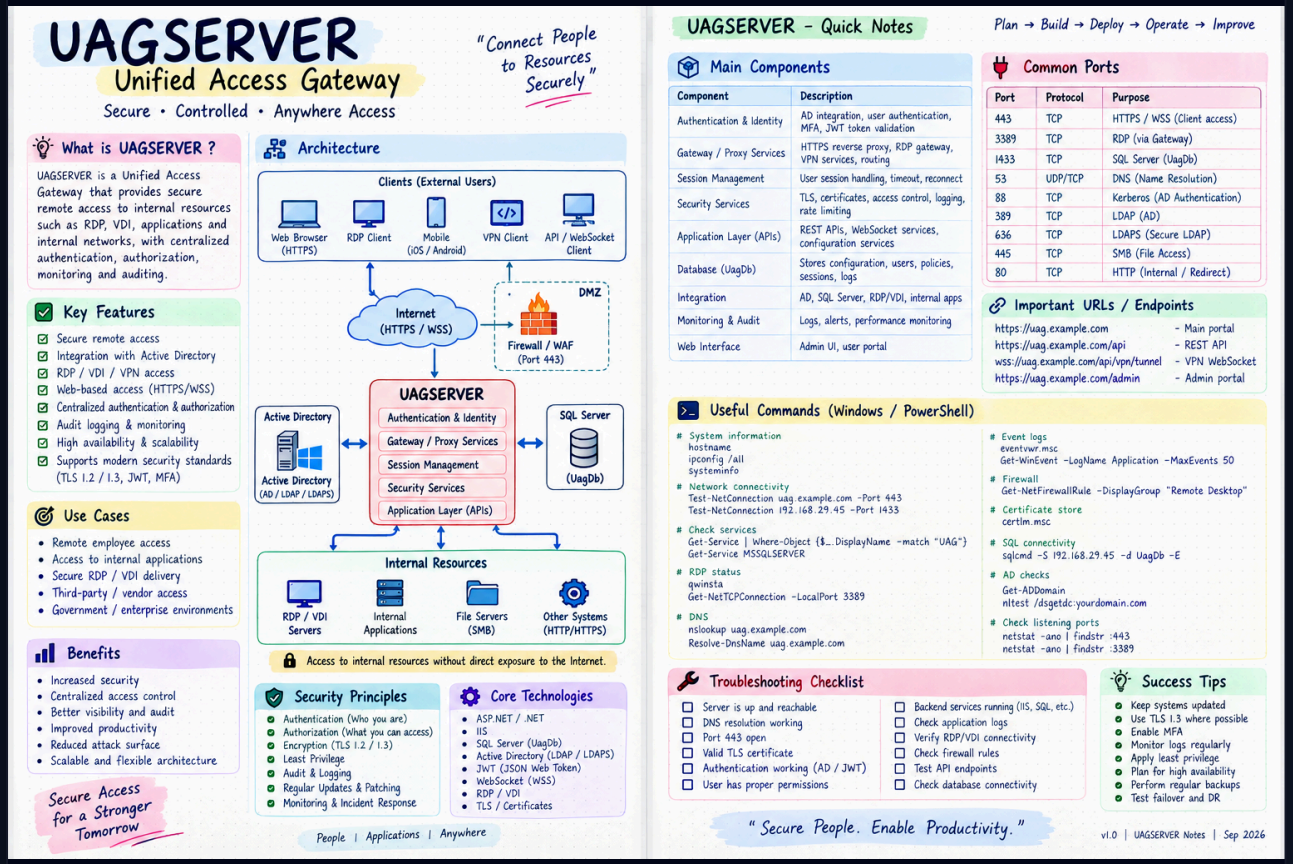
05 Gateway System Architecture & Exploded Blueprint — 42s — Page 07
06 UserApplication Client Blueprint & Stack Architecture — 41s — Page 08
07 Client-to-Gateway WSS Connection Architecture — 44s — Page 09

TIER 3: PROTOCOLS & CRYPTO

08 Step-by-Step WebSocket Secure (WSS) Channel Flow — 38s — Page 10
09 Protocol Upgrade & WSS Handshake Blueprint — 40s — Page 11
10 End-to-End TLS 1.3 Handshake & Certificate Validation — 39s — Page 12
11 Cryptographic Deep-Dive: ECDHE & ECDSA Key Exchange — 41s — Page 13

TIER 4: COMPARATIVE STUDY

12 Platform Comparison: UAGSERVER vs Accops Workspace — 38s — Page 14
13 Strategic Superiority Analysis & Ownership Advantage — 36s — Page 15
14 Comprehensive Synthesis, Security Baseline & Conclusion — 37s — Page 16



Click to Full Screen

Blueprint 01: Foundational Notes, Architectural Components, Network Ports & Operational Commands

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

UAGServer provides secure, audited remote access to internal resources (RDP, VDI, internal applications) with centralized Active Directory authentication, MFA, and JWT session authorization without exposing backend ports directly to the Internet.

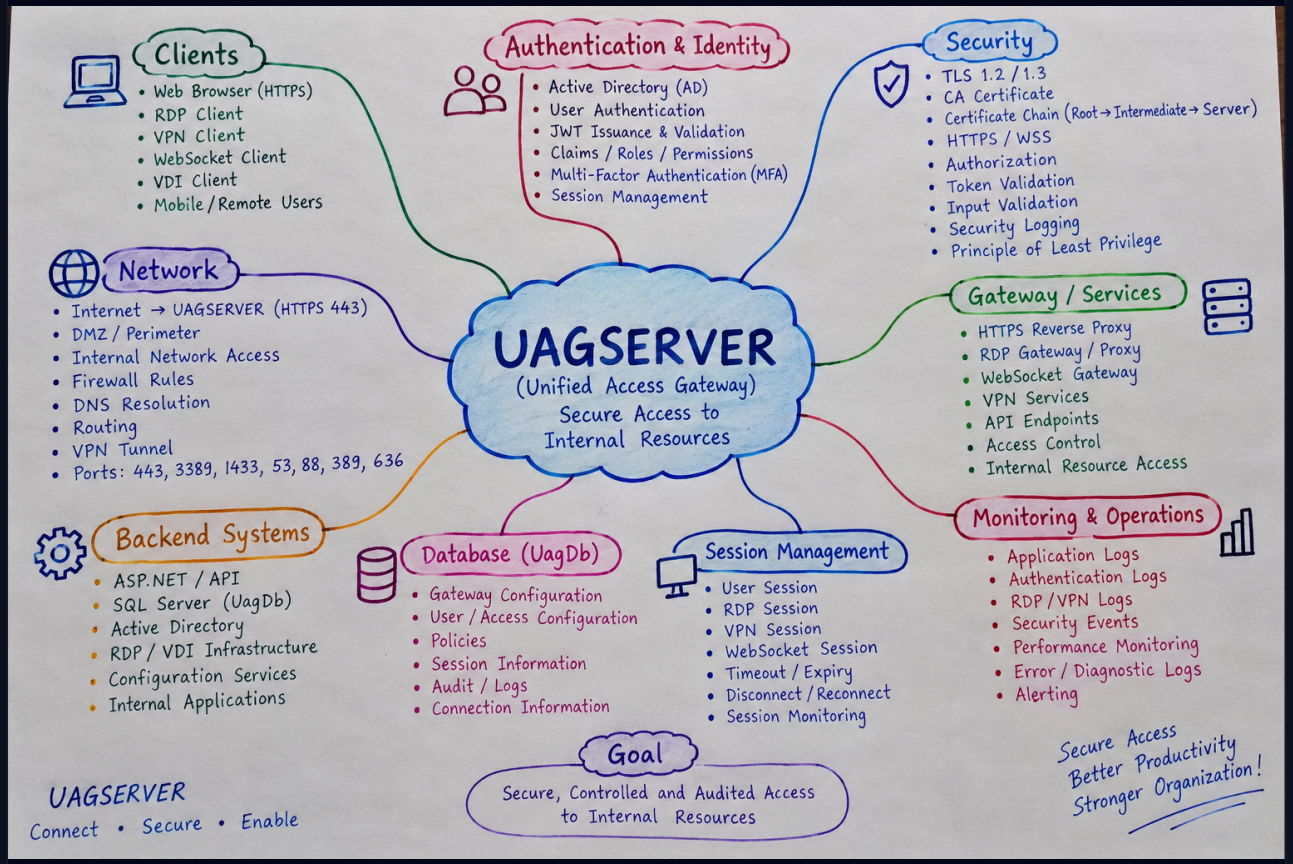
TECHNICAL SPECIFICATIONS

Core Paradigm	Reverse Proxy / Secure WSS Gateway
External Ingress	TCP 443 (HTTPS & WebSocket Secure)
Identity & Auth	Active Directory (LDAP/LDAPS), Kerberos, MFA, JWT
Database Engine	SQL Server (UagDb) for Config, Sessions, Logs
Internal Protocols	RDP (3389), SMB (445), HTTP/HTTPS (80/443), SQL (1433)

