SURF

Cloud encryption

John Segers

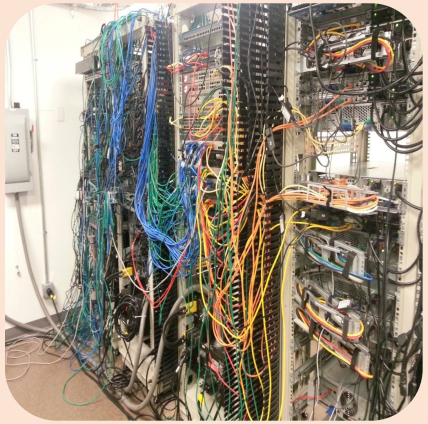
29 June, 2023

Reason & scope

Providers

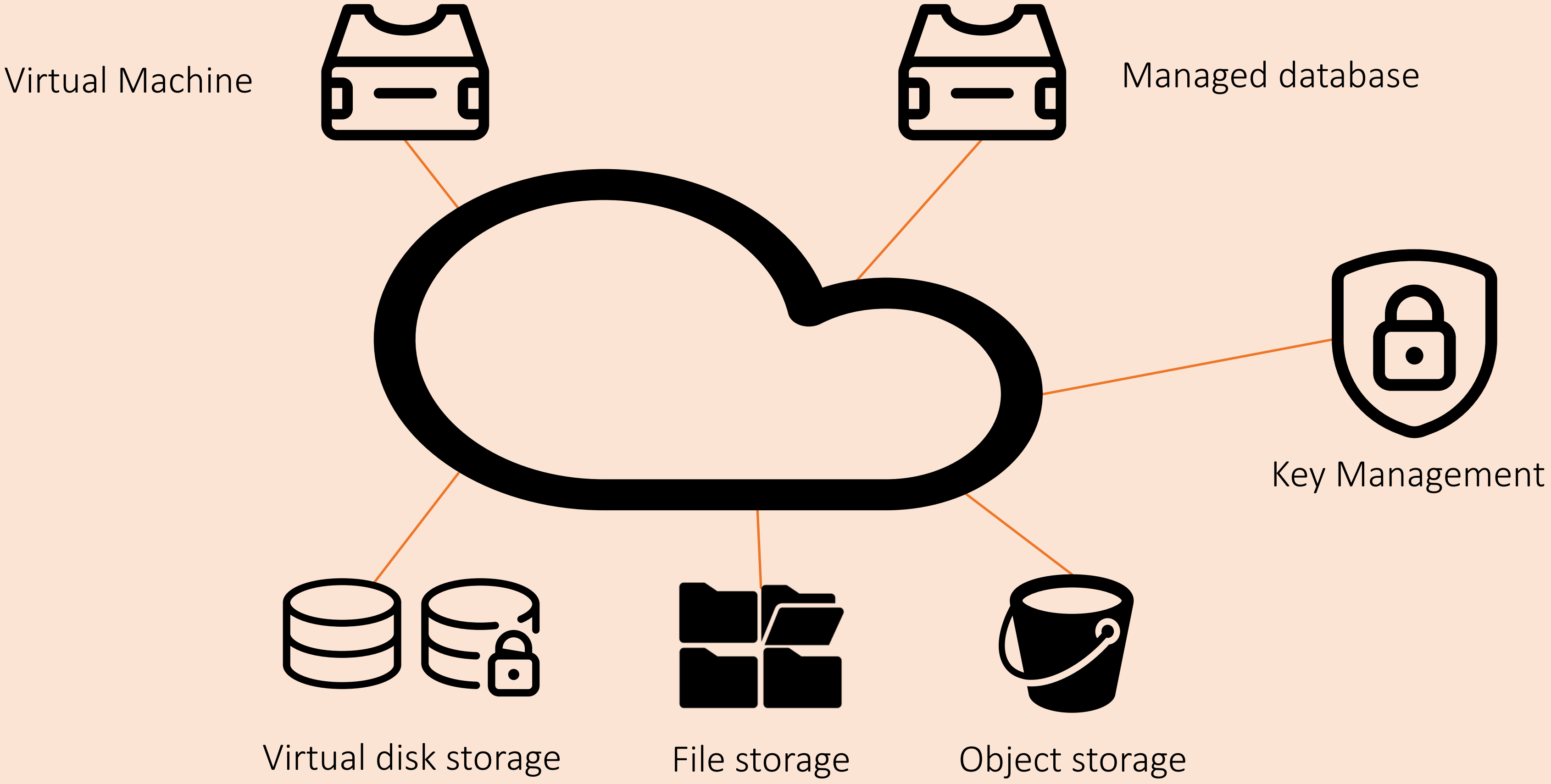
aws

Azure



Risks

Services



SURF

Conclusions

Cloud encryption key findings

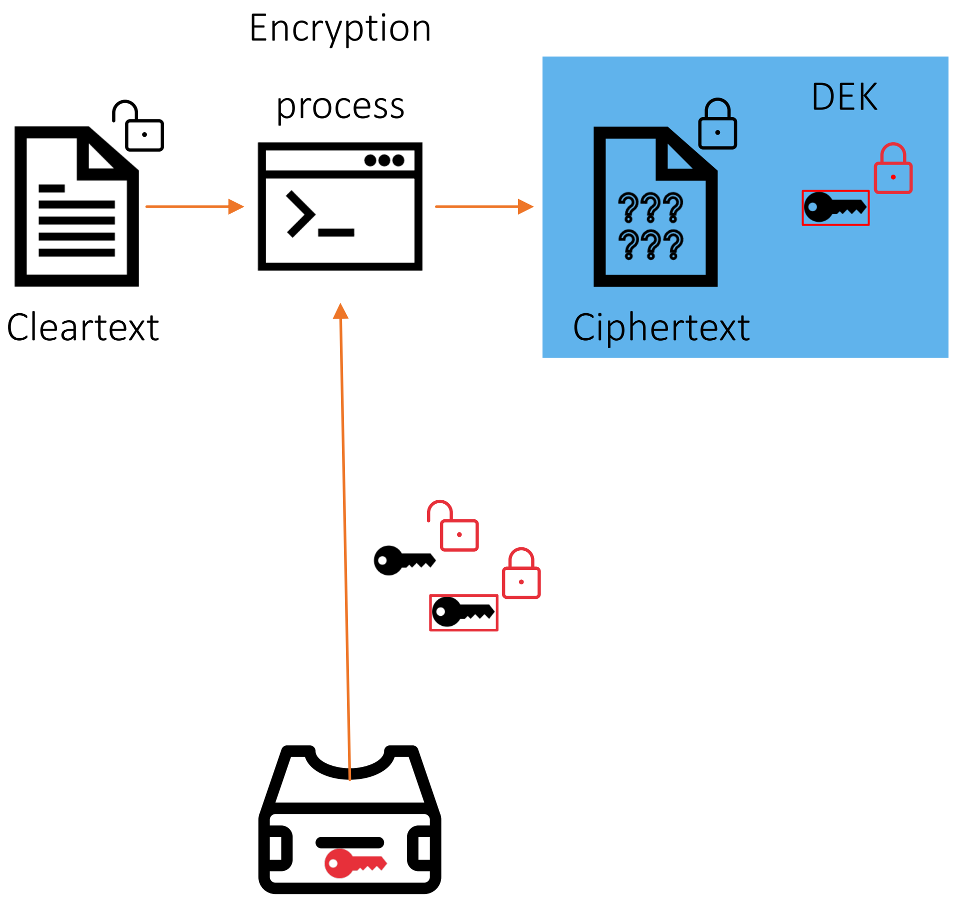
1. Encryption offers protection against data loss via unauthorized access to physical media.
2. Virtual disks: AWS has no access to customer data on virtual disks, even when attached to Nitro VMs. Microsoft has no equivalent guarantee.
3. Object storage and shared files: access to data by the provider cannot be ruled out when using server-side encryption; use client-side encryption to prevent access.
4. Managed relational database services:

- Providers need access to database hosts and have dba privileges within the DBMS to deliver the service; encrypting data storage does not offer sufficient protection.
- SQL Server Always Encrypted and SQL Server Always Encrypted with secure enclaves offer extra protection. These functions are available for Azure SQL. SQL Server Always Encrypted is available for Amazon RDS.

Encryption key management

Envelope encryption

- Encrypt every data object with a unique Data Encryption Key (🔑).
- Protect DEKs by wrapping them with a Key Encryption Key (🔑).
- Store wrapped DEKs (🔑) with the encrypted data objects.
- Store KEKs securely, e.g inside a certified Hardware Security Module.
- Govern access to HSMs.



