eA3 Case Study
Modernizing Identity at the Front Door of the IRS

Makpar

The IRS relies on **eA3** as its enterprise Identity, Credential, and Access Management foundation. Through eA3, Makpar supports secure access for more than **60 million registered users**, protecting taxpayer data while enabling fast, reliable access to critical services.

The Challenge: Identity at National Scale

As digital services expanded, the IRS faced growing pressure to:

- Support a rapidly increasing taxpayer and practitioner population
- Expand its online services portfolio to business entities
- Maintain strong identity assurance and fraud protection
- Deliver consistent access and user experience across dozens of applications
- Maintain high availability during peak filing periods
- Secure access across a growing mix of legacy and modern systems
- Modernize without disrupting mission critical services

DHS and CISA guidance reinforce identity as the primary security perimeter, requiring phishing resistant authentication and enterprise visibility to protect taxpayer trust.

The Makpar Approach: Engineering Identity for Scale, Security, and Resilience

Makpar engineers eA3 as a unified, high availability identity management framework that supports both legacy and modern IRS systems. Embedded automation and governance enable secure updates at speed while preparing the IRS for future modernization.

Solutions Powering eA3: Built for Mission Scale and Operational Reliability

Identity & Access Management

- Secure digital identity at national scale
- Precise, role based access controls
- Federated identity services

DevSecOps, Automation, and Governance

- Identity governance embedded into CI/CD pipelines
- Automated testing and infrastructure as code
- Continuous compliance with federal security and identity standards

Unified API Access Layer

- Single, governed API layer
- Simplified, standards based integration
- Consistent identity, credential, & authorization

Phishing Resistant MFA and Behavioral Analytics

- Hardware backed, phishing resistant MFA
- Behavioral analytics and aggregated logging
- Early detection of anomalous access and fraud signals

Makpar

Monitoring & Analytics

- Real time monitoring of identity, access, & performance
- Fraud detection and anomaly analysis
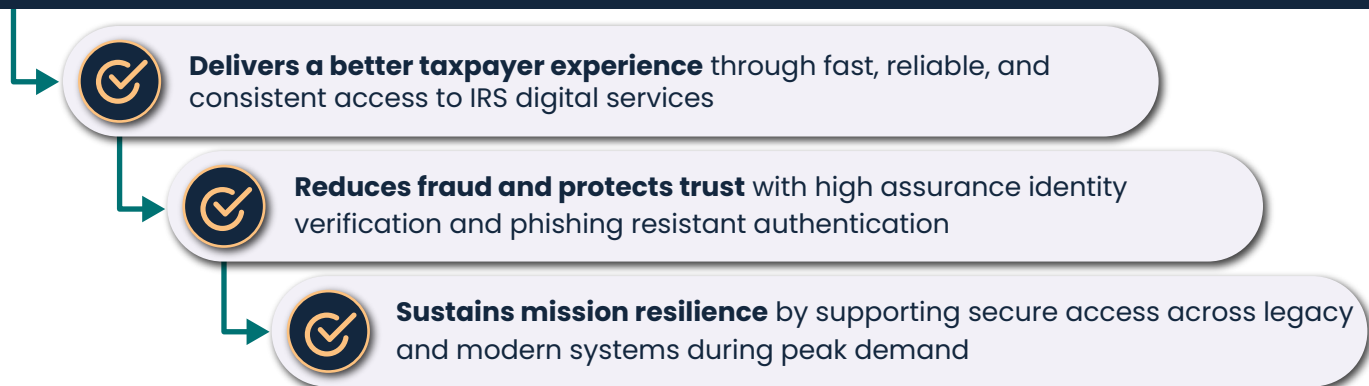- Operational visibility during peak demand

Legacy System Integration

- Brokered and federated integration models
- Support for user to machine and machine to machine access
- Modernization without disruptive rewrites

The Impact: Lower Costs. Seamless Access. Trusted Digital Services.

Through eA3, the IRS has achieved:

- **Fast, reliable access** for tens of millions of taxpayers and practitioners
- **Consistent performance at national scale**, including peak filing periods
- **Simpler, more consistent authentication** across IRS digital services

- **Stronger fraud prevention** through high assurance identity controls
- **Lower cost service delivery**, with digital transactions costing cents instead of hundreds of dollars
- **A future ready identity foundation** supporting unified API access and new digital services

Why It Matters: Identity Enables Trust

Delivers a better taxpayer experience through fast, reliable, and consistent access to IRS digital services

Reduces fraud and protects trust with high assurance identity verification and phishing resistant authentication

Sustains mission resilience by supporting secure access across legacy and modern systems during peak demand

ICAM: Zero Trust

Control Plane:
Standards Based Identity and Zero Trust Policy Enforcement

Policy Decision Point

Policy Engine

Policy Administrator

CDM System

Industry Compliance

Threat Intelligence

Activity Logs

Subject → System — Untrusted → Policy Enforcement Point — Trusted → Enterprise Resource

Data Access Policy

PKI

ID Management

SIEM System

Data Plane:
Federated Access Across Legacy and Modern Systems

Makpar