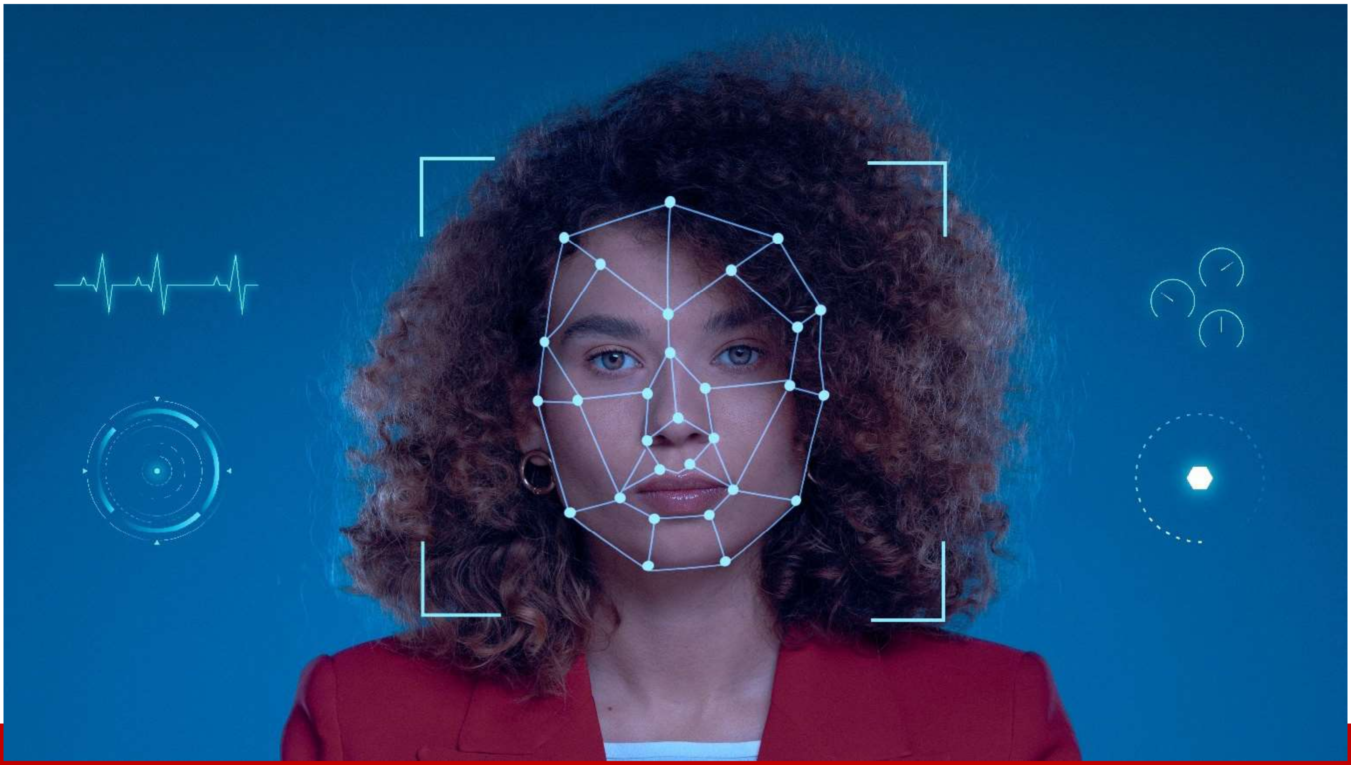

NextGen Identity Management

How to Harness Government Standards and Tech Innovations

By Dr. Sarbari Gupta, Founder and CEO, Electrosoft Services, Inc.

Federal agencies face a pivotal cybersecurity challenge: prevent unauthorized entities from accessing systems and facilities, while granting authorized federal employees and contractors access commensurate with verified need. Two factors complicate this objective: (1) relentless efforts by ever-more-sophisticated cybercriminals and (2) myriad agency systems, many antiquated with ill-defined interfaces that rely on outdated defense mechanisms.

Digital modernization and migration to the cloud comprise important responses. Additionally, technological advancements, combined with federal identity, credential, and access management (ICAM) standards and guidelines, offer federal agencies robust identity management tools.

ICAM Meets Zero Trust

Traditional federal authentication and access control mechanisms relied on perimeter-based trust. Here, users authenticate their identity at the network entry point. Thereafter, the roles assigned to that identity govern further access.