Encryption process

Cleartext

DEK

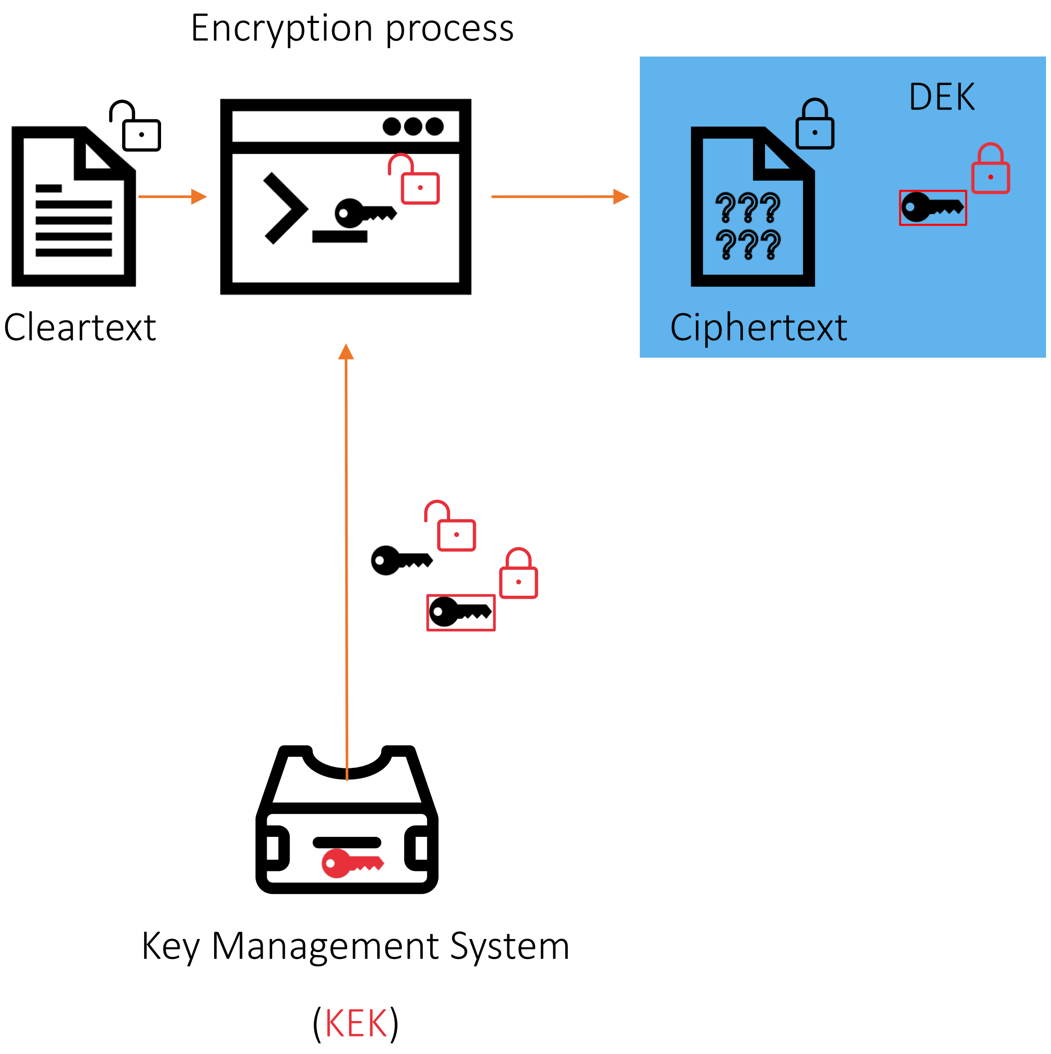
Ciphertext

Key Management System

(KEK)

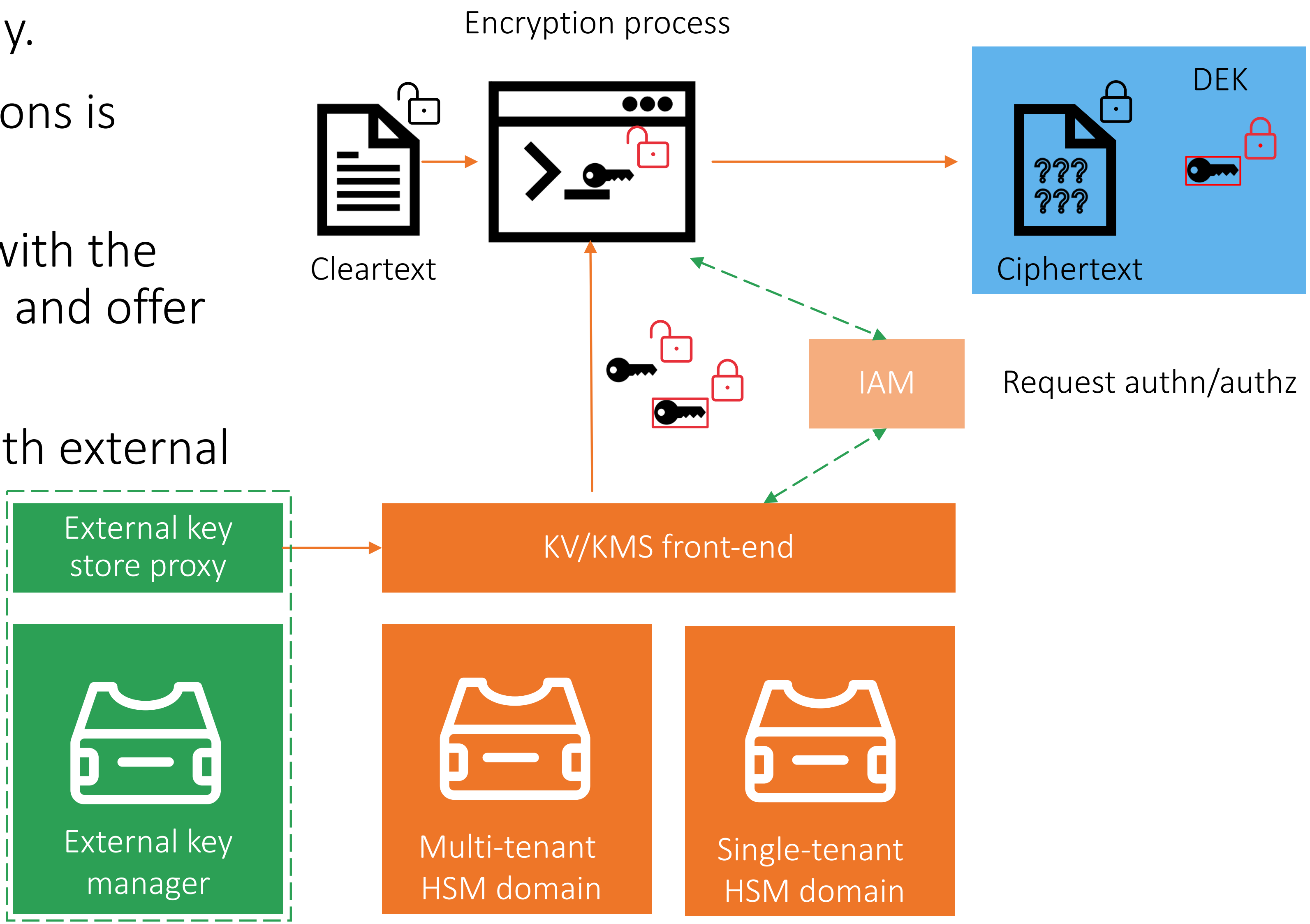
Cloud key management – Azure Key Vault & AWS KMS

- Azure KV Standard uses software keys; KV Premium offers key storage in certified HSMs (FIPS 140-2 L2)
- AWS KMS uses certified HSMs only (FIPS 140-2 L3)
- The default is multi-tenant key storage, single-tenant is an option
- SOC 2, ISO 27001, C5 attestations provide trust in provider’s operating procedures for key management



Cloud key management – IAM & external key storage

- KEKs are stored securely.
- Authn/authz of operations is crucial!
- KV and KMS integrate with the providers’ IAM systems and offer RBAC.
- AWS KMS integrates with external key storage



SURF

Cloud key management – who manages the KEKs?

Two types of KEKs are available

1. Platform Managed Key (PMK).

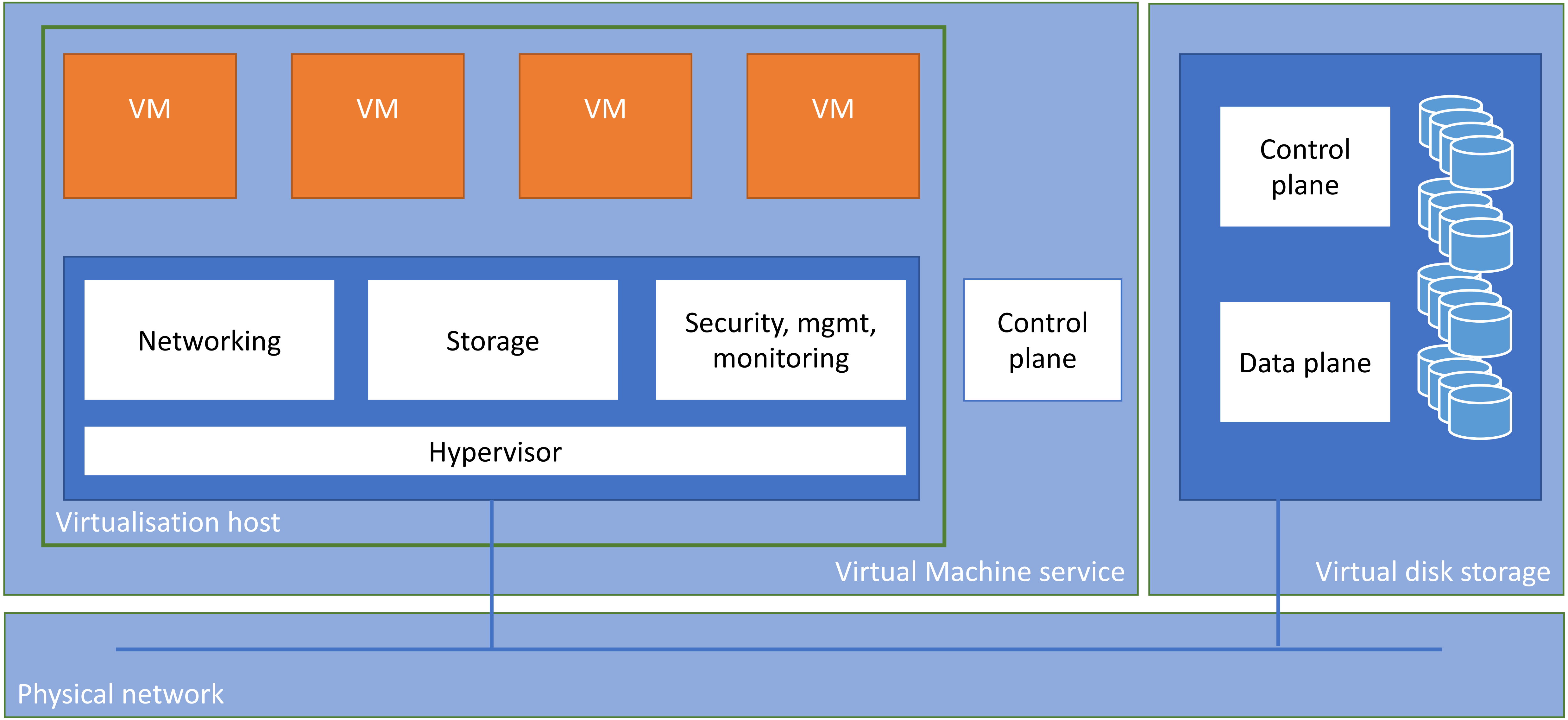
- Provider manages the key life cycle and key scope.

