KRYPTUS

APPLICATION NOTE · CRIPTOGRAFIA PÓS-QUÂNTICA

Autoridade Certificadora pós-quântica no Active Directory Certificate Services

Emitindo certificados ML-DSA no Windows Server 2025 com a chave de assinatura protegida no ASI-HSM AHX5 kNET

Documento: Guia técnico de prova de conceito
Versão: 1.0 · **Data:** Maio de 2026
Aplicável a: Windows Server 2025, AD CS, Provedor CNG (KSP) kNET da Kryptus, ASI-HSM AHX5 kNET
Classificação: Público

Sumário executivo

A atualização de maio de 2026 do Windows Server 2025 (KB5087539) habilitou o algoritmo pós-quântico **ML-DSA** (FIPS 204) no **Active Directory Certificate Services (AD CS)**. Combinada ao provedor CNG (KSP) da Kryptus, ela permite operar uma **Autoridade Certificadora (AC) resistente a ataques quânticos cuja chave de assinatura nunca deixa o HSM**.

Esta Application Note apresenta o contexto da transição pós-quântica e um **passo a passo reproduzível** para: (1) atualizar o Windows Server; (2) instalar e provisionar o provedor CNG da Kryptus; (3) criar uma AC no AD CS usando ML-DSA com a chave gerada e protegida no **ASI-HSM AHX5 kNET**; e (4) **emitir certificados e listas de revogação (LCRs) assinados com ML-DSA**.

1. Contexto

Em agosto de 2024 o NIST finalizou os primeiros padrões pós-quânticos: **FIPS 203 (ML-KEM)** para encapsulamento de chaves, **FIPS 204 (ML-DSA)** e **FIPS 205 (SLH-DSA)** para assinatura digital. A partir daí, a adoção pela indústria avançou rápido.

A Microsoft incorporou o pós-quântico em camadas sucessivas. Em **setembro de 2024**, os algoritmos ML-KEM e XMSS chegaram à biblioteca criptográfica SymCrypt. Em **maio de 2025**, a PQC apareceu nas APIs CNG do Windows Insiders e do Linux em acesso antecipado. No **fim de 2025**, as APIs ML-KEM e ML-DSA entraram em disponibilidade geral no Windows Server 2025 e no Windows 11 24H2/25H2, já integradas ao CNG e às funções de certificado. Em **maio de 2026**, a atualização **KB5087539** (build 26100.32860) levou o ML-DSA ao AD CS, habilitando a emissão de certificados pela role de PKI.

Do lado da Kryptus, o trabalho com algoritmos pós-quânticos começou em **2020**; o marco veio em **2024**, quando o **ASI-HSM AHX5 kNET** obteve a certificação **CAVP do NIST** para sua implementação de ML-DSA e ML-KEM. O HSM gera e custodia chaves ML-DSA (e demais famílias PQC) dentro do hardware seguro, e o provedor CNG (KSP) da Kryptus o integra ao Windows como um *Key Storage Provider* nativo que, com a atualização do AD CS, passa a lastrear ACs pós-quânticas de ponta a ponta.

1.1 Sobre esta prova de conceito

Este documento é um **guia técnico de prova de conceito (PoC)**. O passo a passo dos capítulos seguintes foi validado em ambiente de laboratório, com valores de exemplo (endpoints, credenciais, nomes de servidor e de Autoridade Certificadora). Cada figura corresponde ao resultado real desse laboratório.

Por se tratar de uma PoC, este guia **não substitui um projeto de implantação em produção**. Antes de aplicar a configuração descrita à sua PKI, adeque cada etapa às políticas de segurança vigentes, à topologia de rede, ao dimensionamento de capacidade e aos requisitos de conformidade do seu ambiente. Valide o conjunto em homologação antes da migração para produção.

2. Pré-requisitos

- **Windows Server 2025** para a(s) AC(s), com a atualização **KB5087539 (2026-05)** ou posterior (build 26100.32860+). Para um ambiente de testes, baixe a imagem de avaliação no Microsoft Evaluation Center (ISO ou VHD pronto para Hyper-V).
- **Role do AD CS instalada** no Windows Server 2025: *Server Manager → Manage → Add Roles and Features → Active Directory Certificate Services*, marcando o serviço *Certification Authority*. A *configuração* da AC (escolha do provedor ML-DSA do kNET) é feita no passo a passo da §3.3.
- **Provedor CNG (KSP) da Kryptus** para o kNET (instalador MSI assinado).
- **ASI-HSM AHX5 kNET** acessível por rede, com firmware que suporte ML-DSA, e um usuário/operador com permissão de criação e uso de chaves.
- Conta administrativa no servidor da AC.
- **Para validar os certificados ML-DSA emitidos** e verificar a cadeia de confiança, é preciso uma máquina cliente com suporte a criptografia pós-quântica: **Windows 11 24H2/25H2 com a atualização KB5067036 (out/2025) ou posterior**. Clientes sem suporte a PQC simplesmente não reconhecem certificados ML-DSA.

