SYMBEEO

PUBLIC

DESIGN STUDY

Cloud network as code for a public agency on AWS and Azure, state encrypted under the agency's keys

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Automation	Public Sector	National agency
DOCUMENT	**VERSION**	**DATE**
AUT-005	1.1	Oct 10, 2026

WRITTEN BY

Mark Winston, Principal Network Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	AUT-005	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Automation	Industry	Public Sector
Author	Mark Winston	Role	Principal Network Architect
Credentials	CCIE, CISSP, CCSP, CCISO, CISM, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's, project's or standards body's own current page on Sep 24, 2026 · [S*] figure from the page's published summary where the page itself could not be opened · [A] design assumption, to be confirmed by the signing engineer · [T] design target: the record's outcome figure and anything derived from it. No figure comes from any engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. Mark Winston remains the author.

1 · Scope

Who it is for. The cloud platform lead of a public agency whose cloud networks were built in two consoles by a small team, whose auditors found network changes with no change record, and whose data rules require that anything holding network secrets is encrypted under keys the agency controls.

Typical buyer [A]. A national agency with 40 AWS accounts and 12 Microsoft Azure subscriptions, two regions in each cloud. One hub network per cloud and region and 52 spoke networks — one per account or subscription — about 3,000 network resources in all: networks, subnets, route tables, gateway attachments, security groups, network security groups and private DNS zones. Five cloud engineers. An existing Git service with CI runners inside the agency.

What is in. The code layout; the state backends and their encryption; the pipeline from merge request to apply; the pre-apply model check; the identity the pipeline uses in each cloud; drift reporting; provenance and audit. **What is out.** The landing-zone design itself (account structure, organization policies); workload infrastructure; on-premises connectivity; the Git service.

Assumptions. OpenTofu is the infrastructure-as-code engine, chosen under the agency's open-source licensing policy [A]. Each cloud's key service holds the agency's state-encryption keys [A]. The agency's records rules keep audit evidence seven years [A]. Every existing network resource can be imported into state without being recreated [A].

Related documents, read Sep 24, 2026.

- SRA-AUT-001, Symbeeo reference architecture for infrastructure automation (the pattern this design applies)
- OpenTofu 1.12.0 release — `https://opentofu.org/blog/opentofu-1-12-0/`
- OpenTofu releases (GitHub) — `https://github.com/opentofu/opentofu/releases`
- OpenTofu state and plan encryption — `https://opentofu.org/docs/language/state/encryption/`
- CNCF project page, OpenTofu — `https://www.cncf.io/projects/opentofu/`
- OpenTofu s3 backend, read Sep 27, 2026 — `https://opentofu.org/docs/language/settings/backends/s3/`
- Batfish releases — `https://github.com/batfish/batfish/releases`
- Batfish supported devices — `https://batfish.readthedocs.io/en/latest/supported_devices.html`
- SLSA specification v1.2 — `https://slsa.dev/spec/`

© 2026 Symbeeo. All rights reserved. · Public

1c · Public implementations this design follows

Each row is labeled. **Public deployment**: a named operator's real deployment, published and dated by the operator, its vendor or a partner, used where one exists. **Our own design**: the dated vendor or standards documentation this design was built from, where no public deployment of the design exists. Labels and dates checked Sep 27, 2026.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Public deployment. A national defense department: Terraform and Vault run as shared services for teams working across AWS, Azure and Google Cloud	HashiCorp case study (conference talk) · Oct 7, 2019	§4.1 and §4.5: a public-sector body runs one infrastructure-as-code engine across more than one cloud from a shared service. It predates OpenTofu and is not network-specific, so it settles the operating model only; no figure from it enters the register	`https://www.hashicorp.com/en/resources/adopting-shared-services-terraform-and-vault-at-the-us-dept-of-defense`
Our own design, built from published documentation. OpenTofu 1.10.0: the `s3` backend can lock state without DynamoDB, with a lock file in the state bucket (`use_lockfile`); DynamoDB locking remains fully supported in OpenTofu, while Terraform deprecated it in 1.11.0 (Feb 27, 2025)	OpenTofu project · 1.10.0 released Jun 24, 2025; backend page for 1.12.x read Sep 27, 2026	R12 and §4.2: one S3 lock file per stack, no DynamoDB lock table; the same setting works on Terraform 1.11 or later if the comparison chooses it	`https://github.com/opentofu/opentofu/blob/v1.10/CHANGELOG.md` · `https://opentofu.org/docs/language/settings/backends/s3/` · `https://github.com/hashicorp/terraform/blob/v1.11/CHANGELOG.md`
Our own design, built from published documentation. OpenTofu state and plan encryption at rest, AES-GCM, with AWS KMS, GCP KMS, Azure Key Vault, OpenBao or PBKDF2 key providers	OpenTofu project documentation for 1.12.x · 1.12.0 released May 14, 2026	R4: client-side state encryption under the agency's own keys is an engine feature, not a wrapper	`https://opentofu.org/docs/language/state/encryption/`

Locking uses the S3 backend's own lock file, native in OpenTofu since 1.10.0, not a DynamoDB lock table [S]. Runs are triggered from merge events only, so no long-lived token exists (R5).

