

06 - Identity, network access and PKI

Describe application access, network admission and certificate work so each part can be scoped.

Draft answers do not authorize access or create a contract. The proposal confirms scope, price and acceptance checks.

Keep answers brief. Name the source, owner and date. Leave unknowns marked. Do not include passwords, keys or sensitive records.

1. Which access or certificate problems should we address?

Choose application SSO, network admission, privileged access, PKI lifecycle or a combination.

Answer

Source / owner / date

2. Which directory is the source for identities and roles?

Describe lifecycle approvals, role ownership and emergency recovery.

Answer

Source / owner / date

3. Which applications and access protocols are involved?

Give product versions, federation or provisioning protocols and required entitlements.

Answer

Source / owner / date

06 - Identity, network access and PKI

Describe application access, network admission and certificate work so each part can be scoped.

Draft answers do not authorize access or create a contract. The proposal confirms scope, price and acceptance checks.

Keep answers brief. Name the source, owner and date. Leave unknowns marked. Do not include passwords, keys or sensitive records.

4. What can the network devices and clients support?

Give vendors, versions, 802.1X methods, enforcement options and fallback behavior.

Answer

Source / owner / date

5. How will approved and unknown devices be handled?

Reference the device register. Describe BYOD, unknown devices, roles and denial rules.

Answer

Source / owner / date

6. Which network access workflows are needed?

Describe profiling, guest access or posture checks, and confirm support in the actual products.

Answer

Source / owner / date

06 - Identity, network access and PKI

Describe application access, network admission and certificate work so each part can be scoped.

Draft answers do not authorize access or create a contract. The proposal confirms scope, price and acceptance checks.

Keep answers brief. Name the source, owner and date. Leave unknowns marked. Do not include passwords, keys or sensitive records.

7. Who owns the certificate authorities, enrollment and keys?

Describe templates, enrollment, protected key custody, backups and the responsible owners.

Answer

Source / owner / date

8. How should applications and devices check certificate trust?

Agree hostname, chain, expiry and revocation checks, including certificate status service outages.

Answer

Source / owner / date

06 - Identity, network access and PKI

Describe application access, network admission and certificate work so each part can be scoped.

Draft answers do not authorize access or create a contract. The proposal confirms scope, price and acceptance checks.

Keep answers brief. Name the source, owner and date. Leave unknowns marked. Do not include passwords, keys or sensitive records.

9. Which access and recovery checks should the pilot include?

Name representative apps and devices. Test approved access, invalid access, removal and recovery.

Answer

Source / owner / date

10. How should changes be introduced and reversed?

Agree the window, operator, backups, acceptance decision and rollback path.

Answer

Source / owner / date