KEY ARCHITECTURAL HIGHLIGHTS

- Centralized session management with automated timeout and reconnect handling.
- Complete network isolation: internal servers have zero direct public IP exposure.
- Comprehensive audit logging spanning authentication, connections, and diagnostic events.

```
PowerShell Diagnostics: Test-NetConnection uag.example.com -Port 443; qwinsta; Get-WinEvent -LogName Application -MaxEvents 50; sqlcmd -S 192.168.29.45 -d uagDb -E
```



Click to Full Screen

Blueprint 02: Conceptual System Schematic, Perimeter DMZ Boundaries & Data Isolation Model

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

The foundational topology isolates external untrusted clients from internal resources via a strict DMZ perimeter boundary. External users authenticate through UAGServer, which governs all session brokering and traffic forwarding.

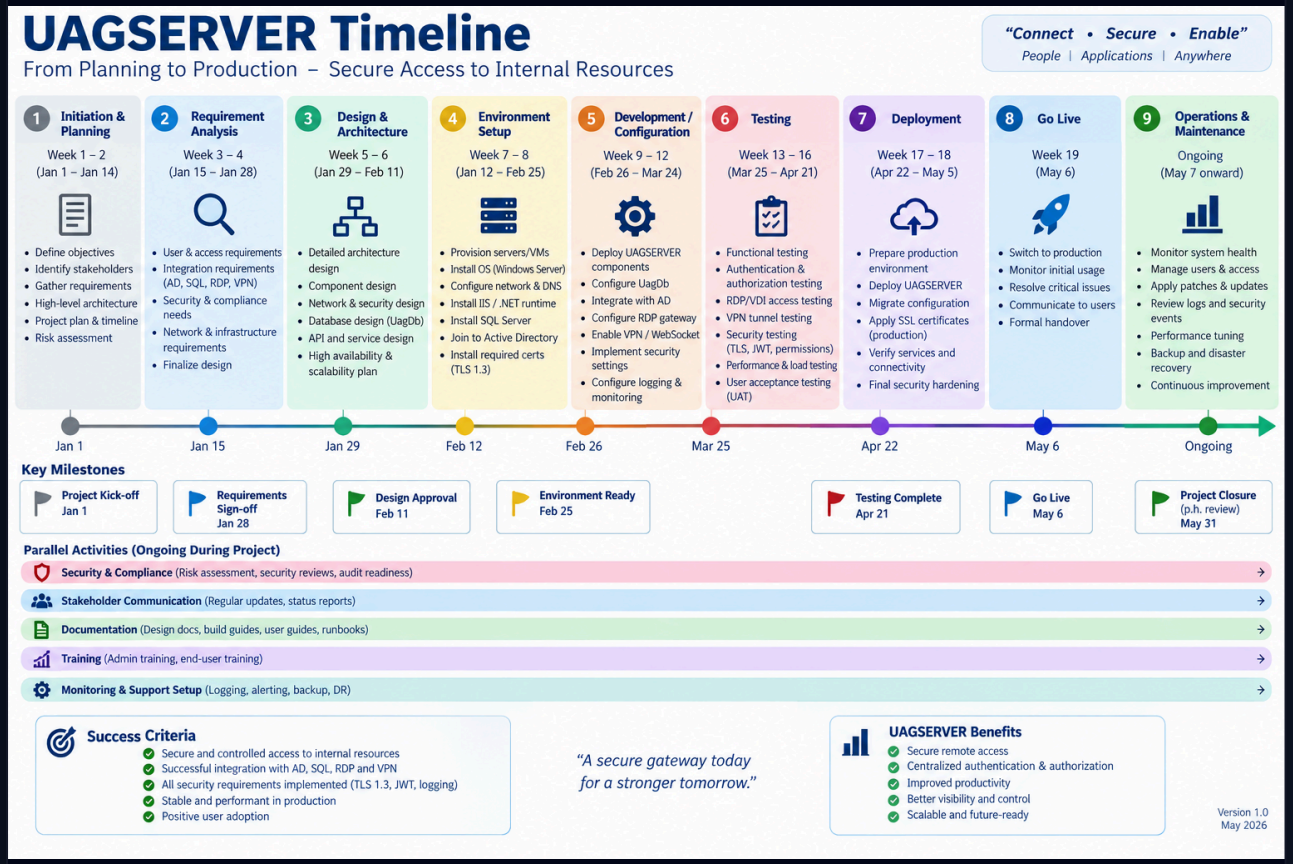
TECHNICAL SPECIFICATIONS

Perimeter Zone	Demilitarized Zone (DMZ) behind Dual Firewalls
Inbound Policy	Allow Port 443 only; Deny all other public inbound
Session Types	User Session, RDP Session, VPN Session, WebSocket Session
Security Controls	TLS 1.2/1.3, CA Chain Validation, Token Check, Least Privilege
Telemetry	Application Logs, Auth Logs, RDP/VPN Logs, Security Audits

KEY ARCHITECTURAL HIGHLIGHTS

- Clients supported: Web Browser (HTML5), RDP Client, VPN Client, WebSocket Client, VDI.
- Backend Systems: ASP.NET Core API, SQL Server (UagDb), Active Directory, VDI Clusters.
- Granular access control based on user claims, organizational roles, and IP policies.

```
Core Principle: 'Secure Access to Internal Resources without Direct Internet Exposure — Enforcing Least Privilege at Every Layer.'
```



Click to Full Screen

Blueprint 03: 19-Week Implementation Lifecycle Roadmap, Milestone Gates & Parallel Tracks

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

A structured 19-week implementation lifecycle guiding UAGServer from project kick-off to production switchover, followed by ongoing continuous operations, health monitoring, and security patching.