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Estate	40 AWS accounts · 12 Azure subscriptions · 2 regions each · ≈ 3,000 network resources	[A]
R2	Every network resource declared in code	100 %; zero console-created network resources found by the nightly scan	[T]
R3	Every plan reviewed in a merge request	author ≠ reviewer; plan output attached	[T]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R4	State and plan files encrypted at rest under the agency's keys	AES-GCM; AWS KMS and Azure Key Vault key providers	[S] OpenTofu state encryption
R5	No long-lived cloud credential in the pipeline	OIDC role assumption per run	[T]; mechanism [A], confirmed per cloud at design
R6	Model check before apply, AWS	security-group and routing questions answered on the planned state	[S] Batfish models AWS constructs; [T]
R7	Accidental destroy blocked in production	`prevent_destroy` set per environment	[S] OpenTofu 1.12 dynamic `prevent_destroy`
R8	Provider integrity	checksums for all platforms recorded at `tofu init`	[S] OpenTofu 1.12
R9	Provenance of every applied artifact	SLSA Build L2 minimum	[S] SLSA v1.2 (via SRA-AUT-001); [T] level
R10	Drift	scheduled plan per stack; non-empty plan reported ≤ 1 h	[T]
R11	Rollback, one stack	revert commit and apply ≤ 30 min	[T]
R12	State locking	one state and one lock per stack, stored in the stack's own account or subscription; on AWS an S3 lock file (`use_lockfile`), no DynamoDB table	[S] OpenTofu `s3` backend, 1.10 and later; [A] per region and Azure equivalent
R13	Audit retention	pipeline runs and cloud control-plane logs, 7 years	[A]

Thirteen rows; six carry a vendor, project or standards figure, three are design assumptions, four are design targets.

3 · Architecture overview

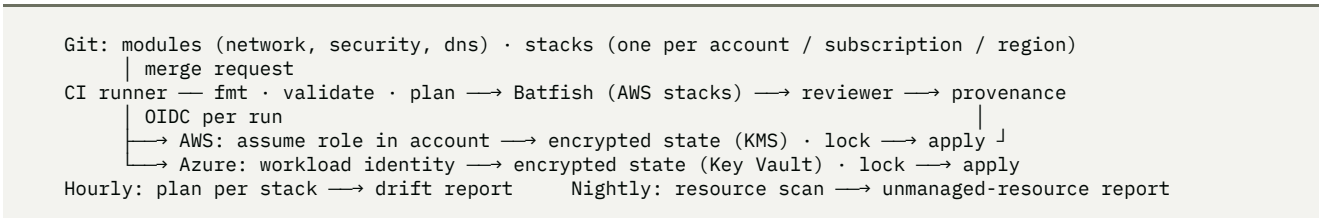


Figure 1. Cloud network pipeline, AWS and Azure

One module set for each cloud, one stack per account or subscription and region, one state file per stack. The pipeline never holds a stored cloud credential, and state is never written in clear to a backend: the engine encrypts it before it leaves the runner.

© 2026 Symbeeo. All rights reserved. · Public

Table 4. Architecture overview

Role	Product (exact version)	Qty	Capacity used	Why this unit
IaC engine	OpenTofu 1.12.6 (Aug 19, 2026) [S]	in CI	104 stacks [A]	state encryption, dynamic `prevent_destroy` [S]
AWS state backend	Amazon S3 bucket per account, S3-native lock file per stack [S]	40	80 stacks [A]	per-account layout [A]; locking without DynamoDB since OpenTofu 1.10.0 [S]
Azure state backend	Azure Storage container per subscription [A]	12	24 stacks [A]	same layout, second cloud [A]
State keys	AWS KMS · Azure Key Vault [S]	1 key per cloud and environment [A]	104 state files [A]	OpenTofu key providers [S]
Model check	Batfish v2026.08.27 [S]	1 service	AWS stacks [A]	models VPCs, security groups, gateways, network ACLs [S]
Stack orchestration	Terragrunt [S]	in CI	104 stacks [A]	runs with OpenTofu or Terraform [S] (`https://docs.terragrunt.com/docs/getting-started/quick-start`, no page date, read Sep 27, 2026)