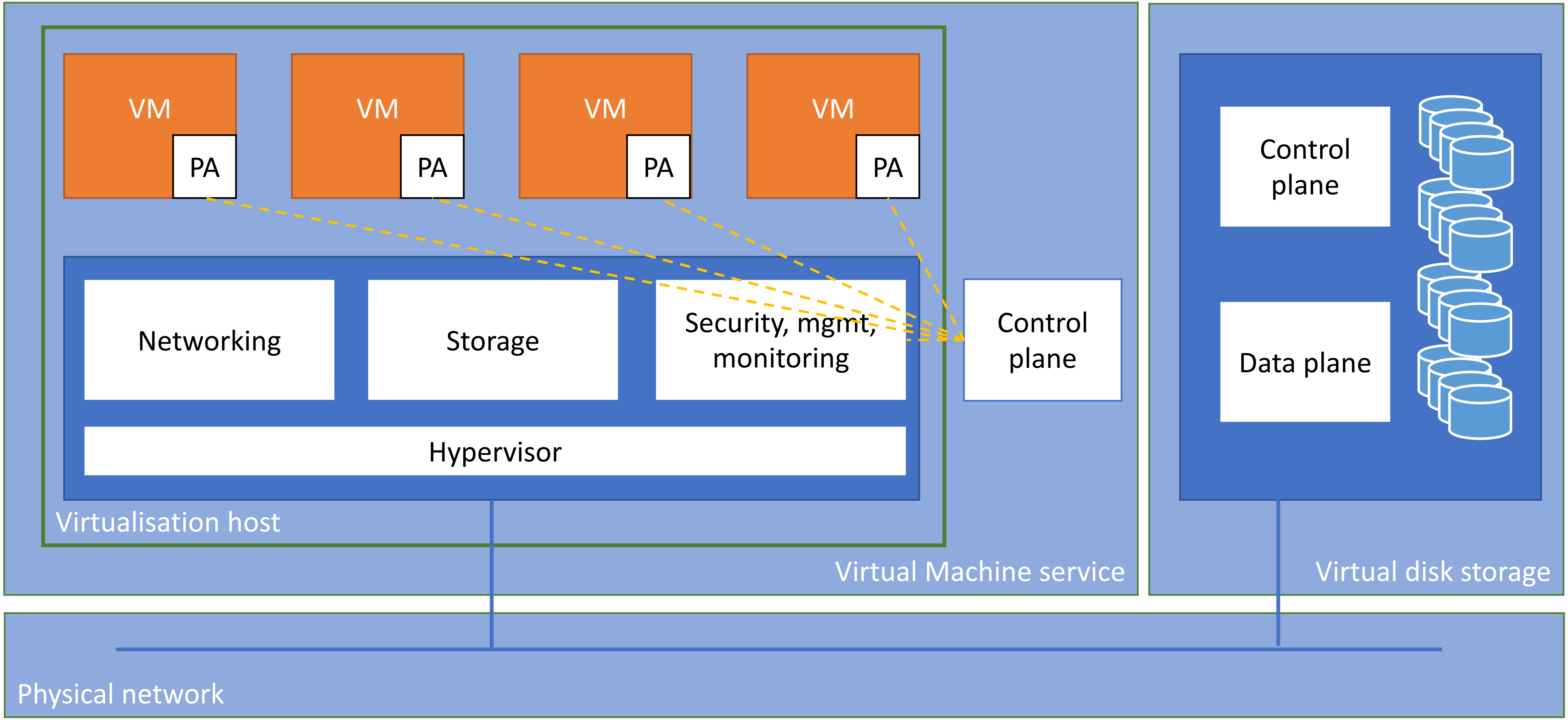
2. Customer Managed Key (CMK).

- Customer manages the key life cycle and key scope.

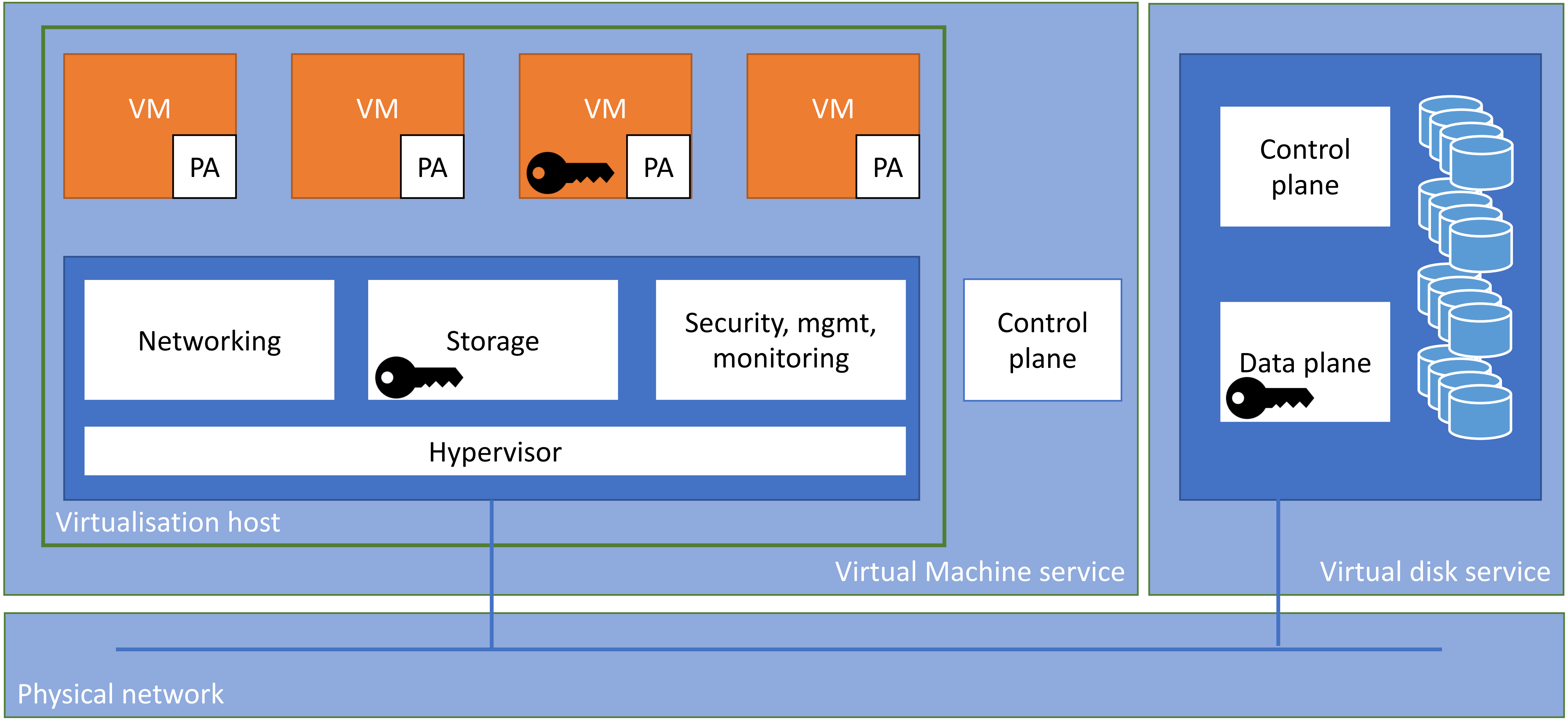
In view of NBA security control SM.10 or ISO 27001 A.10.1.2, institutions should use CMKs to encrypt sensitive data.