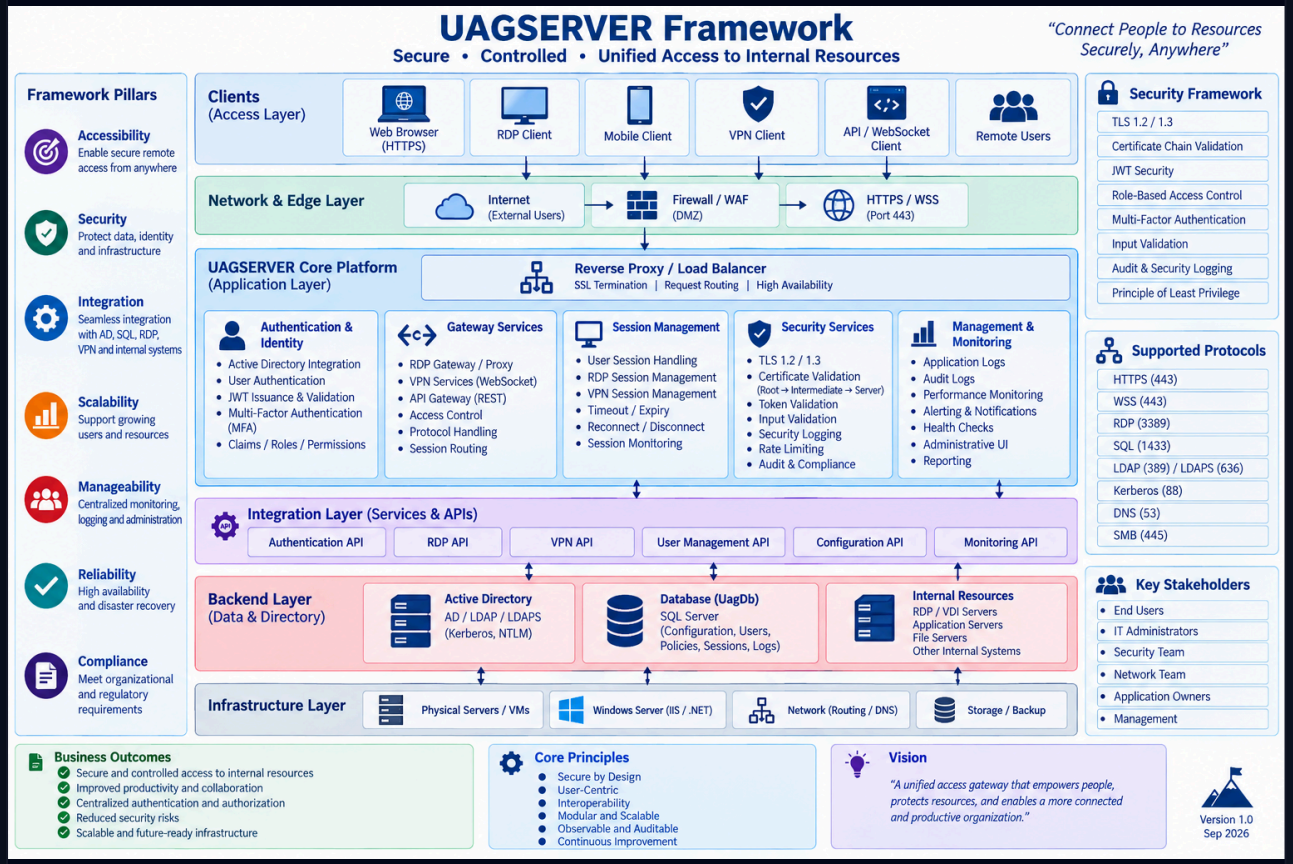
TECHNICAL SPECIFICATIONS

Total Duration	19 Weeks (Phased Planning to Production Go-Live)
Phase 1 & 2	Initiation, Stakeholder Gathering & Requirements Sign-off (Jan 1-28)
Phase 3 & 4	Detailed Design, Database Schema & Environment Setup (Jan 29-Feb 25)
Phase 5 & 6	Core Development, RDP Integration & Rigorous Testing (Feb 26-Apr 21)
Phase 7 & 8	Staging Deployment, Production Switch (May 6) & Operations (Ongoing)

KEY ARCHITECTURAL HIGHLIGHTS

- Four continuous parallel tracks: Security & Compliance, Communication, Documentation, Training.
- Success Criteria: High availability, zero unpatched vulnerabilities, full AD/SQL integration.
- Formal sign-off gates at Design Approval (Feb 11) and Testing Completion (Apr 21).

```
Operational Standard: 'Continuous health monitoring, proactive patching, weekly audit reviews, and tested disaster recovery failover.'
```



Blueprint 04: Six Security Framework Pillars, Multi-Tiered Architecture & Governance Matrix

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

The enterprise security framework establishes an end-to-end governance model balancing seamless accessibility with military-grade security, standards compliance, and multi-tenant organizational scalability.

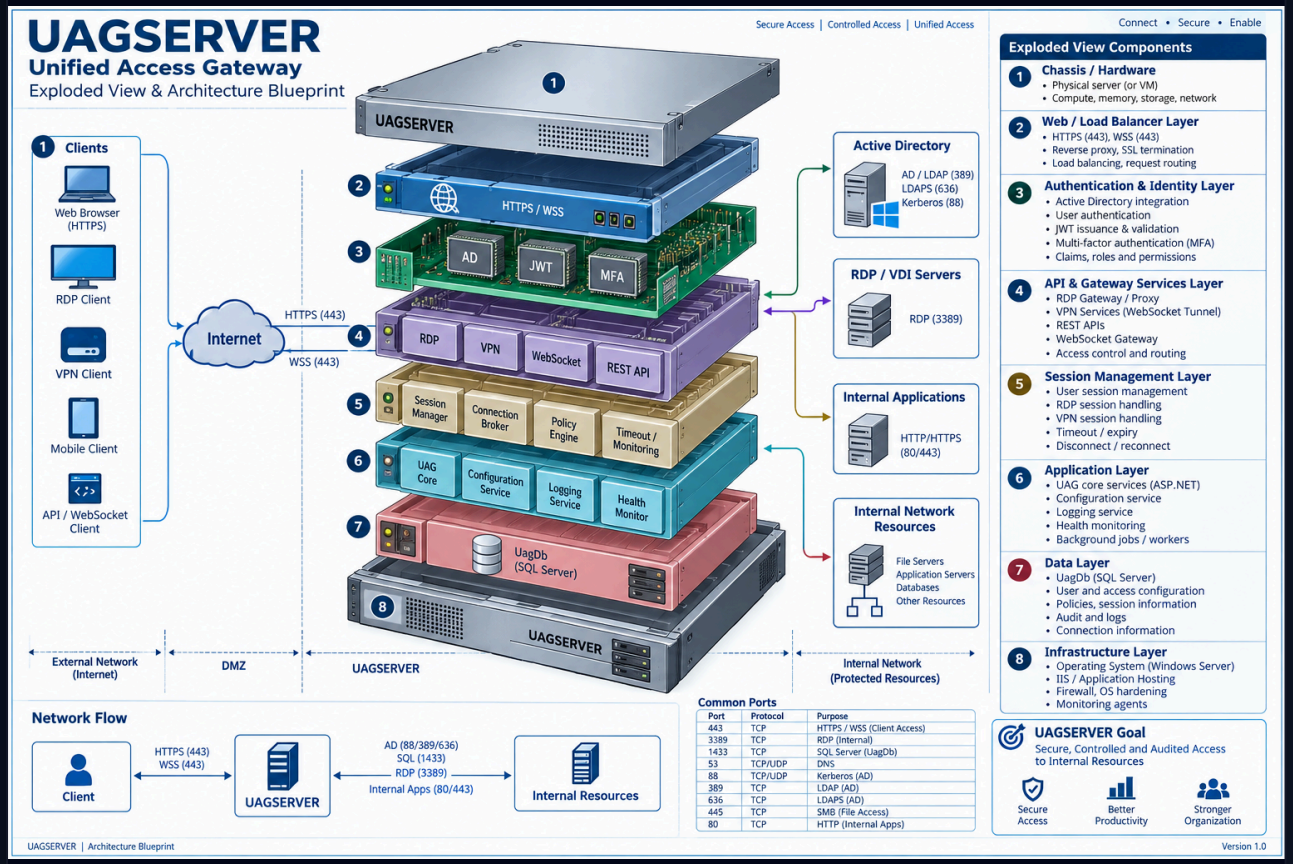
TECHNICAL SPECIFICATIONS

Pillar 1 & 2	Internet Accessibility (Anywhere Access) & Security (Identity Defense)
Pillar 3 & 4	Seamless Integration (AD, SQL, RDP, VPN) & Elastic Scalability
Pillar 5 & 6	Centralized Manageability & Strict Regulatory Compliance
Core Principles	Secure by Design, User-Centric, Interoperable, Modular, Auditable
Protocols Supported	HTTPS (443), WSS (443), RDP (3389), SQL (1433), Kerberos (88), SMB (445)

KEY ARCHITECTURAL HIGHLIGHTS

- Multi-tiered decoupling: Access Layer -> Network & Edge -> Core Platform -> Integration -> Backend.
- Strict adherence to least privilege, rate limiting, token validation, and CA chain verification.
- Comprehensive stakeholder alignment spanning end users, SecOps, network engineers, and management.

```
Framework Vision: 'A unified access gateway that empowers people, protects resources, and enables a more connected and productive organization.'
```



Click to Full Screen

Blueprint 05: Layer-by-Layer Exploded Architecture of the UAGServer Gateway Stack

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

An exploded decomposition of the eight modular layers constituting UAGServer, demonstrating how requests traverse from bare-metal hardware and web load balancing through authentication, session brokering, and backend dispatch.

