

CYBERRAVE VOICE AUTHENTICATION SYSTEM

Abstract

The Voice Authentication System (VAS) is designed to integrate with standards-built network architectures that authenticate users and protect access to critical data resources using discreet voice authentication services for authorized parties. It establishes a practical voice biometric defense layer, and human-to-computer interface needed to connect people, policies, and compliance controls. It integrates with existing technology investments and can provide defense-in-depth through “trusted third party” provider networks.

Description

VAS incorporates COMMON NAMING schemes to underpin scripting LANGUAGE HANDLERS that connect PRIVACY POLICIES to DIGITAL CERTIFICATE controls. The combinations of TECHNOLOGY & PROCESSES establish a VOICE AUTHENTICATION SYSTEM with advanced INTELLIGENCE CAPABILITIES that scale using GLOBAL STANDARDS.

- **Common Naming** is established to achieve strategic ends. Names are at the root of all communications, whereas any human-to-computer effort to achieve ontological goals should associate a cognitive reference model that is relevant. Industry-specific keywords and phrases frame language variables that extend namespace rules. Taxonomically engineered domains that use sector-specific dictionaries can achieve context and realize control elements for rudimentary terms.
- **Language Handlers** create technology “hooks” needed for provisioning and traffic shaping. Lexical keywords and phrases possess inherent syntax variables that can be used for mapping connection instructions to virtual file systems and IT resources. Voice language technology can be used to model business processes using semantic links that associate policies and clearly defined operational outcomes.
- **Privacy Policies** protect and guarantee service for subscribers. The public Internet creates new assumptions and responsibilities when obtaining access permission to controlled, private network environments. Written, spoken and digital promises assure risk controls and protect personal preferences and settings using specific classes of coverage. The quality expectation of subscription service translates to tolerances that arise locally or globally for a given domain.
- **Digital Certificates** safeguard packet payloads and increase data value. Certificate Authorities provide validation services for user authentications. The integrity of data transmitted can be enforced using transparent encapsulation methods to protect packet contents. Enforcement over data lifecycle further benefits those certificates with instructions that point to accounting and reporting services.

- **Technology & Processes** establish trust mechanisms. Converging fixed-to-mobile technologies enable anywhere, anytime remote access to data networks. A logical link structure and advanced AAA capabilities support Interactive Voice Recognition and analytic services. Encrypted keys and layered permission schemes unlock service directories programmed to navigate proxy servers using discreet transportation protocols that report and adapt policy-defined events.
- **Voice Authentication Systems** simplify hands-free access for user groups that use a virtual interface. Web-based service subscription provides an authorization platform needed by people, devices and network connectors. Permission statements provided at registration define directory controls and policy coverage. Peering agreements with Virtual Network Operators, Managed Security Service Providers, long haul and last-mile carriers establish a hub-and-spoke trust framework. Certified vendors strengthen the network infrastructure with service guarantees that include non-repudiation and event resolution.
- **Intelligence Capabilities** establish knowledge superiority. Policy information and subscription characteristics provide evidence that is helpful to law enforcement when situations warrant. Abstract metadata helps define threats and vulnerabilities, especially where data context exists. Information Lifecycle Management collaboration between human and computer resources produces patterns that predictive analytics can capture through trend modeling and simulation of characteristic data. Related knowledge is managed and distributed through training and human resource education programs.
- **Global Standards** assure future-proof solutions. Common criteria in informatics helps provide cost efficiencies and scalable solutions for very large network environments. Data security achieves maximum benefit when standards are strategically aligned. Important considerations include compliance issues that surround sensitive data including its collection, management, accountability, transparency, and survivability. Universal protocols are designed to increase security and safeguard user group privacy.

Conclusion

Scalable Voice Authentication Systems must associate namespace fundamentals inherent to voice communications and data security. The public trust depends on creative solutions that incorporate marketing, technology and business process together to achieve strategic goals. Evolving common criteria use keyword naming and industry taxonomies to frame domains of interest. Advanced intelligence capabilities exist within managed private networks having Voice Authentication Systems that connect common names, language handlers and privacy policies. Global voice standards can propel security and privacy towards safe and resilient networks.