Virtual disk encryption

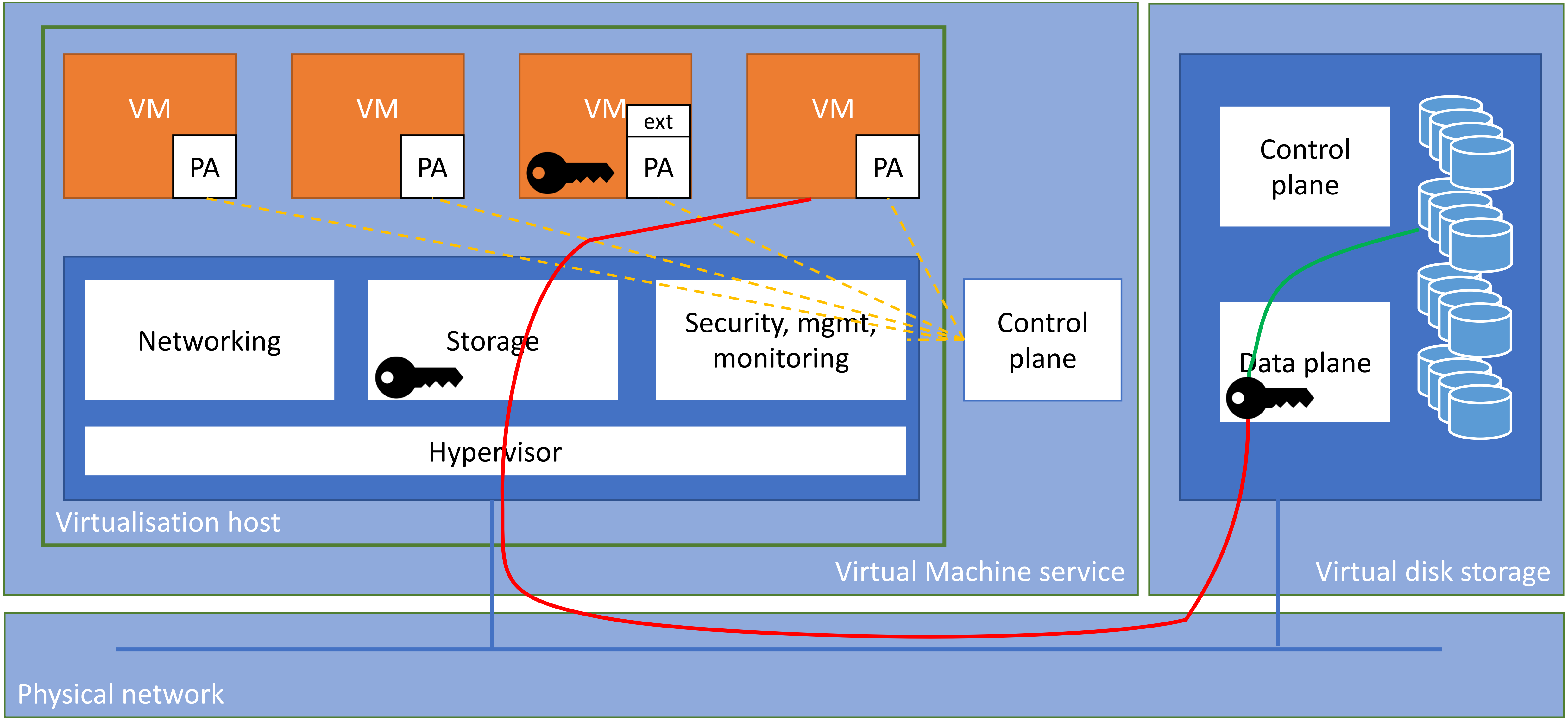

VM
VM
VM
VM
Networking
Storage
Security, mgmt, monitoring
Hypervisor
Virtualisation host
Control plane
Virtual Machine service
Control plane
Data plane
Virtual disk storage
Physical network