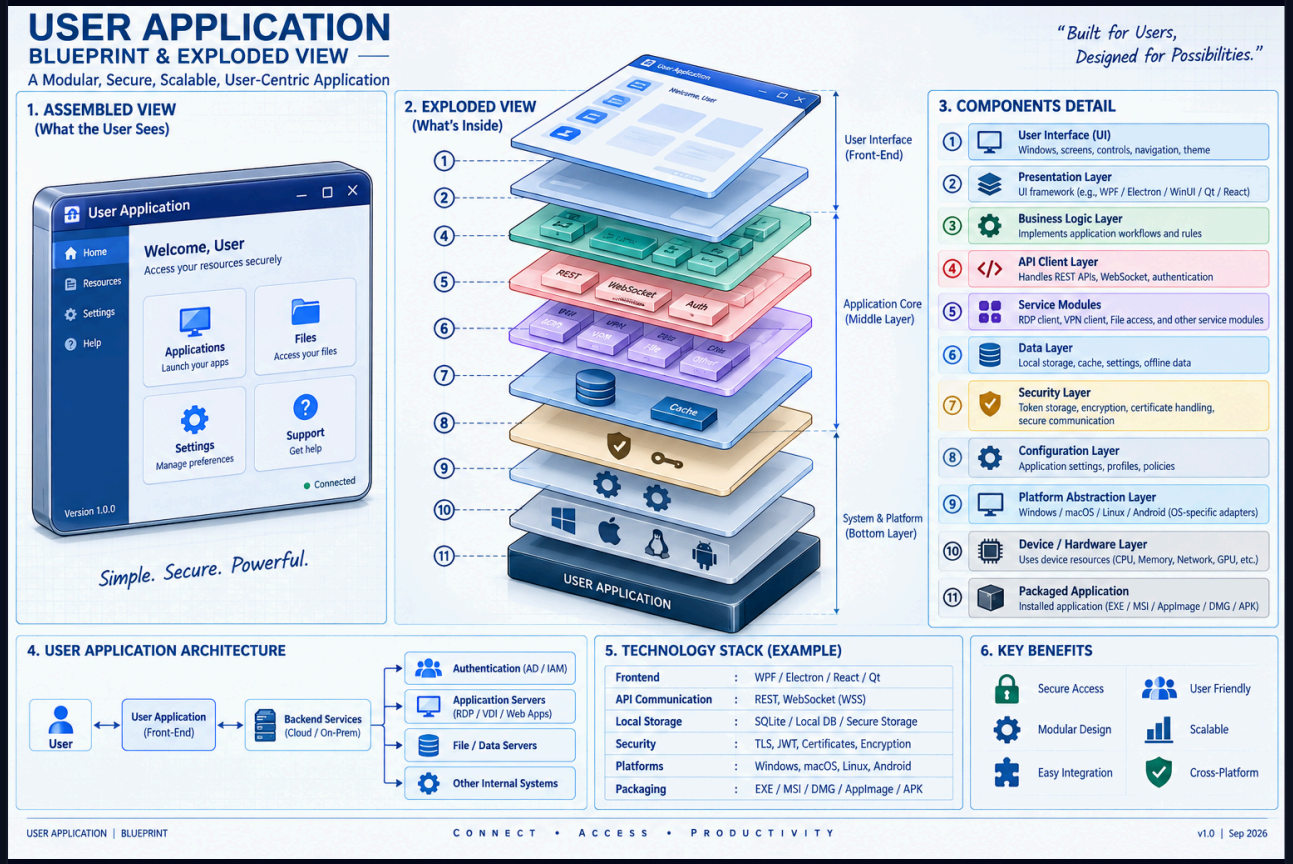
TECHNICAL SPECIFICATIONS

Layer 1 & 2	Physical Chassis/VM Compute & Web Load Balancer (Reverse Proxy, SSL Termination)
Layer 3 & 4	Authentication & Identity (AD, MFA, JWT) & API Gateway Services (RDP/WSS)
Layer 5 & 6	Session Management (State, Timeouts) & Application Layer (ASP.NET Core Engine)
Layer 7 & 8	Data Layer (UagDb SQL Server) & Infrastructure Layer (Windows Server, IIS, Hardening)
Network Path	Client (HTTPS/WSS) -> Firewall 443 -> Reverse Proxy -> UAG Core -> Backend (3389/1433)

KEY ARCHITECTURAL HIGHLIGHTS

- Decoupled micro-services allow independent scaling of the WebSocket gateway and auth engine.
- Centralized UagDb stores user profiles, access policies, active sessions, and tamper-resistant audit logs.
- Built-in health monitor continuously validates Active Directory, SQL, and desktop cluster connectivity.

```
Architectural Goal: 'Secure, Controlled, and Audited Access to Internal Resources — Better Productivity, Stronger Organization.'
```



Click to Full Screen

Blueprint 06: UserApplication Exploded Client Blueprint, Internal Modules & Cross-Platform Packaging

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

UserApplication provides a unified, cross-platform client experience across Windows, macOS, and Linux, abstracting underlying protocol complexities while enforcing local token security and cryptographic verification.

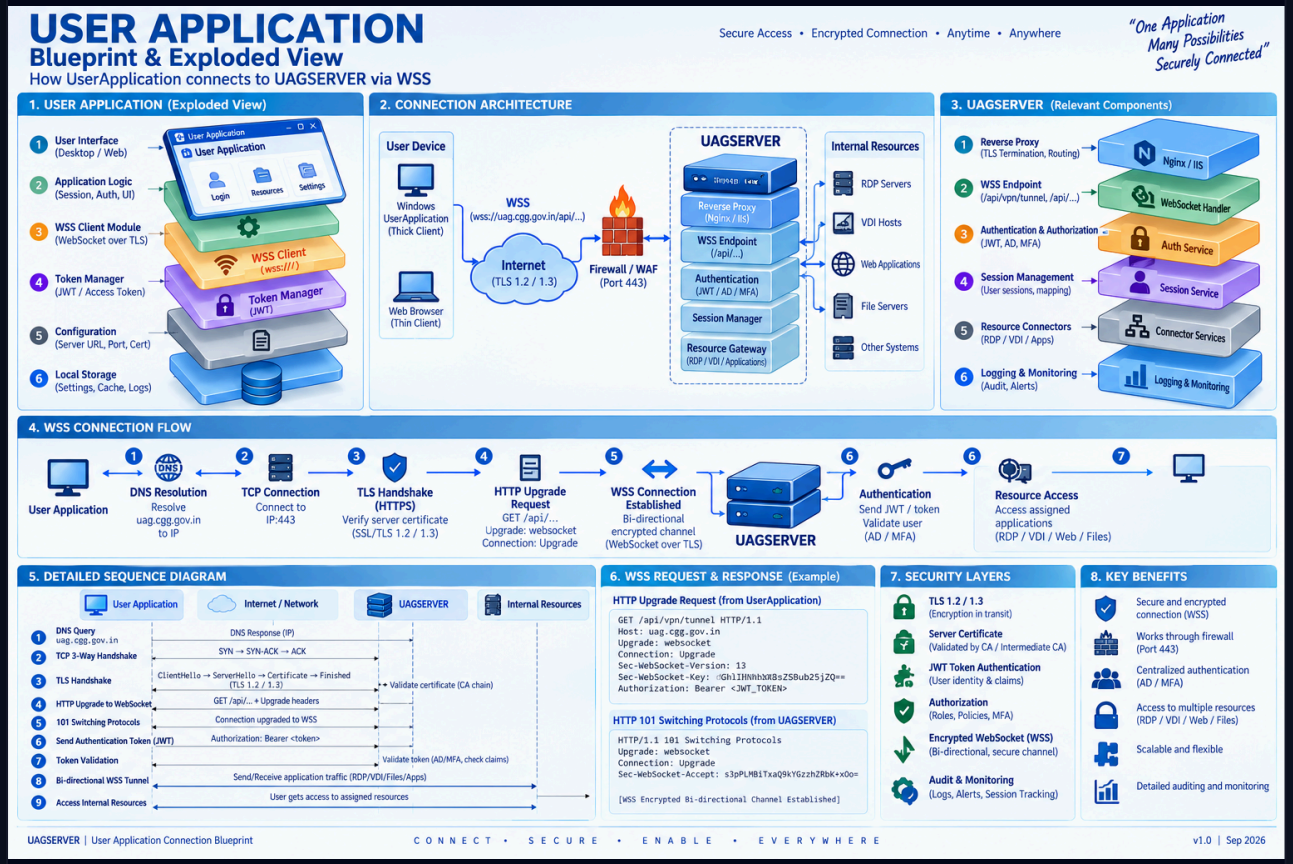
TECHNICAL SPECIFICATIONS

Presentation Layer	Modern UI Framework (WPF / Electron / React Native Shell)
Application Core	Business Logic, Access Workflows, Policy Enforcement
Client Protocols	REST API Client, Asynchronous WSS Client Module, RDP/VDI Launcher
Security & Data	Secure Vault for JWT, SQLite Local DB, TLS 1.3 Stack, Certificate Store
Packaging Targets	Windows (MSI/EXE), macOS (DMG/PKG), Linux (AppImage/DEB), Android (APK)

KEY ARCHITECTURAL HIGHLIGHTS

- Seamless resource catalog presenting authorized remote desktops, VDI sessions, and web portals.
- Offline token caching with cryptographically enforced hardware-bound expiry.
- Built-in connection diagnostics and automatic tunnel recovery upon network interruption.

```
Client Motto: 'Built for Users, Designed for Possibilities – Simple, Secure, Powerful Cross-Platform Remote Workspace Access.'
```



Click to Full Screen

Blueprint 07: Client-to-Gateway Protocol Handshake, WSS Upgrade & Cryptographic Token Exchange

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

Detailed sequence flow illustrating how UserApplication establishes a secure, persistent WebSocket channel over TLS to UAGServer, exchanges authorization headers, and securely streams remote desktop payloads.

