

Microsoft 2024 Identity Partner of the Year Nomination – Government Case Review

Overview

The client is a public sector ministry with 100,000 internal identities and 5M citizens. For years, they have been seen as a global leader in digital ID with their innovative Citizen Card and emerging capabilities in Self-sovereign decentralized identity through Verifiable Credentials. The Office of the CIO (OCIO) within the Ministry of Citizen Services is responsible for all these identity types and has partnered with N8 Identity to push forward on multiple fronts on their journey towards Zero Trust.

After successfully enrolling 80,000 internal identities to use MFA with the Authenticator app, they turned their attention to external identities. N8 Identity led the OCIO to define a roadmap and execute a multi-year phased rollout strategy.

Background

The demand for collaboration exploded through the Covid pandemic and organizations were often forced to accelerate plans for how their workforce could access resources securely from remote locations and non-corporate devices. Microsoft made the ability to invite partners and other external collaborators extremely simple, and as a result the proliferation of Guest Accounts continued for an extended period with limited compensating controls.

With 30,000 external identities now in the tenant (and growing at a rate of 1,000 per month), the focus turned to exploring, validating, and implementing new methods to restore a balance of governance against the convenience that had fuelled this explosion.

To achieve this, N8 Identity is enabling multiple capabilities across External Identities, including other methods of collaboration that have been grouped under this evolving program. Our 3-phase process includes POCs in non-prod tenants, pilots in production tenant with presentations to architecture review boards, and operationalization into a new enterprise service.

Guest Account Lifecycle Management

With a focus on getting Guest Accounts under control, N8 Identity is utilizing 5 different approaches:

Access Packages – 20,000 SharePoint 2016 sites have been modernized to Teams/SharePoint Online. This has created an increased demand on Guest Accounts due to more than 300,000 legacy accounts previously used which are no longer an option for accessing M365 services. N8 Identity has focused on critical Access Packages scenarios that have enabled thousands of users across diverse populations such as law enforcement, international consulates, privileged citizens, and other ministries to gain access to M365 services in a secure and convenient manner with improved controls:

- Outbound Requests – authorized Access Package Managers can add users, triggering an outbound invitation
- Inbound Requests – allow external users to initiate requests for an Access Package with a variety of approval scenarios (e.g. approved by Sponsor at home tenant, auto approval based on “whitelist” of domains)
- Proactive Compliance – Access Reviews on every Access Package, and the option for time-based access that auto-expires

Direct Managed Guest Accounts – in anticipation of this increased demand for Guest Accounts, N8 Identity designed a proven bulk migration offering (including create and assign) to minimize friction of the transition. These approaches are ultimately expected to limit or eliminate invitations initiated from within M365 services (Teams, SPO, Power Platform, Viva Engage, etc.) in order to streamline the adoption and uptake

Access Reviews – beyond Access Reviews triggered by Access Packages, N8 Identity also created additional recurring campaigns to clean up Guest Accounts that have accumulated unchecked. This will force a self-service review for any users that have not logged in for more than 1 year, the first wave purged over 5,000 “stale” Guest Accounts

Tenant Sync – due to the tightly coupled relationship between different public sector ministries, N8 Identity has conducted POCs to provide alternate methods of Guest Account management using this function that will allow for accelerated and simplified collaboration across public sector entities

Hybrid External Identities - over the last 20+ years, thousands of users from other agencies and contractors have been issued traditional on-prem AD Accounts to access apps and resources. These “external” users often have their existing, non-gov email addresses “over-written” on their account, and they increasingly need access to both traditional, on-prem applications and M365 services. However, inviting a Guest Account creates conflicts with these existing IDs due to the email value which has forced multiple unpleasant workarounds that are costly and confusing for end users (additional licenses, multiple logins, etc.)

N8 Identity has created an innovative new process to validate and convert users that preserves the existing legacy ID which thousands of apps still depend on, while allowing a Guest Account to also exist as an External ID on a single object in Entra. Not only does this enable the user to have the best of both worlds in terms of how they log in, but it also positions the client to transition thousands of these users to a “true” Guest Account and optimize significant license costs in the process.

Other External Collaboration

N8 Identity has also enabled 4 additional patterns for collaboration that will further enhance the client’s ability to provide secure access to resources for citizens and workers:

Multi Tenant Apps – N8 Identity identified an emerging pattern for large populations of users that required access to secure apps and resources where a Guest Account is unnecessary. A pilot has moved into production which allows 5,000 users across 60 school districts to access custom developed apps using the credentials from their home tenants without the need to create or maintain any other identities. Going forward, N8 Identity is defining a robust intake process to streamline onboarding and help clean up the hundreds of rogue applications that have proliferated within the tenant

B2C – although the client has one of the most trusted Digital IDs in the world, there are many use cases where a lower assurance identity is sufficient for lower friction transactions. N8 Identity has configured a B2C POC instance to illustrate these capabilities and have begun defining an intake process to leverage this, allowing for rapid adoption and simplified access for millions of citizens to key government services across transportation and recreation ministries

Calendar Sharing – in addition to accessing documents and applications, many user populations require visibility to other user’s calendars and rooms. This had been done ad-hoc with legacy on prem Exchange, but with the migration to Exchange Online, the methods for this collaboration are also changing. N8 Identity successfully designed and executed a POC to provide cross-visibility of eligible users and rooms

Shared Teams Channels – after a successful POC, this capability has proven to be an intriguing option in place of Guest Accounts for highly trusted external partners across both public and private sectors. Adoption is continued to expand as another effective tool to simplify the adoption of M365 services

Summary

In addition to these workstreams, N8 Identity is leading other parallel initiatives to modernize applications to use Entra as their authentication source and unlock the power of Conditional Access and MFA, while also shifting the management of 150,000 Groups to Entra and enable a new Employee Verifiable Credential pilot.

N8 Identity has been honoured to work with the OCIO to lead them on this challenging and exciting journey and look forward to continuing to push the adoption and maturation of these offerings in the coming years.

Customer Testimonial

“My team and I are thrilled and feel very fortunate to be collaborating with N8 Identity, who’s expertise and structured delivery approach has been vital in helping us capitalize on new opportunities through a measured and well-informed methodology that has given us confidence every step of the way as we forge this new future together.”

Director of Authentication & Directory Management Services