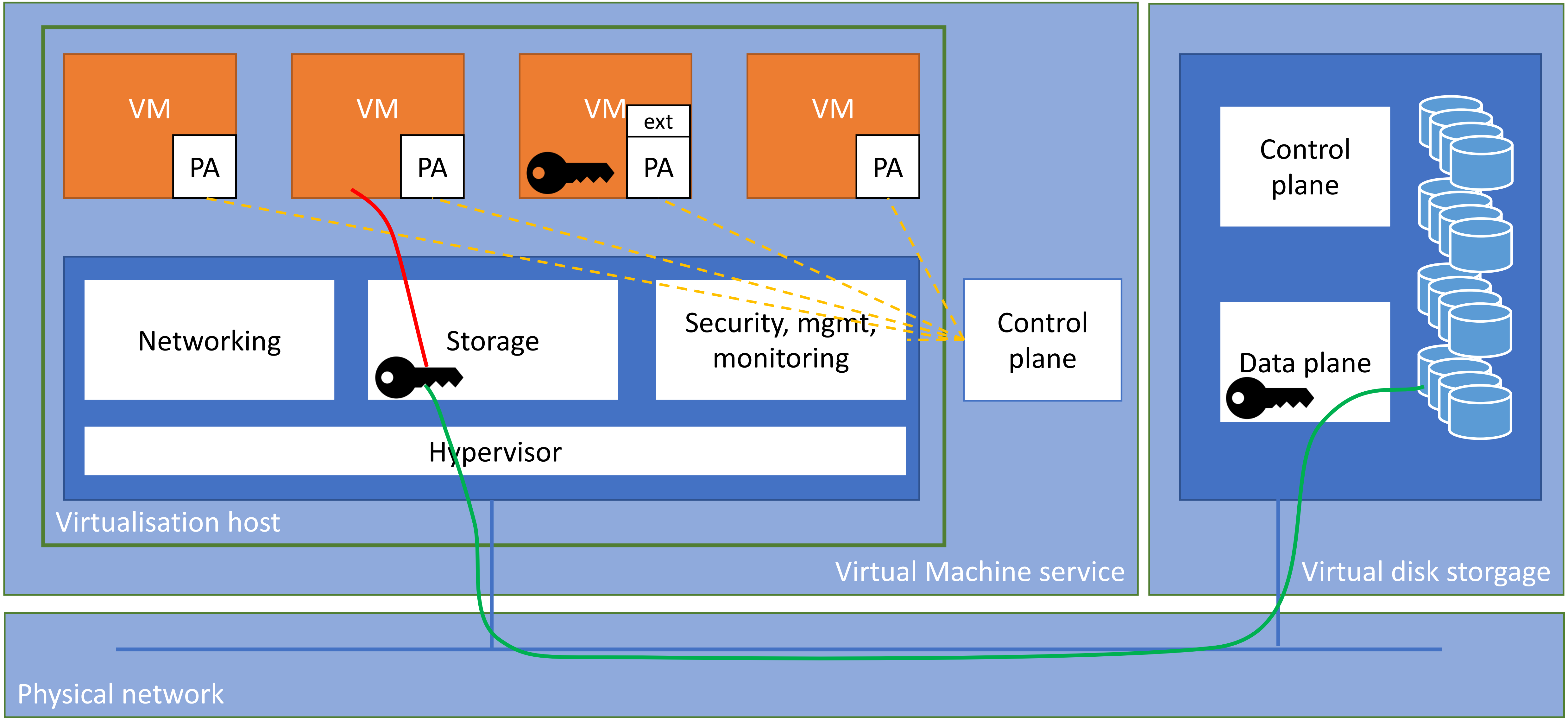
PA = Provider Agent



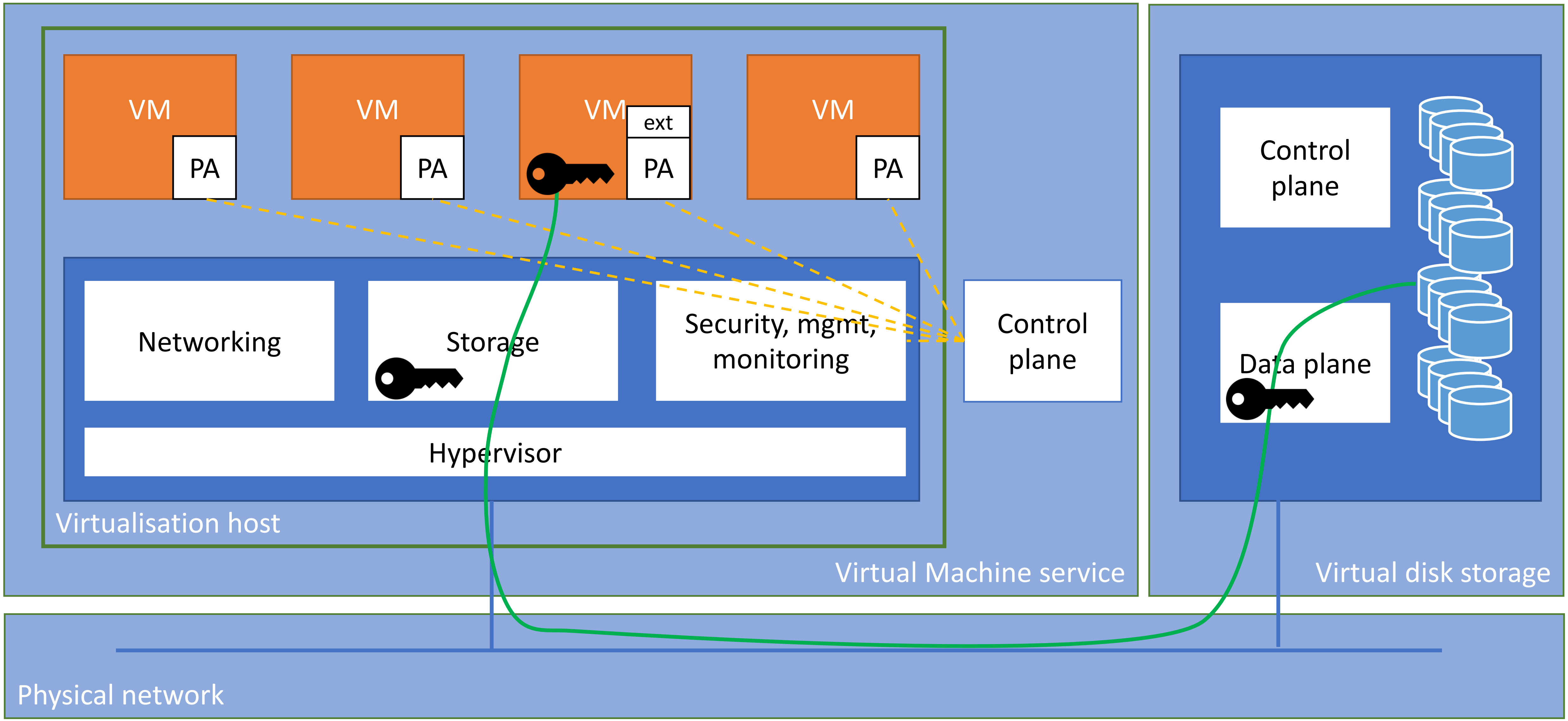
PA = Provider Agent



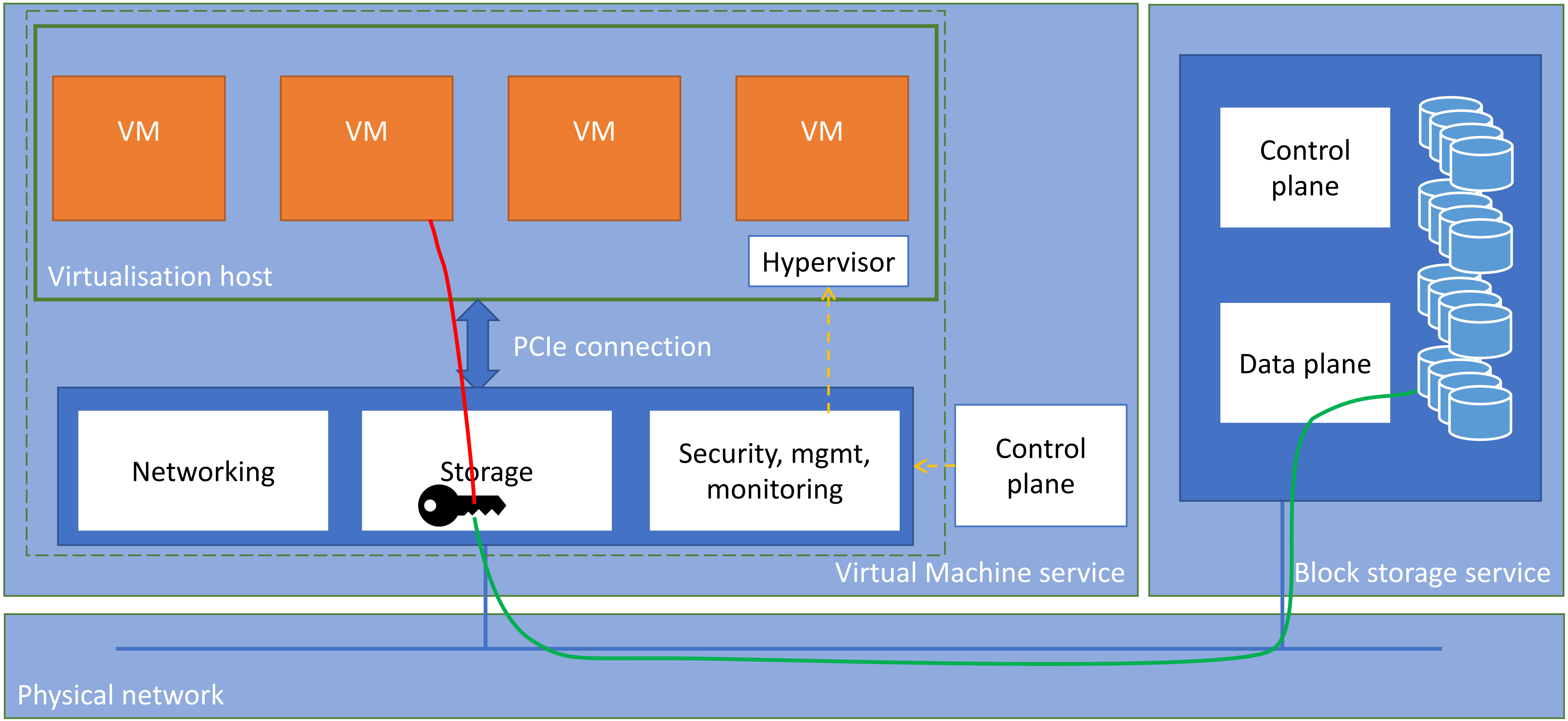
PA = Provider Agent



PA = Provider Agent



PA = Provider Agent



VM

VM

VM

VM

Virtualisation host

Hypervisor

PCIe connection

Networking

Storage

Security, mgmt, monitoring

Control plane

Virtual Machine service

Control plane

Data plane

Block storage service

Physical network

~~PA = Provider Agent~~

AWS Service terms

96. AWS Nitro System

AWS personnel do not have access to Your Content on AWS Nitro System EC2 instances. There are no technical means or APIs available to AWS personnel to read, copy, extract, modify, or otherwise access Your Content on an AWS Nitro System EC2 instance or encrypted-EBS volume attached to an AWS Nitro System EC2 instance. Access to AWS Nitro System EC2 instance APIs – which enable AWS personnel to operate the system without access to Your Content - is always logged, and always requires authentication and authorization.

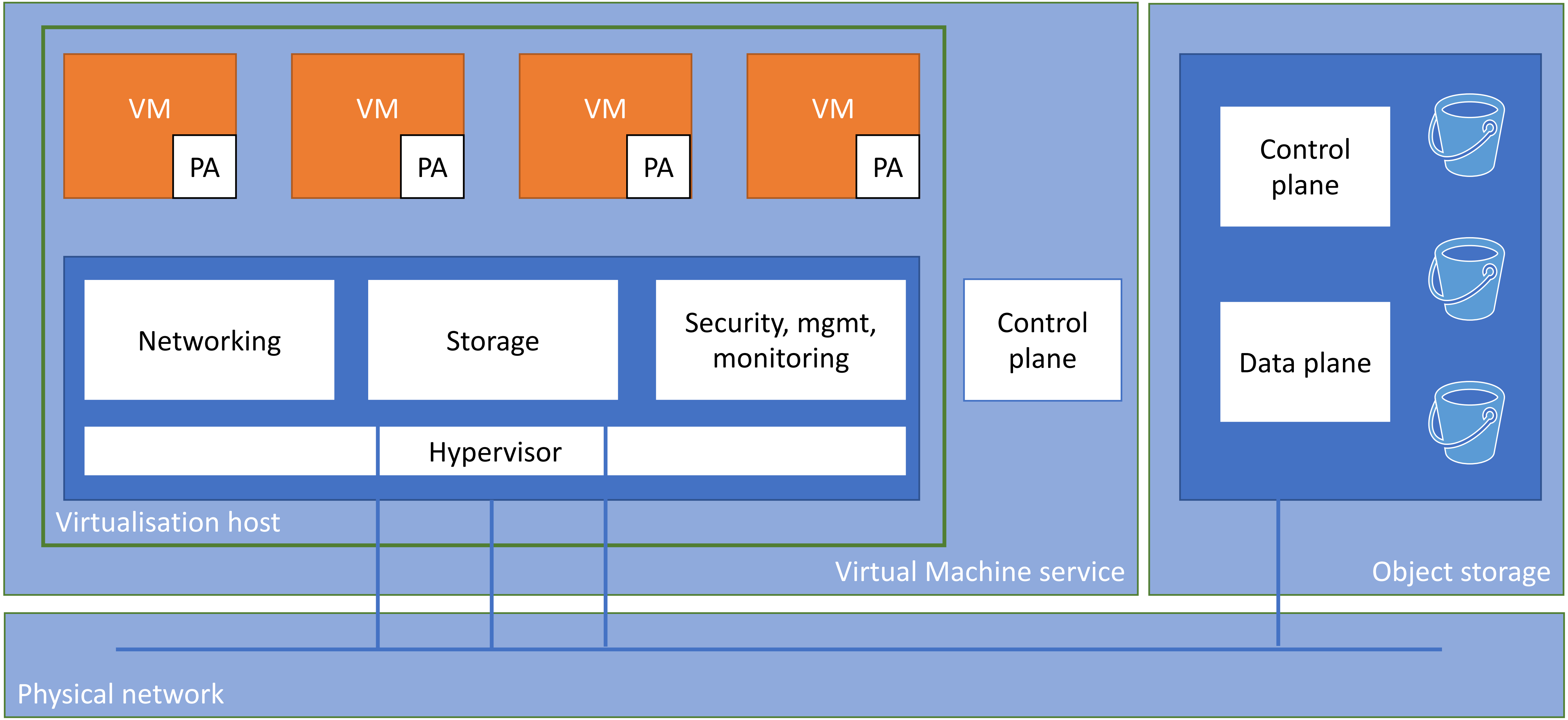
From *https://aws.amazon.com/service-terms/*