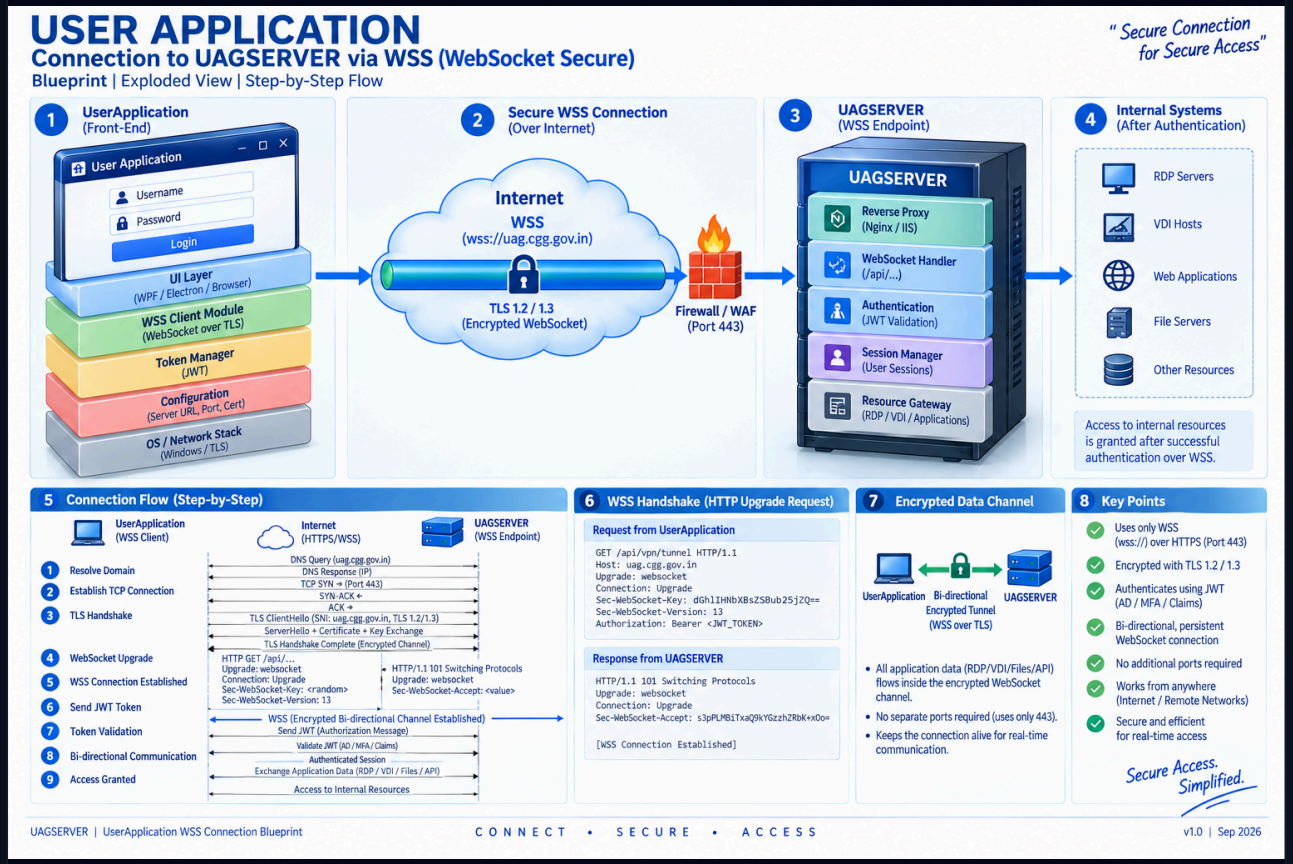
TECHNICAL SPECIFICATIONS

Phase 1: TCP/TLS	DNS Resolution -> TCP 3-Way Handshake -> TLS 1.2/1.3 Certificate Negotiation
Phase 2: Upgrade	HTTP GET /api/vpn/tunnel with Upgrade: websocket & Sec-WebSocket-Key
Phase 3: Switching	Server validates headers -> Returns HTTP 101 Switching Protocols
Phase 4: Auth	Client transmits Authorization: Bearer inside the encrypted tunnel
Phase 5: Gateway	UAGServer validates token against AD/IdP -> Dispatches to target RDP host

KEY ARCHITECTURAL HIGHLIGHTS

- Complete bi-directional multiplexing: one single TCP connection handles all control and desktop traffic.
- No special firewall ports needed on client side: operates seamlessly through corporate HTTP proxies.
- Detailed sequence diagram validates CA chain integrity before any credentials or tokens are sent.

```
Upgrade Request Sample: GET /api/vpn/tunnel HTTP/1.1 | Host: uag.example.com | Upgrade: websocket | Connection: Upgrade | Authorization: Bearer
```



Click to Full Screen

Blueprint 08: Nine-Step End-to-End WebSocket Connection Lifecycle & Data Tunnel Flow

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

A comprehensive nine-step blueprint detailing every discrete stage of the WSS communication lifecycle from initial client domain resolution to active multi-gigabit encrypted tunnel throughput.

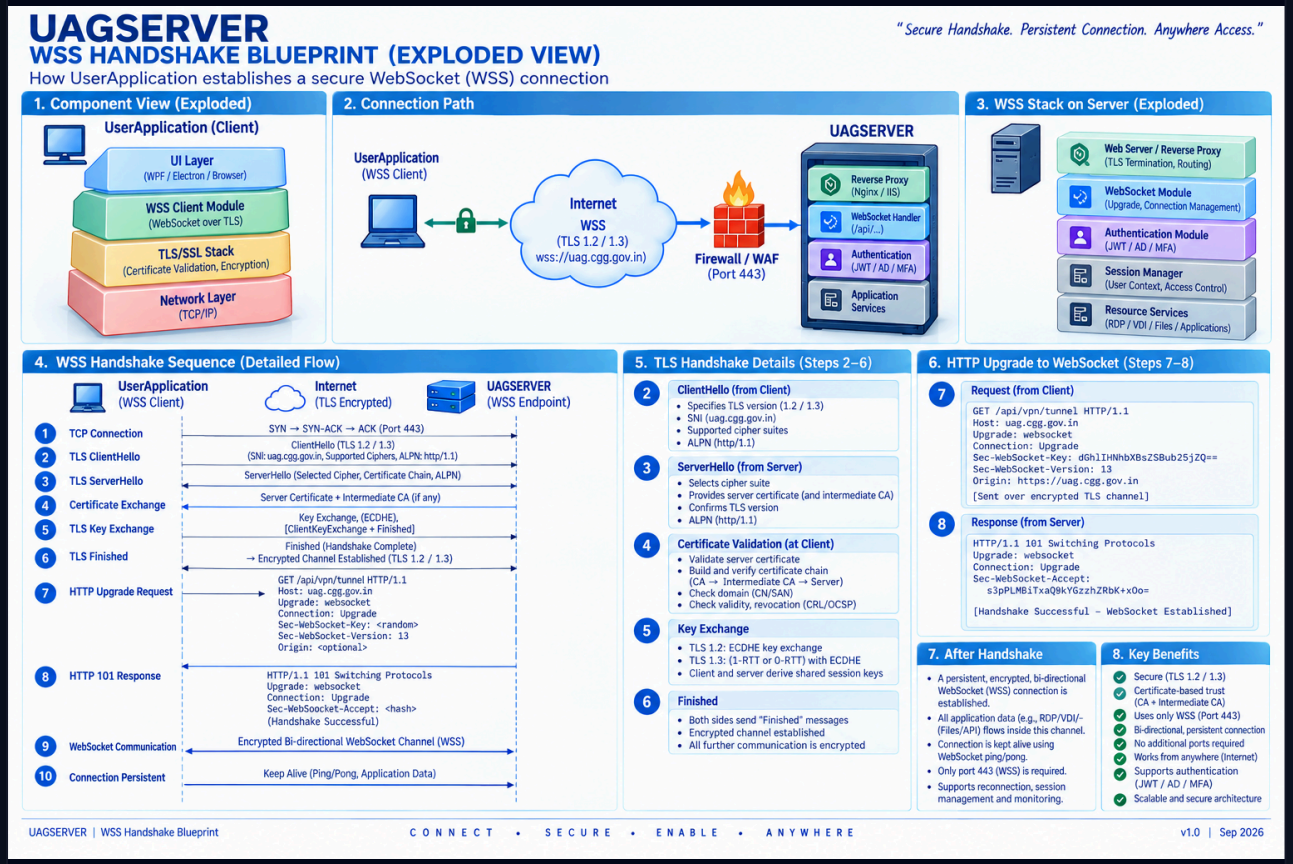
TECHNICAL SPECIFICATIONS

Step 1 & 2	Resolve Domain via DNS & Establish TCP SYN/ACK Handshake on Port 443
Step 3 & 4	Execute TLS Handshake with SNI & Issue HTTP Upgrade Request to /api/...
Step 5 & 6	Establish WSS Channel (101 Switching) & Transmit Signed JWT Token
Step 7 & 8	Validate Token & Claims against AD -> Open Bi-directional Encrypted Data Channel
Step 9	Grant Access to Internal Resources (RDP 3389, VDI Hosts, File Servers, Web Apps)