3. Passo a passo

3.1 Atualizar o Windows Server 2025

1. Instale a atualização cumulativa **KB5087539 (2026-05)**. Há três formas equivalentes; escolha a que se encaixa no seu ambiente:
   - **Windows Update (mais simples):** em *Configurações → Windows Update*, clique em *Verificar se há atualizações*. O pacote é baixado e instalado automaticamente.
   - **Pacote offline (.msu):** baixe o arquivo no Microsoft Update Catalog e instale com **duplo-clique** (abre o *Instalador Autônomo do Windows Update*) ou pela linha de comando:

     ```
     PS> wusa.exe .\windows11.0-kb5087539-x64.msu /quiet /norestart
     ```

   - **Gestão corporativa:** em parques administrados, a atualização é distribuída automaticamente pelos servidores corporativos de atualização, como o **WSUS** (*Windows Server Update Services*) ou o Microsoft Intune.

   Reinicie o servidor quando solicitado.

2. Confirme a build após o reboot:

   ```
   PS> $cv = Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion'
   PS> "$($cv.CurrentBuild).$($cv.UBR)"
   26100.32860             # build esperada (ou superior)
   ```

3.2 Instalar e provisionar o provedor CNG da Kryptus (KSP)

3. Execute o instalador assinado `knet-ksp-<versão>.msi` e siga o assistente: aceite o contrato de licença e conclua em *Install → Finish*. O provedor é registrado no Windows como `kNET Key Storage Provider` (Figura 1).

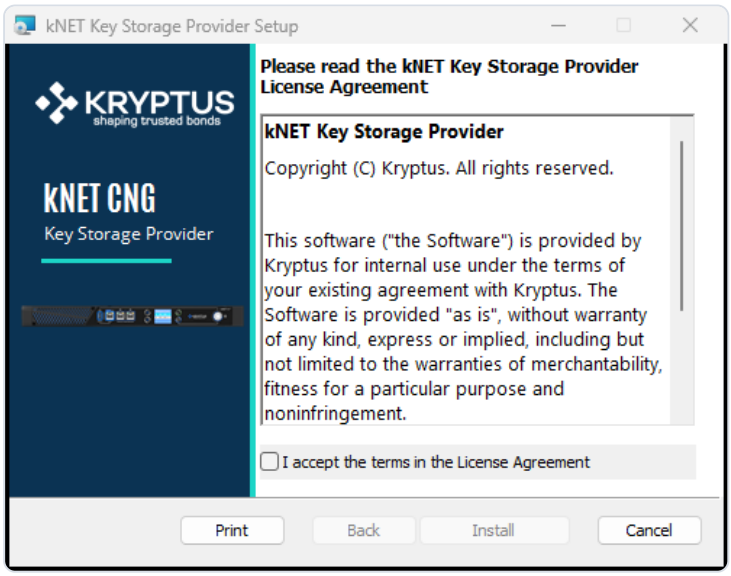

Figura 1. Instalador do provedor CNG da Kryptus.

4. Abra a **ferramenta gráfica do KSP**. Na aba *Connection*, informe um ou mais *HSM hosts* (um por linha, vários endpoints para cluster/alta disponibilidade), a *Port*, o *Username* e a senha do operador. Marque *Verify TLS* e clique em **Fetch TLS Conf** para que a ferramenta busque a cadeia e o certificado TLS do HSM e preencha os campos correspondentes. Use **Test Connection** para validar e clique em **Apply** para salvar (Figura 2).