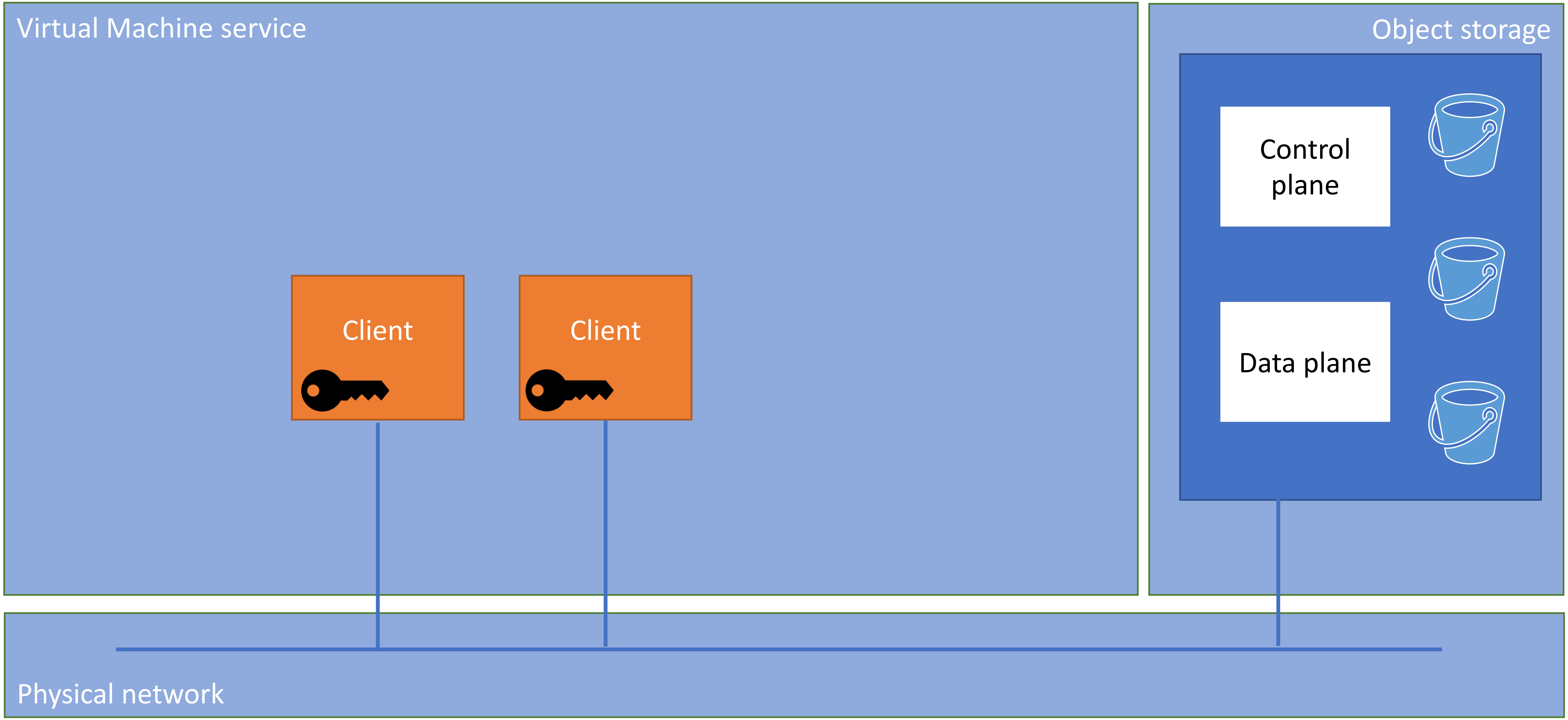
Encryption of virtual disk storage

	AWS	Azure	On-prem
Vanaf VM	User can configure Bitlocker or LUKS, no integration with KMS	Azure Disk Encryption (Bitlocker/LUKS with Key Vault integratie)[1]	User can configure Bitlocker or LUKS
Vanaf host	EBS encryption[2]	Host-based encryption[1]	vSphere: encrypted VMs & disks
- Key management	AWS KMS	Azure Key Vault	vSphere Native Key Provider[3] or external key server
Server-side encryption	No	Yes	Depends on storage solution,e.g. vSAN
- Encryption-in-transit	Not applicable	No	No

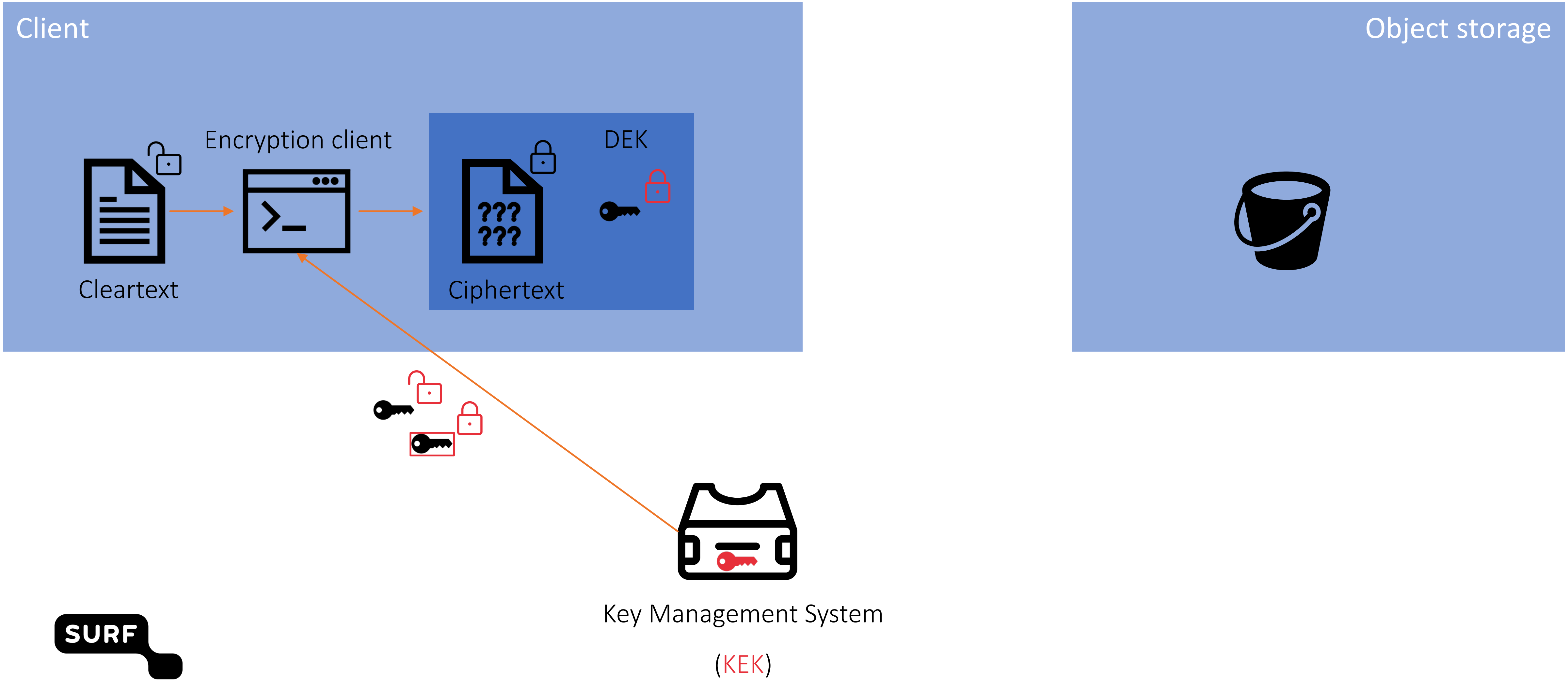
[1] Niet voor Ultra Disks, [2] Vanaf Nitro controller, [3] sleutels staan op de host