KEY ARCHITECTURAL HIGHLIGHTS

- Encrypted Data Channel: All RDP, VDI, file, and API payloads flow inside the single WSS stream.
- Persistent keep-alive: WebSocket ping/pong frames detect network failure in under 2 seconds.
- High efficiency: eliminates per-packet TCP handshake overhead inherent in legacy VPN solutions.

```
Core Value: 'Uses only WSS over Port 443 — No additional ports required — Works from anywhere — Secure Access Simplified.'
```



Click to Full Screen

Blueprint 09: Granular Protocol Mechanics of TLS Negotiation, HTTP 101 Upgrade & Frame Streaming

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

In-depth protocol inspection of the handshake sequence, detailing ClientHello/ServerHello parameter negotiation, certificate validation, key exchange algorithms, and HTTP upgrade header specifications.

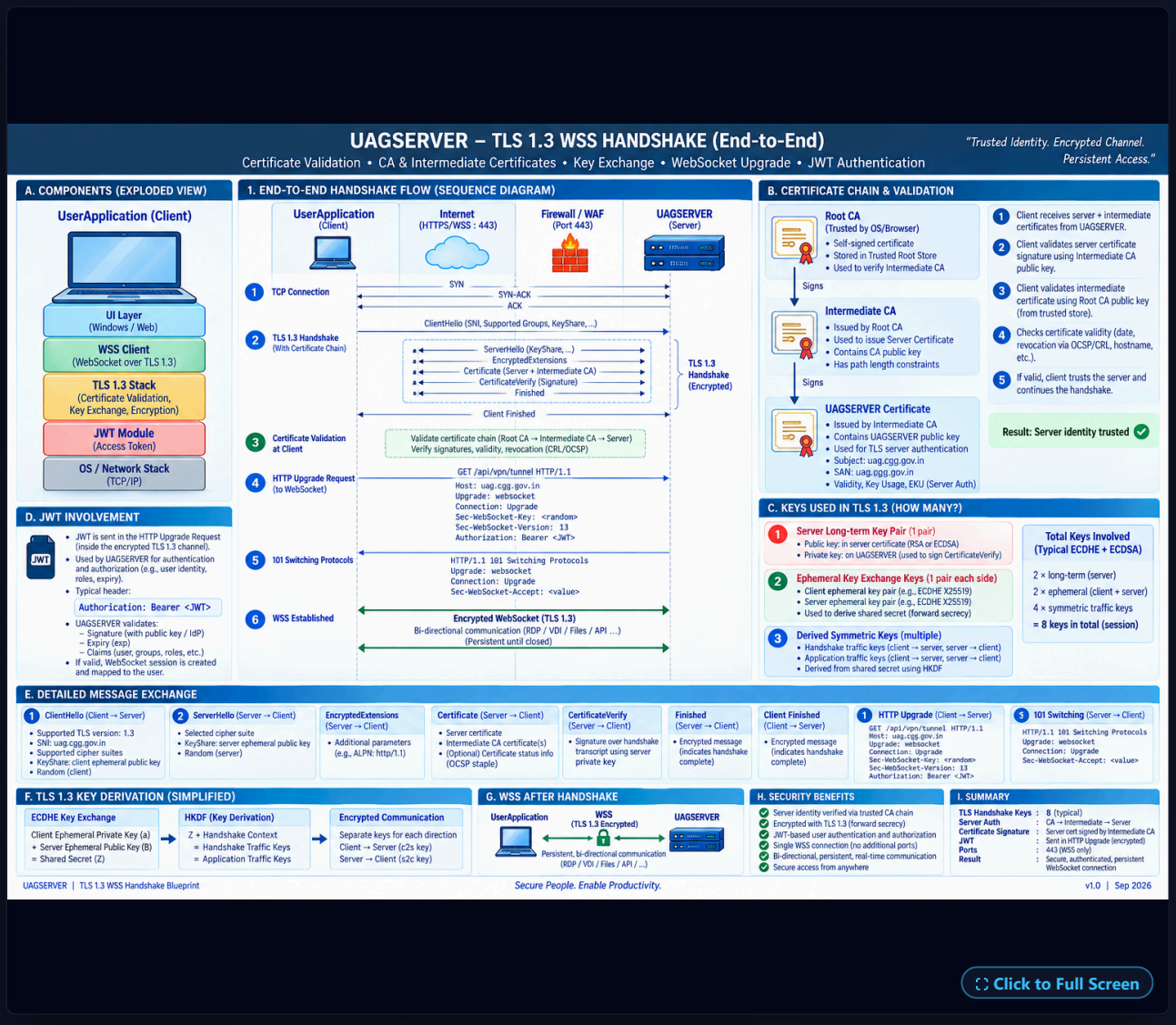
TECHNICAL SPECIFICATIONS

ClientHello	Specifies TLS version, SNI hostname, supported cipher suites, ALPN (http/1.1)
ServerHello	Selects cipher suite, supplies server certificate chain, completes ECDHE exchange
Client Validation	Validates certificate chain (Root CA -> Intermediate CA -> Server Cert), checks CRL/OCSP
Upgrade Request	GET /api/vpn/tunnel with Sec-WebSocket-Key and Sec-WebSocket-Version: 13
Switching Protocols	HTTP/1.1 101 Switching Protocols with Sec-WebSocket-Accept:

KEY ARCHITECTURAL HIGHLIGHTS

- Both endpoints send Finished messages verifying transcript integrity before payload transmission.
- WSS Server Stack exploded: Reverse Proxy -> WebSocket Module -> Auth Module -> Session Manager.
- Bi-directional framing guarantees zero packet loss and minimal latency for high-frame-rate RDP.

```
Security Standard: 'Certificate-based trust via hierarchical CA verificat
ion ensures zero vulnerability to Man-in-the-Middle eavesdropping.'
```



Click to Full Screen

Blueprint 10: TLS 1.3 Handshake Sequence, 8-Key Derivation Lifecycle & JWT Authorization

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

Exhaustive analysis of the TLS 1.3 protocol exchange, detailing the 1-RTT handshake, certificate chain hierarchy, derivation of 8 session keys, and seamless JWT authorization mapping.