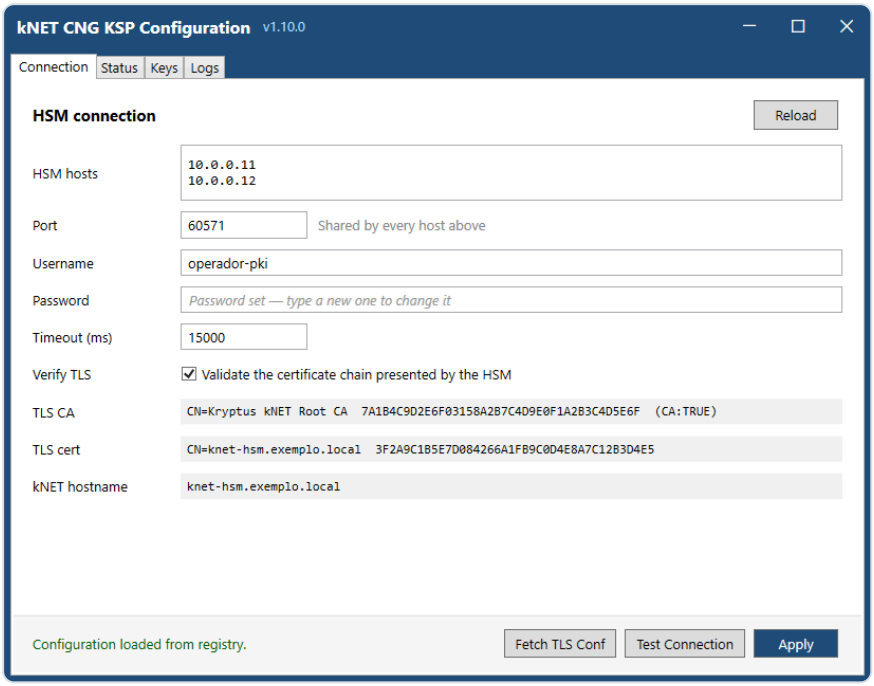

Figura 2. Ferramenta gráfica do KSP: conexão ao HSM, com os campos TLS preenchidos por *Fetch TLS Conf*.

A partir daqui o provedor `kNET Key Storage Provider` fica disponível ao AD CS, incluindo os conjuntos `ML-DSA:44/65/87#kNET Key Storage Provider`.

3.3 Criar a AC pós-quântica no AD CS

Há duas formas de fazer isso, e o resultado é o mesmo nas duas: o **assistente gráfico** e a **linha de comando**. Use a que preferir; em ambas, a chave ML-DSA é gerada e permanece dentro do HSM.

3.3.1 Pela interface gráfica (GUI)

5. Instale a role *Active Directory Certificate Services* (Server Manager → *Add Roles and Features*). Em seguida, pela notificação do Server Manager, abra o **assistente de configuração do AD CS** (*Configure Active Directory Certificate Services*). A primeira página, *Credentials*, confirma a conta administrativa que executará a configuração (Figura 3). Em seguida, na página *Role Services*, marque **Certification Authority** (Figura 4).

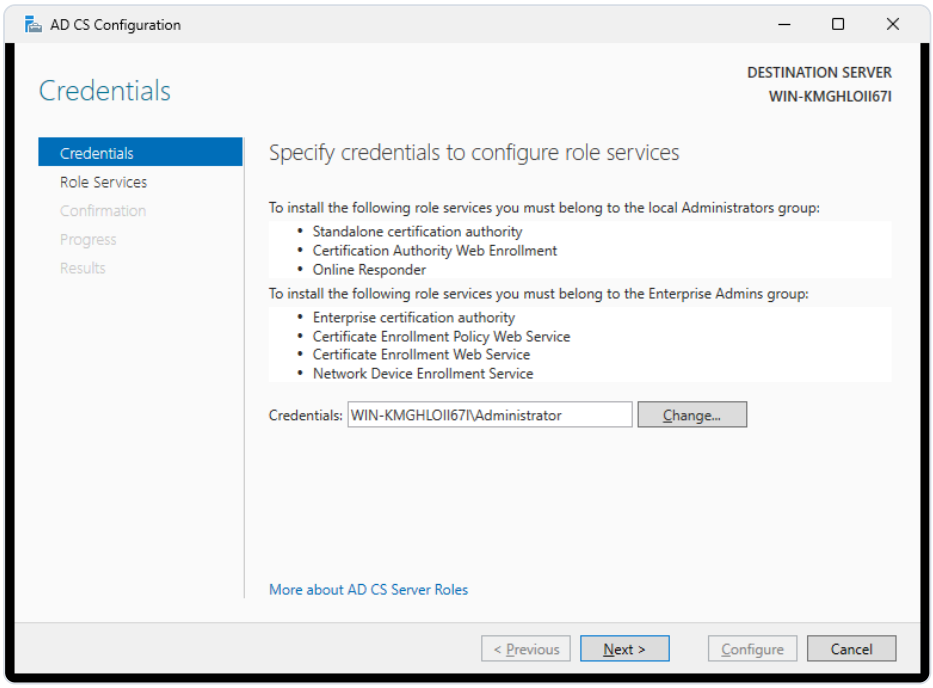

Figura 3. Página *Credentials*: conta administrativa que executa o assistente de configuração.