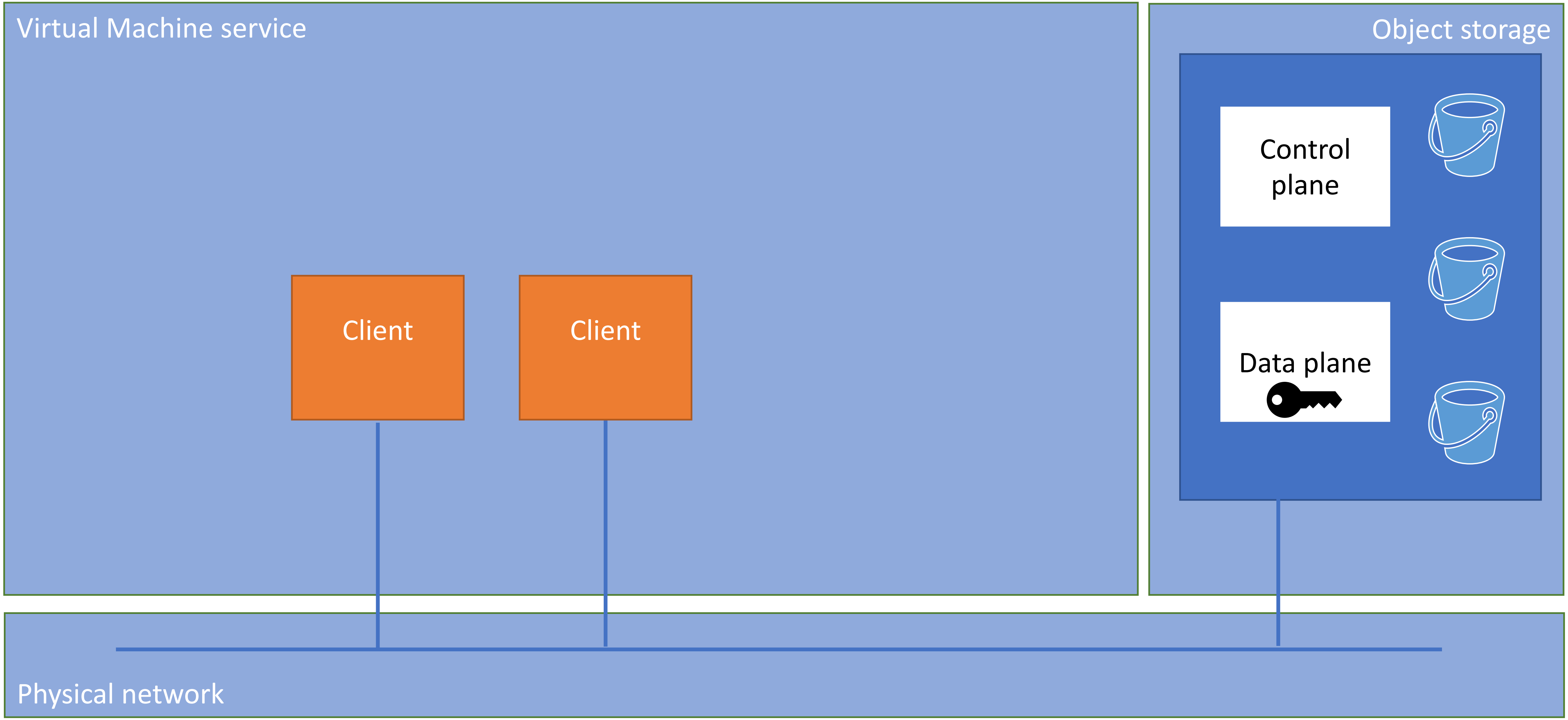
Object storage encryption


VM
PA
VM
PA
VM
PA
VM
PA
Networking
Storage
Security, mgmt, monitoring
Hypervisor
Virtualisation host
Control plane
Virtual Machine service
Control plane
Data plane
Object storage
Physical network


Virtual Machine service
Object storage
Control plane
Data plane
Client
Client
Physical network

Client-side encryption

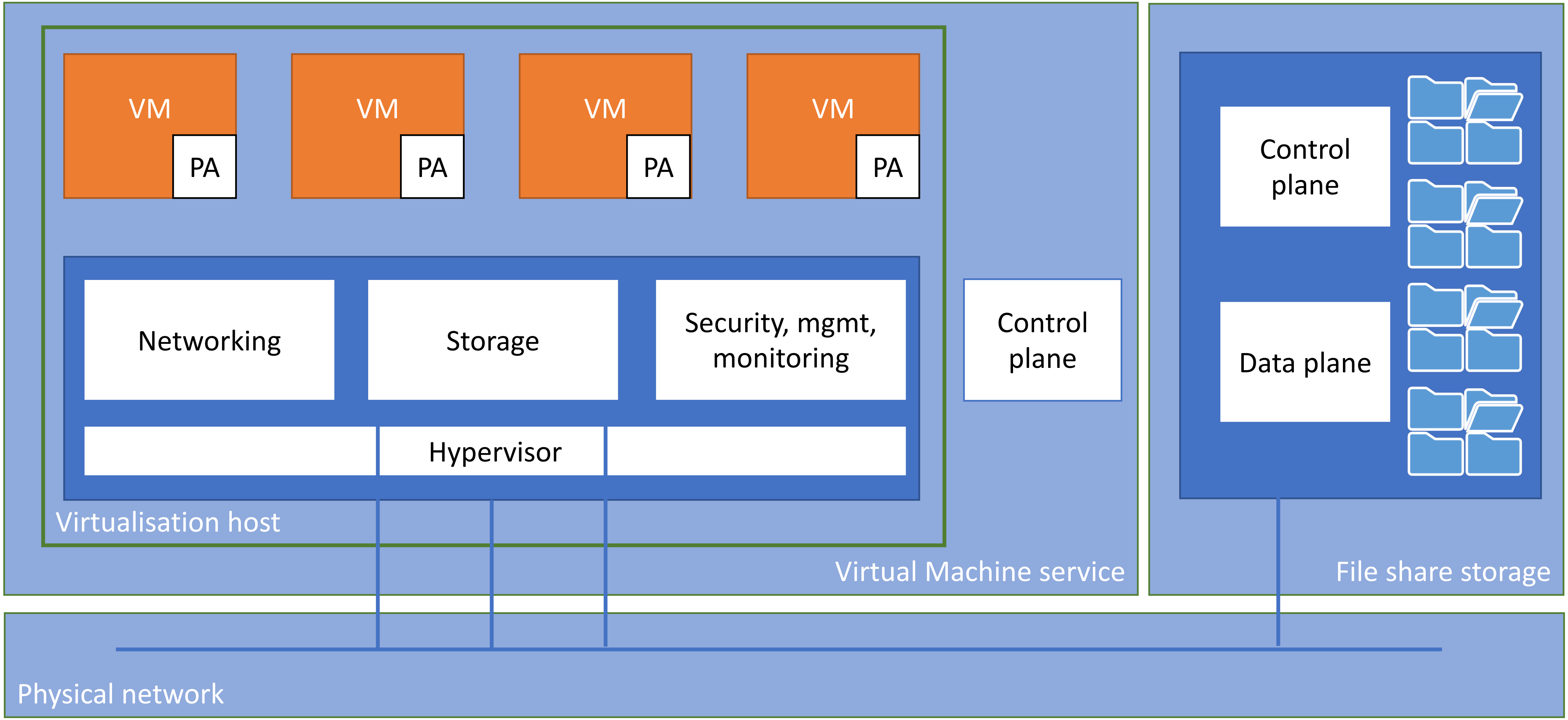



Virtual Machine service
Object storage
Control plane
Data plane
Client
Client
Physical network