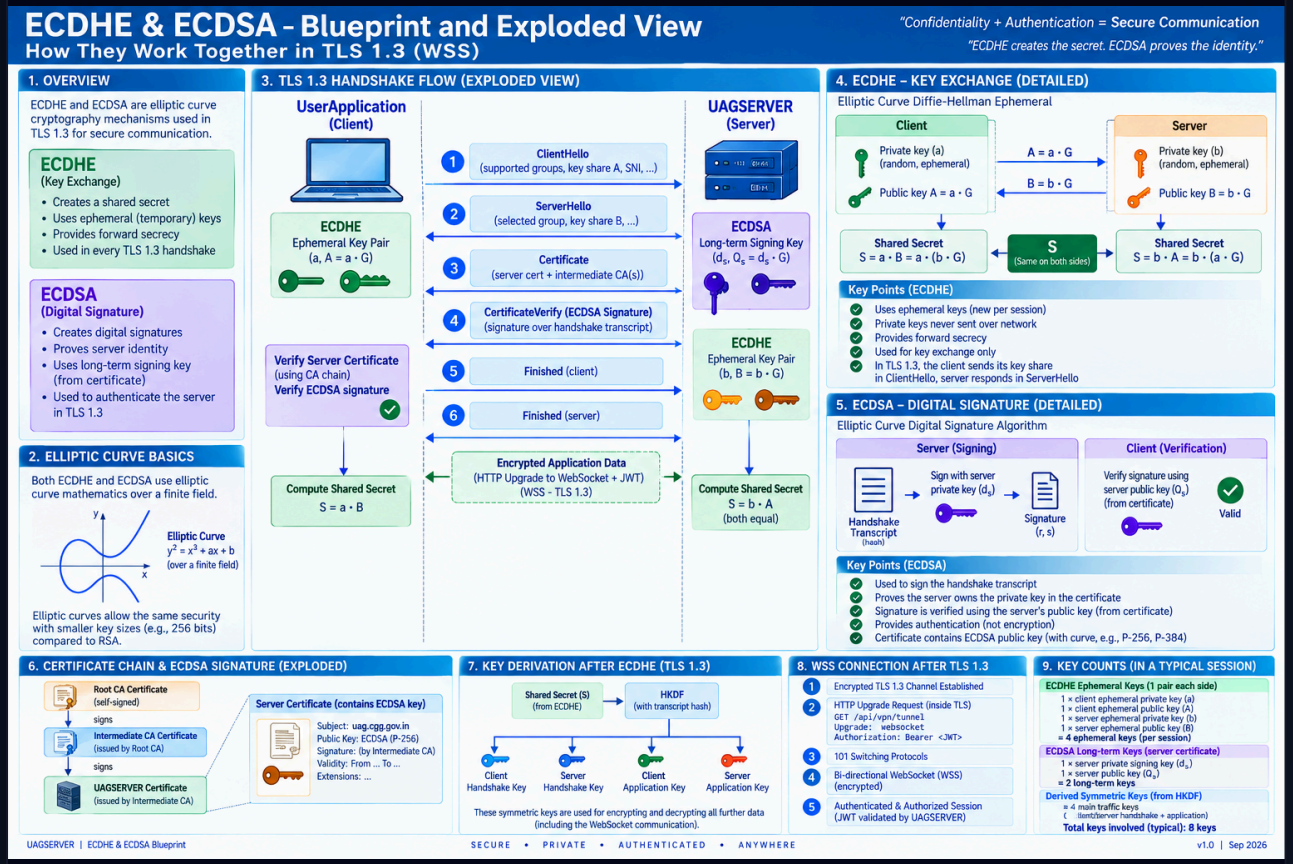
TECHNICAL SPECIFICATIONS

Root CA Store	Self-signed Root CA trusted by OS/Browser -> Signs Intermediate CA
Intermediate CA	Issues Server Certificate with Subject Alternative Name (SAN) & Server Auth EKU
Server Certificate	Contains ECDSA/RSA Public Key, validated against CRL and OCSP stapling
Total Keys (8)	2 Server Long-Term + 2 Ephemeral ECDHE (Client/Server) + 4 Derived Symmetric Traffic Keys
JWT Validation	Signature verified against IdP public key; Expiry (exp), Roles, and Claims validated

KEY ARCHITECTURAL HIGHLIGHTS

- Mandatory Forward Secrecy: Ephemeral ECDHE keys ensure past traffic cannot be retroactively decrypted.
- HKDF Key Derivation: Handshake and Application traffic keys derived separately for each direction (c2s, s2c).
- Zero round-trip latency overhead: ServerHello, EncryptedExtensions, and Certificate arrive in 1-RTT.

```
Cryptographic Key Budget: 2 Long-Term Keys + 2 Ephemeral Keys + 4 Symmetr
ic Traffic Keys = 8 Keys Total per Session.
```



Click to Full Screen

Blueprint 11: Elliptic Curve Mathematics, Ephemeral Diffie-Hellman & Digital Signature Verification

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

Mathematical and structural deep-dive into Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for secret derivation and the Elliptic Curve Digital Signature Algorithm (ECDSA) for server identity authentication.

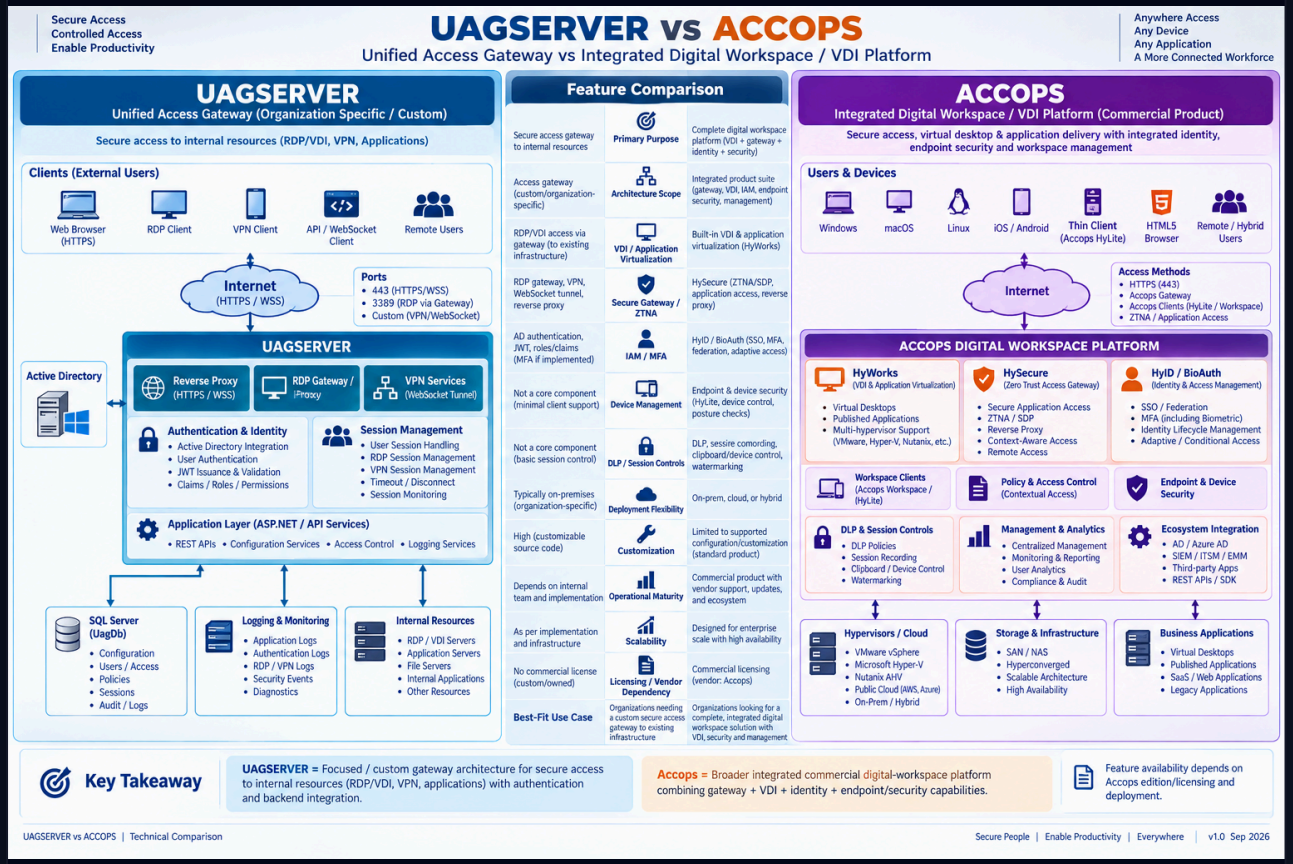
TECHNICAL SPECIFICATIONS

Curve Equation	Weierstrass Equation: y^2 = x^3 + ax + b over finite field F_p (NIST P-256 / secp256r1)
Key Size Advantage	256-bit Elliptic Curve provides security equivalent to 3072-bit RSA with 10x speedup
ECDHE Mechanics	Client (a, A=a*G) & Server (b, B=b*G) compute Shared Secret S = a*B = b*A = a*b*G
ECDSA Mechanics	Server signs handshake transcript with private key d_s; Client verifies signature (r, s) with Q_s
Forward Secrecy	Ephemeral private keys (a, b) discarded immediately after HKDF symmetric derivation

KEY ARCHITECTURAL HIGHLIGHTS

- Formula for Success: 'Confidentiality + Authentication = Secure Communication.'
- ECDHE creates the secret; ECDSA proves the identity without revealing private keys.
- Compact signatures and keys dramatically reduce network packet size during high-volume logins.

```
Cryptographic Theorem: S = a · B = b · A = a · b · G (Points on elliptic curve commute, yielding identical shared secret S).
```



Click to Full Screen

Blueprint 12: Architectural Comparison between Custom Access Gateway & Commercial Product Suite

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

A balanced architectural comparison evaluating UAGServer (a customized, protocol-level access gateway) against the Accops Digital Workspace Suite (an integrated commercial VDI platform).