4 · Design by subsystem

4.1 Engine and code layout.

OpenTofu 1.12.6, the latest release on Sep 24, 2026 [S], pinned in the CI image [A]. Modules per concern — network, security rules, DNS — and one stack per account or subscription and region: 40 × 2 + 12 × 2 = 104 stacks [A]. Rejected: one state for the whole estate — a single lock serializes five engineers, and a bad apply reaches every account. Terraform 1.16 meets the same requirements (SRA-AUT-001 D5); the agency's licensing policy decides for OpenTofu [A].

4.2 State, encryption and locking.

One state per stack in its own account's backend, locked per stack (R12) [A]. On AWS the lock is the `s3` backend's own lock file (`use_lockfile = true`), written beside the state object; no DynamoDB lock table is created [S]. The engine encrypts state and plan files before they are written, AES-GCM with a key from AWS KMS or Azure Key Vault [S] (R4). A reader of the storage bucket sees ciphertext; the key policy, not the bucket policy, decides who can read network secrets [A].

4.3 Pipeline and review.

Format, validate and plan for every stack the merge request touches; the plan output is attached to the merge request for a reviewer who is not the author (R3) [T]. Provider checksums for all platforms are recorded at init [S] and the lock file is committed, so a changed provider binary fails the run (R8) [A]. Production stacks set `prevent_destroy` through a variable, which OpenTofu 1.12 allows [S] (R7). The applied artifact carries a signed build record at SLSA Build L2 (R9) [T].

4.4 Model check.

For AWS stacks, the planned security groups, route tables and network ACLs are loaded into Batfish, which models AWS VPCs, security groups, gateways and network ACLs [S]; baseline questions — no spoke reachable from another spoke except through the hub, no inbound rule from the internet outside the approved list — fail the run on any

© 2026 Symbeeo. All rights reserved. · Public

unexpected answer (R6) [A]. Batfish v2026.08.27 adds Azure modeling as experimental [S]; until it leaves that status, Azure stacks are checked by plan-policy rules only [A].

4.5 Pipeline identity.

Each run requests a short-lived identity from each cloud through OpenID Connect and assumes a role scoped to the stack's account or subscription — each cloud's workload-identity federation, confirmed per cloud at design [A]. No cloud access key or client secret exists in the pipeline or the repository (R5) [T].

4.6 Drift, rollback and audit.

Every hour each stack runs a plan; a non-empty plan opens a drift ticket (R10) [T]. A nightly scan lists network resources in every account and subscription and reports any not in state (R2) [A]. Rollback is a revert commit through the same pipeline, ≤ 30 minutes per stack (R11) [T]. Pipeline runs and each cloud's control-plane log are kept seven years (R13) [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Key service unreachable	engine cannot decrypt state; plan and apply fail closed; cloud networks unaffected	[S] state encryption; [A] behavior
Two engineers change one stack	second run fails to take the stack's lock and is re-queued	[S] S3 lock file; [A] re-queue
Batfish finds a spoke-to-spoke path	run fails before review; nothing applied	[T] R6
Engineer changes a route table in the console	hourly plan shows drift; ticket opened ≤ 1 h	[T] R10
Apply fails part-way on one stack	state records what was created; re-run or revert commit	[A]
Planned change would delete a production network	`prevent_destroy` stops the run	[S] OpenTofu 1.12
OIDC provider unreachable	runs fail closed; break-glass role held by two named engineers	[A]

6 · Limits

- The account counts and resource total are assumptions; the first import sets the real inventory, and resources that cannot be imported cleanly are rebuilt in a window.
- The model check covers AWS only; Batfish's Azure modeling is experimental on Sep 24, 2026.
- Hourly drift planning of 104 stacks costs API calls in both clouds; the interval is tuned after the first month.
- Losing a state key makes that state unreadable; key deletion protection and a second key holder are part of the key-service design, which is out of scope here.
- S3-native locking is chosen over a DynamoDB table; OpenTofu still supports both, Terraform has deprecated the DynamoDB arguments since 1.11.0 [S], so the choice keeps D5 open.

© 2026 Symbeeo. All rights reserved. · Public

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

Mark Winston

Principal Network Architect

CCIE, CISSP, CCSP, CCISO, CISM, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

AUT-005 · Version 1.1 · Oct 10, 2026