Introduction to SPIDER

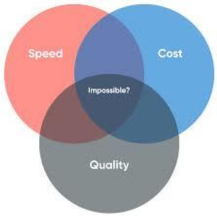
After more than 20 years of experience accumulated through numerous IAM (IGA) projects, OPNS observed that, in most cases, customers struggle to cover 100% of the scope in user provisioning.

In some extreme situations, an IAM project deploys an initial set of provisioning interfaces (connectors) for let's say 5 applications, and then nothing happens for months or years, meaning that only a little percentage of business applications are effectively managed through IAM…

This has multiple negative consequences as:

- A parallel process exists in the organization so people can request/approve accounts and access rights on applications that are not in IAM scope.
- Any effort to build an enterprise role catalogue, with business-level roles, can't deliver a satisfactory result when too many applications are left out of scope.
- Effective security controls and/or security measures as, for example, a simple "disable" of a user, can't be implemented in one central place, rather requiring multiple actions in multiple places.

The main reason for this situation is the lack of time & money: it takes too much effort to integrate 100% of the application scope into the IAM provisioning. The budget and time allocated to the initial project did demonstrate the feasibility, but further expansion to all IT sub-systems never happens…



To solve this OPNS developed SPIDER*, enabling simple, fast & efficient integration of any application or system into the provisioning scope.

With SPIDER anyone can expand their NetIQ provisioning layer to hundreds of applications in just a few days!

You can now benefit from all your NetIQ IDM processes (request/approval self-service for Roles & Resources, full RBAC-compliant role catalogue, standard & custom workflows, all unchanged) and propagate associated provisioning instructions to any system or application.

No one need to know if actions are either fully automated through a native provisioning connector or partially automated through SPIDER; from a business user standpoint this is 100% transparent: they can request/approve accounts and access rights for any application without even knowing if it will ultimately be handled through a native connector or through SPIDER. From an IT standpoint the only difference is that a native connector provides full automation while SPIDER will translate a provisioning action into a 'Task' and forward that Task for processing by:

- the appropriate administrator (manual action; he knows how to do it!), or
- your ticketing (ITSM) solution, which then forwards to the administrator, or
- to a robot, which receives enough information to perform the task (full automation), or
- to our universal REST tool, to execute REST calls to any available API (full automation).

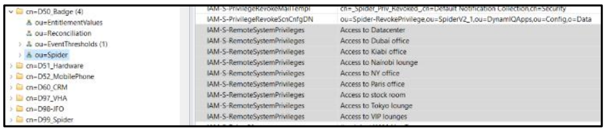
It's so smart some organizations use SPIDER for >90% of applications!

* SPIDER = **S**olution for **P**rovisioning of **I**dentities in **D**isconnected **E**nd-point **R**esources

Basically, adding SPIDER to your existing NetIQ IDM environment is as simple as deploying the SPIDER driver and, optionally, its associated front-end; that's it!

> *Note: using SPIDER front-end is optional but handy in case you don't want (or have no time) to pass the Tasks through your existing ticketing (ITSM) system or automate the Task (through a robot or a REST API call). In such situations the Tasks are displayed in SPIDER front-end sitting right in NetIQ portal (UA / Identity Apps). Obviously default front-end configurations are provided for the main transactions: Create an account, enable/disable an account, grant a permission to an account, revoke a permission to an account. Using these default configurations enables you to use SPIDER right out-of-the-box. SPIDER front-end is based on OPNS DynamIQ-Apps®, our no-code framework to ease the build of customized front-end without the need to code anything; this framework is available on its own in our solution catalog and is often used to expose business-friendly 'Tiles' in the NetIQ portal for transactions like 'Create User', 'Activate User' and many other user-lifecycle processes.*

Once SPIDER is deployed you can define applications through simple declarations in eDirectory, and this is done in minutes, maximum an hour. Each new application is defined its container (OU) where you define characteristics like application name, email address to use to notify about new Tasks, what is the list of Permissions (or Access Rights) that exists on that application and (optional) which DynamIQ-Apps® configuration to use for the front-end.

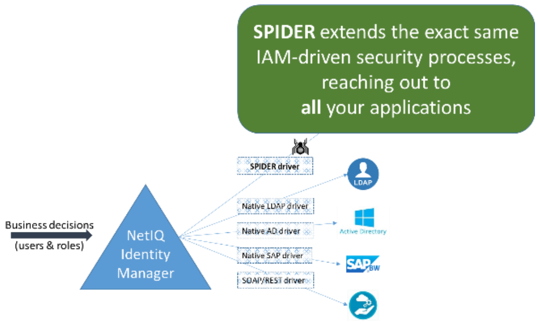


cn=D50_Badge (4)
ou=EntitlementValues
ou=Reconciliation
ou=EventThresholds (1)
ou=Spider
cn=D51_Hardware
cn=D52_MobilePhone
cn=D60_CRM
cn=D97_VHA
cn=D98-JFO
cn=D99_Spider

IAM-S-PrivilegeRevokeMailTempl	cn=_Spider_Priv_Revoked_,cn=Default Notification Collection,cn=Security
IAM-S-PrivilegeRevokeScnCnfgDN	ou=Spider-RevokePrivilege,ou=SpiderV2_1,ou=DynamIQApps,ou=Config,o=Data
IAM-S-RemoteSystemPrivileges	Access to Datacenter
IAM-S-RemoteSystemPrivileges	Access to Dubai office
IAM-S-RemoteSystemPrivileges	Access to Kiabi office
IAM-S-RemoteSystemPrivileges	Access to Nairobi lounge
IAM-S-RemoteSystemPrivileges	Access to NY office
IAM-S-RemoteSystemPrivileges	Access to Paris office
IAM-S-RemoteSystemPrivileges	Access to stock room
IAM-S-RemoteSystemPrivileges	Access to Tokyo lounge
IAM-S-RemoteSystemPrivileges	Access to VIP lounges

SPIDER driver icon: SPIDER

Once your application is defined in SPIDER it fully participates in your NetIQ IDM environment, exposing entitlements to create Resources (possibly linked to Roles), and generating 'Tasks' for each provisioning event triggered by any upper-level process. Basically, SPIDER extends your IDM platform to any application!


SPIDER extends the exact same IAM-driven security processes, reaching out to **all** your applications

SPIDER most appreciated use-cases are:

- Bridge IDM provisioning with any application or system for which automated provisioning isn't relevant (for example when there is not so many transactions per month → cost of automation is higher than labor cost)
- Quickly add IT services to the organization role-model (RBAC), so associated provisioning tasks do follow the Role(s) granted to a User (for example: grant an *upgraded mobile phone subscription* to Sales and Managers → Task for the relevant staff managing mobile phone subscriptions)
- Use SPIDER as an easy way to add email notifications; for example, add a SPIDER Resource to an existing Role → when a User is granted/revoked that role SPIDER sends a mail; no code change on your existing IDM drivers.
- Efficiently integrate all applications in the IDM provisioning scope, possibly as an interim solution waiting for full automation to come → immediately benefit from all advantages at process level, RBAC level and many more. Only the 'last mile' is still manual, possibly automated later.
- Initially control an application through SPIDER to have human supervision in the provisioning process and, once validated, move to full automation mode through deployment of a native connector.

SPIDER is part of ***Mir.IAM***, our overarching framework for a maturity level 5 IAM, and is available separately as a product to enrich your NetIQ solution; contact us for details.