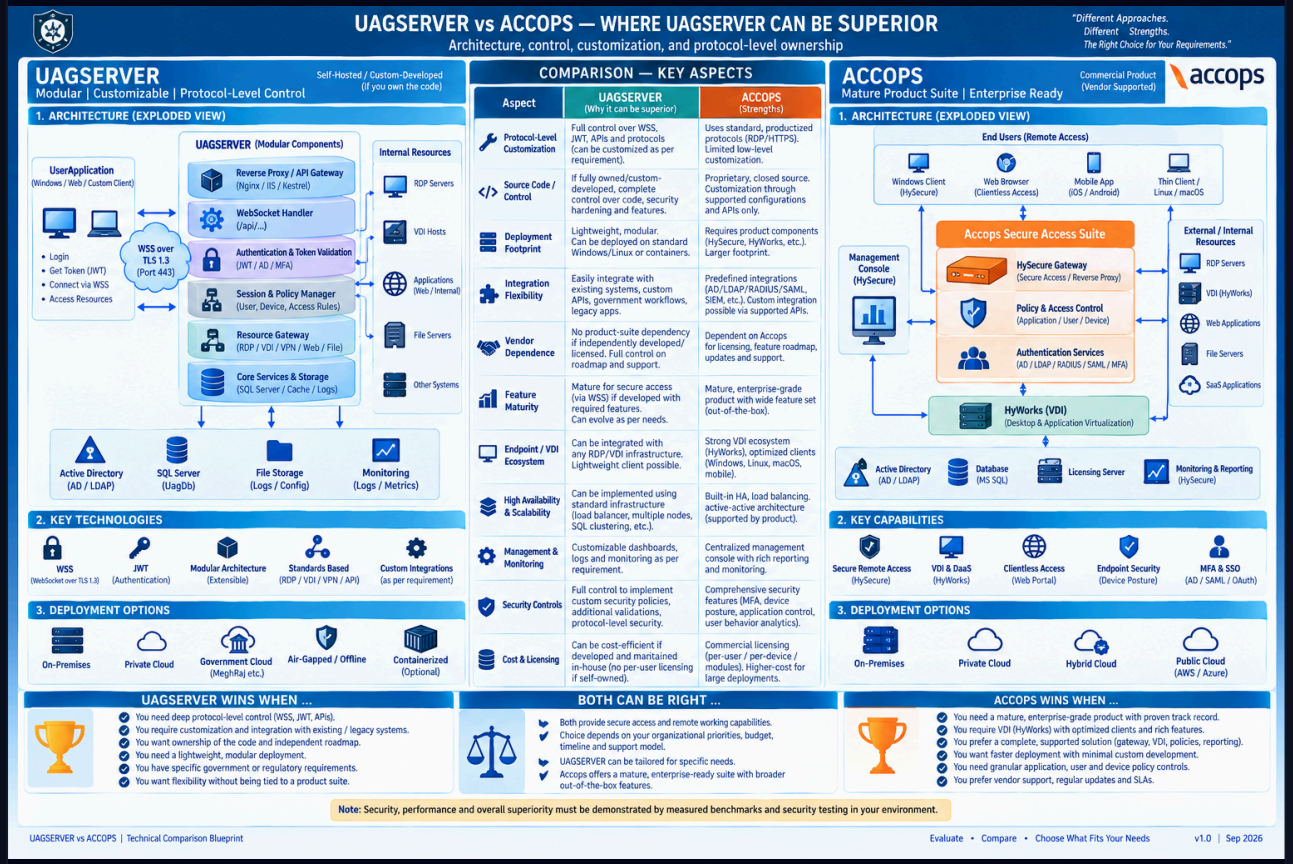
TECHNICAL SPECIFICATIONS

Primary Focus	UAG: Focused Gateway & Protocol Tunnel | Accops: End-to-End VDI Product Suite
Virtualization	UAG: Connects to existing infrastructure | Accops: Built-in HyWorks VDI & App broker
Identity & MFA	UAG: Active Directory + JWT + Custom MFA | Accops: HyID / BioAuth with Biometrics
Endpoint Control	UAG: Lightweight native/web client | Accops: HyLite client, device posture & DLP
Licensing Model	UAG: Self-owned, zero per-user license | Accops: Commercial subscription / perpetual per-user

KEY ARCHITECTURAL HIGHLIGHTS

- UAGServer excels when organizations seek total code ownership, protocol control, and cost predictability.
- Accops excels when turnkey commercial vendor support, pre-packaged VDI brokers, and DLP are mandated.
- Both platforms achieve secure remote access but cater to fundamentally different organizational models.

```
Key Takeaway: 'UAGServer = Tailored protocol gateway with zero license ov
erhead. Accops = Broad commercial workspace suite.'
```



Click to Full Screen

Blueprint 13: 11-Point Competitive Superiority Matrix & Strategic Decision Framework

1536 × 1024 Native HD

ARCHITECTURAL SUMMARY

An exhaustive 11-aspect evaluation detailing where UAGServer provides superior autonomy, lower total cost of ownership, and protocol-level customization compared to commercial off-the-shelf alternatives.

TECHNICAL SPECIFICATIONS

Protocol Control	Full ownership over WSS, JWT, and custom API routes vs fixed vendor protocols
Source Code	100% auditable and customizable in-house vs closed-source proprietary vendor binaries
Footprint	Lightweight, deployable on standard OS or containers vs multi-VM appliance footprint
Integration	Directly binds to custom legacy systems and government workflows without vendor middleware
Cost / Licensing	Zero per-user or per-device recurring subscription costs — massive long-term TCO savings

KEY ARCHITECTURAL HIGHLIGHTS

- UAGServer Wins When: You require code ownership, independent roadmap, air-gapped/gov cloud deployment.
- Accops Wins When: You need turnkey vendor SLAs, out-of-the-box VDI management, and minimal in-house development.
- Decision Matrix: Both can be right depending on budget, timeline, compliance mandates, and engineering capability.

```
Strategic Recommendation: 'For government and high-security enterprise environments, UAGServer provides total sovereign control.'
```

PRODUCTION SECURITY & COMPLIANCE BASELINE

The following cryptographic and architectural controls are validated for production deployment across all UAGServer gateway nodes:

CONTROL AREA	IMPLEMENTATION STANDARD	STATUS
TLS 1.3 Enforcement	Enforce TLS 1.3 exclusively; disable legacy TLS 1.0/1.1 and insecure CBC ciphers.	VERIFIED
HSTS & Certificate Chain	HTTP Strict Transport Security (HSTS) with max-age=31536000 and valid CA chain.	VERIFIED
Ephemeral Key Exchange	Mandatory ECDHE over NIST P-256 for perfect forward secrecy.	VERIFIED
Cryptographic Tokens	Short-lived JWT (15-min expiry) with asymmetric ECDSA signature verification.	VERIFIED
Least Privilege Access	Zero direct public exposure for internal ports 3389, 1433, 389, or 445.	VERIFIED
Auditing & Log Ingestion	Tamper-resistant audit trail in SQL Server UagDb with automated SIEM forwarding.	VERIFIED

```
Baseline Policy: Zero Trust Architecture (NIST SP 800-207) with continuous token assertion and strict perim
eter isolation.
```

STRATEGIC RECOMMENDATIONS

- Deploy UAGServer in an active-active clustered topology behind an enterprise hardware load balancer.
- Implement multi-region database replication for SQL Server UagDb to guarantee sub-second disaster recovery failover.
- Establish automated certificate lifecycle renewal via ACME / enterprise CA with OCSP stapling enabled.

FINAL ARCHITECTURE SIGN-OFF

UAGServer establishes an ultra-secure, highly performant, and cost-effective remote access gateway. By eliminating third-party licensing dependencies and leveraging modern standards (TLS 1.3, WebSocket WSS, and ECDHE cryptography), the platform delivers sovereign enterprise access ready for government and mission-critical cloud deployments.

APPROVAL STATUS: ARCHITECTURALLY CERTIFIED

Reviewed and approved by Technical Architecture & Security Committee — September 2026.