Office of Management and Budget Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, inaugurated a shift to a zero trust architecture (ZTA). Here, trust is not accorded to any person, non-person entity, system, or network—whether within or beyond the security perimeter. ZTA emphasizes enterprise-level controls, especially phishing-resistant multifactor authentication.

Demand for robust ICAM solutions, complemented by the right mix of standards and policies, is the result. Standards and innovation are the watchwords on our NextGen journey.

Key Identity Standards Guiding Federal Implementations

The three most important identity management standards for federal agency adoption are:

1. **NIST Special Publication 800-63**. The four-volume publication Digital Identity Guidelines forms the cornerstone of federal identity management. It prescribes the technical requirements for implementing digital identity in federal agencies and offers processes for risk assessment, assurance level selection, and appropriate controls.

   This document combines the best thinking of public and private information security professionals and offers both worlds a risk-based approach to digital identity management. Important enhancements include the infusion of an updated digital identity model, greater process orientation in risk management, and a revised assurance level selection methodology.

2. **Federal Information Processing Standards 201**. FIPS 201 implements the requirements of Homeland Security Presidential Directive 12 relative to Personal Identity Verification (PIV) of federal employees and contractors. It addresses logical and physical access applications with special focus on smart card–based identity credentials.

   This mandatory standard, issued by NIST, defines the technical specifications and operational requirements for creating, issuing, and managing PIV credentials, which include smart cards used for accessing federal facilities and information systems.

3. **X.509v3.** X.509v3 is the international standard for issuing and managing PKI identity credentials. PKI facilitates the secure electronic transfer of information by using digital certificates and cryptographic key pairs.

   The combination of digital certificates and key pairs based on asymmetric cryptography establishes the trust ZTA requires – sender (user and device) authentication, content authentication (secure data transmission), and non-repudiation.

Emerging Innovations

Continuous innovation is a feature of the identity management space. While there are far too many advances to cover, every federal ICAM leader should be aware of these technologies:

- **AI.** Artificial intelligence already plays a role in identity and access management, performing a range of critical tasks without human intervention. By all predictions, future applications — especially those relying on generative AI and machine learning — will transform the identity and access management world.

AI offers many benefits. For example, faster pattern recognition can quickly trigger automatic network-protecting measures. On the other hand, AI in the wrong hands – or applied with evil intent – can create threats beyond imagination.

- **Fast Identity Online (FIDO)**. Developed by the FIDO Alliance, FIDO is an industry standard for strong, easy-to-use asymmetric cryptography-based identity credentials that are available across popular operating system platforms and browsers.

  Derived PIV Passkeys (DPPs) – FIDO2 credentials implemented as derived PIV credentials in accordance with FIPS 201 and NIST Special Publication 800-157r1 – are user-friendly, multifactor, and phishing-resistant authenticators that can be used by federal enterprise users. I recently proposed an authentication model using DPPs for authentication to federal online services. It could represent a leap into modern authentication.

- **Attribute-based access control.** ABAC is a versatile approach for dynamically managing access. Access decisions compare real-time attributes with those assigned to the user, the resource, and the environment and digital policies governing the same.

  Many postulate an either-or proposition when it comes to ABAC and role-based access control models. I tend to agree with OMB M-22-09, which suggests that using the two in conjunction offers greater assurance than either model individually.

- **Identity governance and administration (IGA) tools**. Enterprise-level tools that manage digital identities across their lifecycle and control user access across the digital ecosystem via data aggregation and correlation.

  Complex digital ecosystems – on-site, cloud, and hybrid – make tracking and reporting on the activities of multiple users, devices, and access requirements across differing environments a manual nightmare. IGA tools apply automation to make risk management and regulatory compliance manageable.

Limitless possibilities attend ZTA implementation. What an exciting time to be part of the federal identity, credential, and access management landscape!

About the Author

Dr. Sarbari Gupta is the Founder and CEO of Electrosoft Services, Inc. She is a recognized thought leader and speaker on cybersecurity, zero trust, ransomware, ICAM, FIDO passkeys, OSCAL and more. She is an active NIST collaborator and co-author, helping to shape cybersecurity standards and guidelines to improve federal cyber resilience. 2022 was a banner year for Electrosoft, with record revenue and 25% Y/Y growth – and the company is on track for 60% growth in 2023. Dr. Gupta is passionate about STEM education and encouraging women to embrace and stay in STEM fields. She serves as a mentor for Women in Technology (WIT) and is a member of the board of advisors for University of Maryland Women in Engineering (WIE), providing support and mentoring to women entering an engineering field.

Dr. Gupta can be reached online via LinkedIn and at our company website https://electrosoft-inc.com/