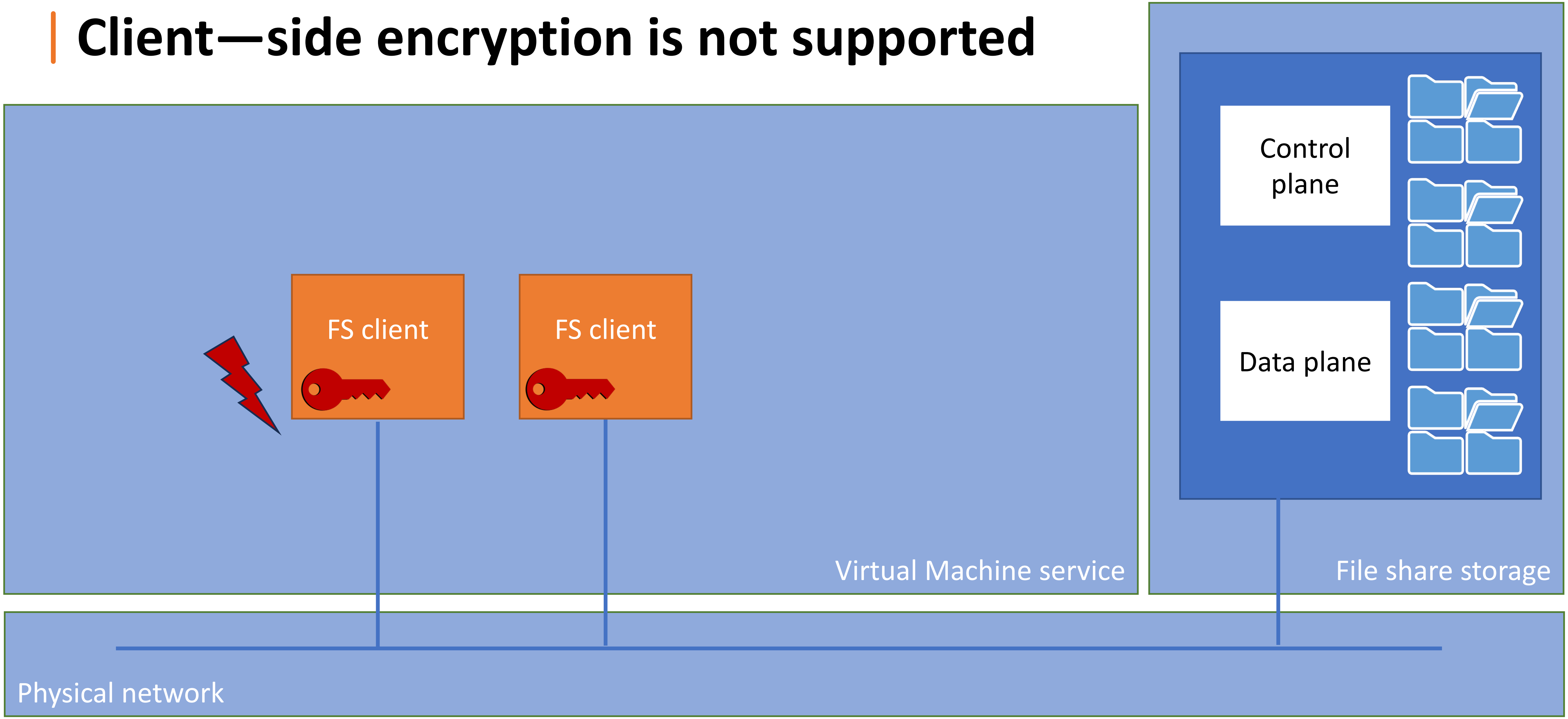
Encryption of object storage

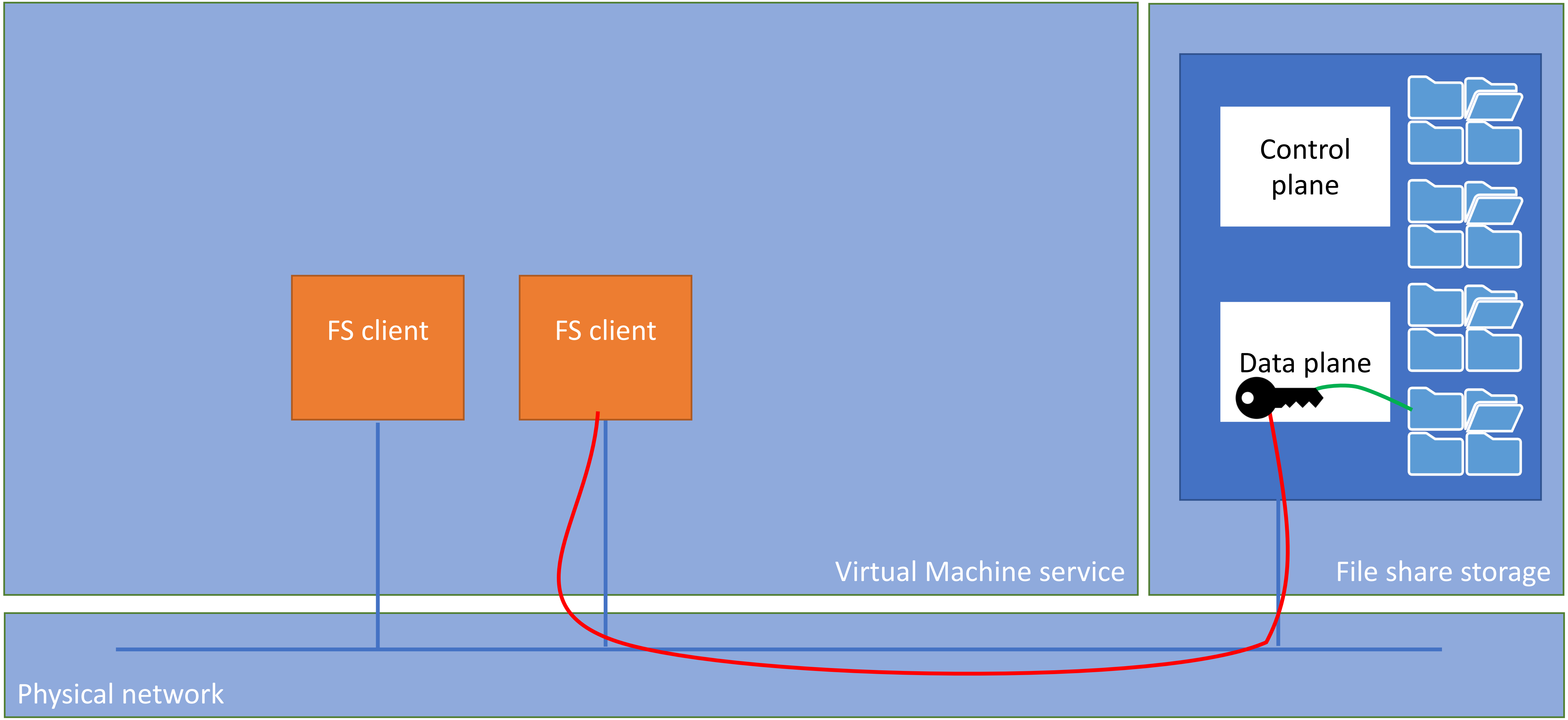
	AWS	Azure
Server-side encryption	Standard	Standard
- KEK	Standaard is platform-managed, customer-managed is optional	Standard is platform-managed, customer-managed is optional
User authenticatie	RBAC & ABAC	RBAC
Client-side encryptie	Optional	Optional
- Encryption client	.Net, Java, Go, PHP, Ruby, C++	.Net, Java, Python *Use v2!*
- Key management	AWS KMS or external	Azure KV or external

File share encryption


VM
PA
VM
PA
VM
PA
VM
PA
Networking
Storage
Security, mgmt, monitoring
Hypervisor
Virtualisation host
Control plane
Virtual Machine service
Control plane
Data plane
File share storage
Physical network

Client—side encryption is not supported




FS client
FS client
Control plane
Data plane
Virtual Machine service
File share storage
Physical network

Encryption of file shares

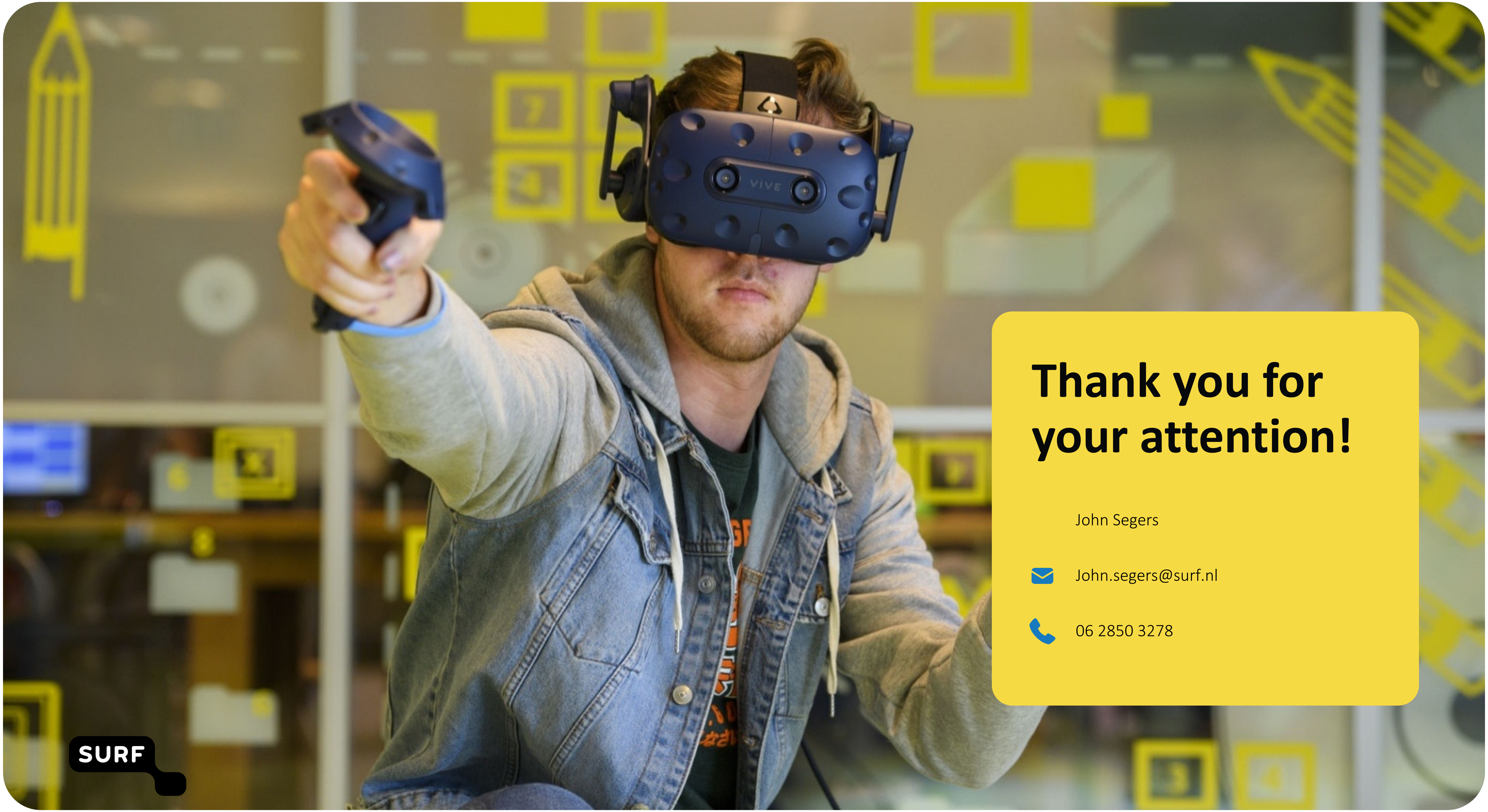
	AWS	Azure
SMB file sharing		
- Encryption in transit	Default for SMB 3.x clients	Default for SMB 3.x clients
- Encryption at rest	Optional, CMK suppored	Default, CMK **not** supported
- User authentication	Yes	Yes
NFS file sharing		
- Encryption in transit	Optional with stunnel or Amazon EFS mount helper	**Not supported**
- Encryption at rest	Optional, CMK supported	Default, CMK **not** supported
- User authenticatie	Yes	**No,** only netwerk security rules

Conclusions

Key findings

1. Protection against data loss by access to physical media.
2. Virtual disks: AWS has no access to customer data on virtual disks, even when attached to Nitro VMs; Microsoft has no equivalent guarantee.
3. Object storage and shared file: access to data by the provider cannot be ruled out when using server-side encryption; use client-side encryption to prevent access.
4. Managed relational database services:

- Providers need access to database hosts and have dba privileges within the DBMS to deliver the service; encrypting data storage does not offer sufficient protection.
- SQL Server Always Encrypted and SQL Server Always Encrypted with secure enclaves offer extra protection. These functions are available for Azure SQL. SQL Server Always Encrypted is available for Amazon RDS.



Thank you for your attention!

John Segers

✉ John.segers@surf.nl

☎ 06 2850 3278