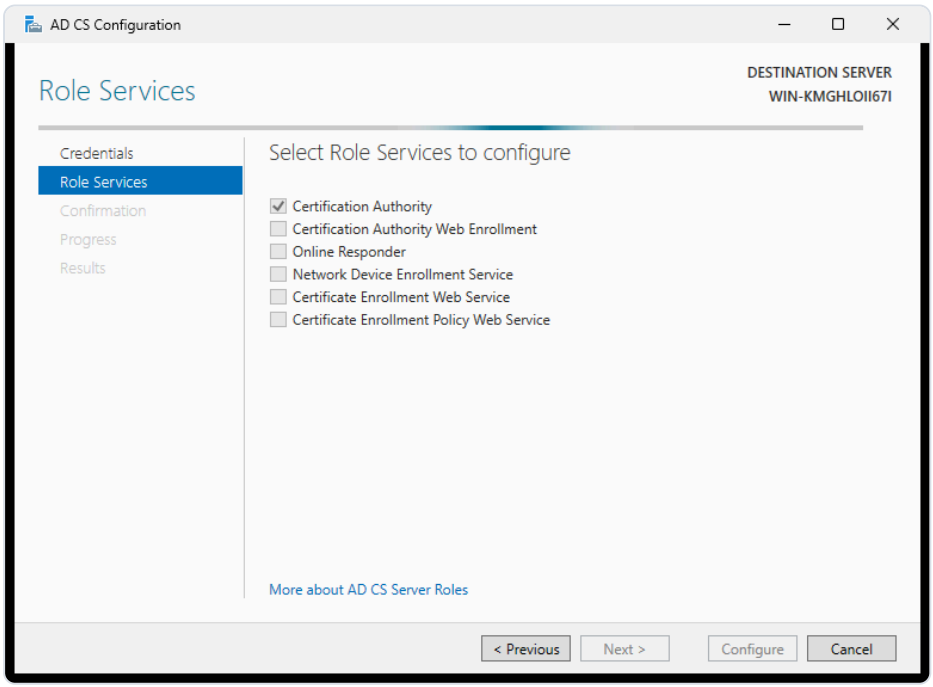

Figura 4. Página *Role Services* com **Certification Authority** selecionada.

6 Em seguida, escolha o tipo e a chave: **Standalone CA** (Figura 5), **Root CA** (Figura 6) e **Create a new private key** (Figura 7).

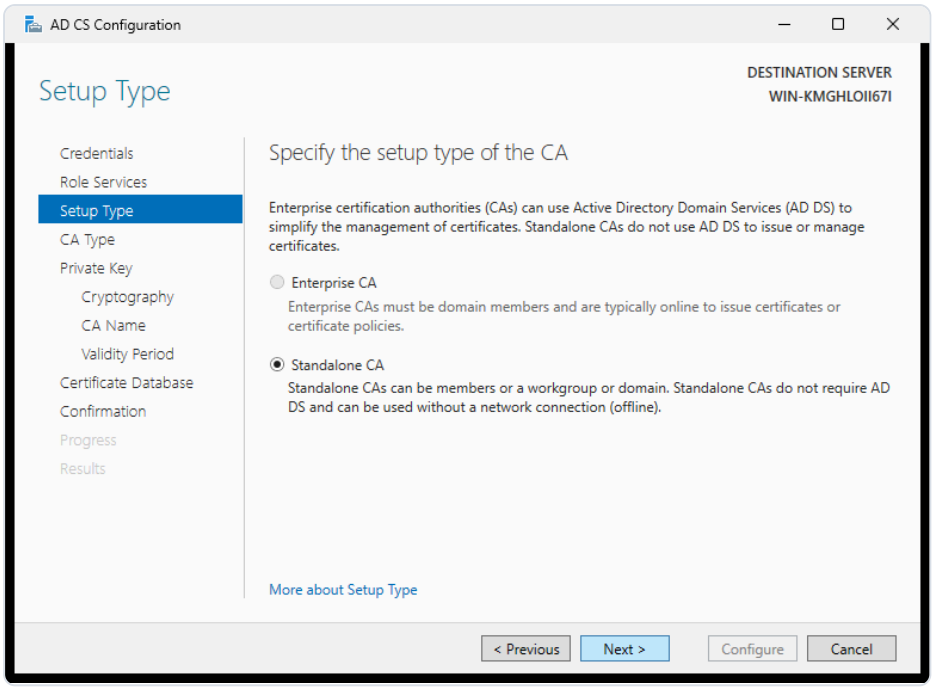

Figura 5. *Setup Type*: **Standalone CA**.

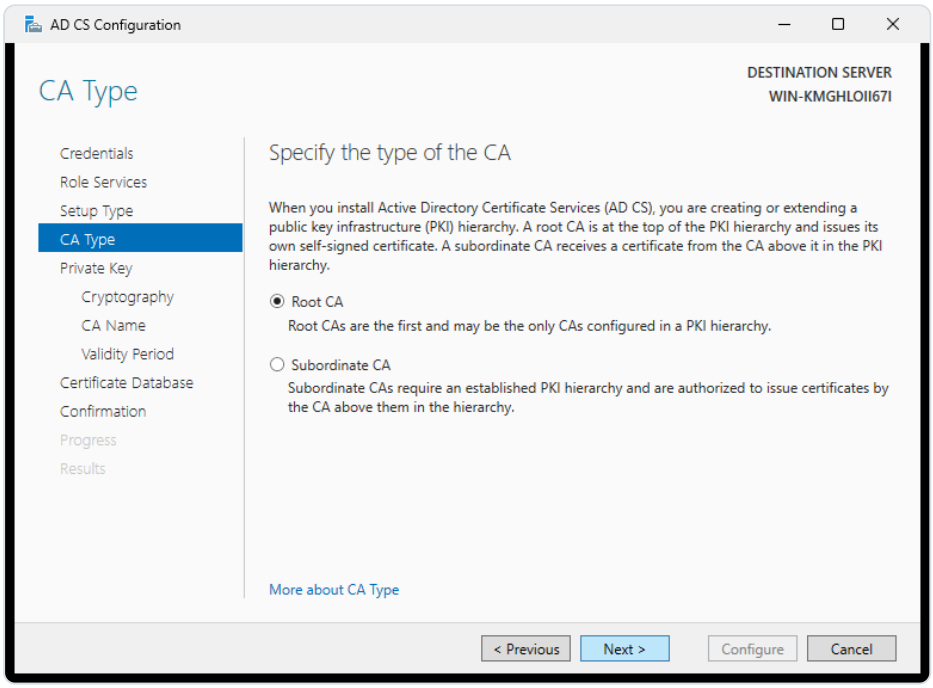

Figura 6. *CA Type*: **Root CA**.

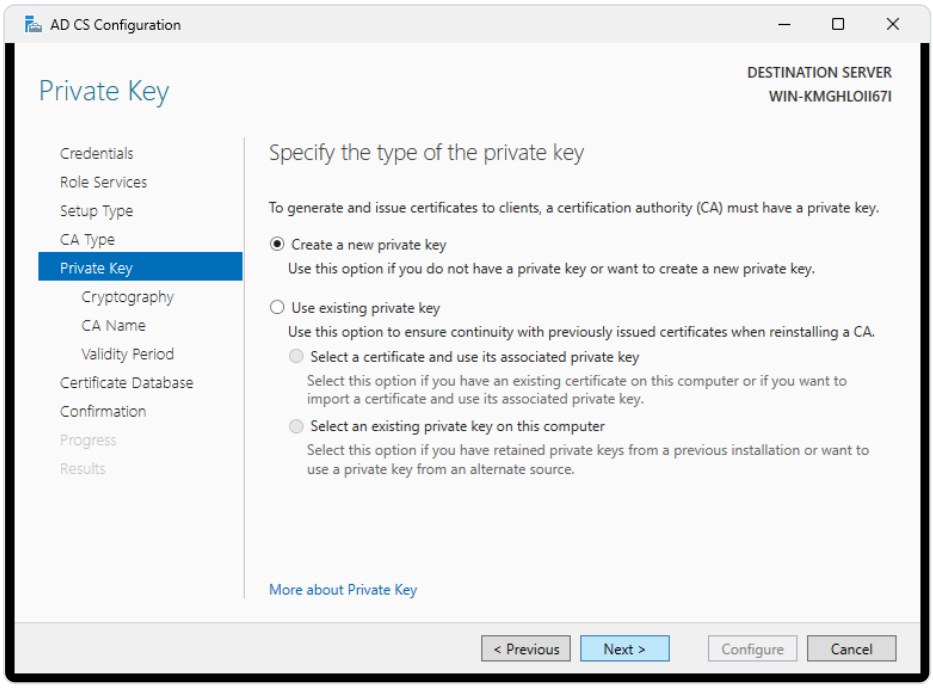

Figura 7. *Private Key*: **Create a new private key**.

7 Na página *Cryptography for CA*, abra a lista de provedores: o KSP da Kryptus publica os conjuntos ML-DSA (além de RSA/ECDSA/Brainpool/DSA).

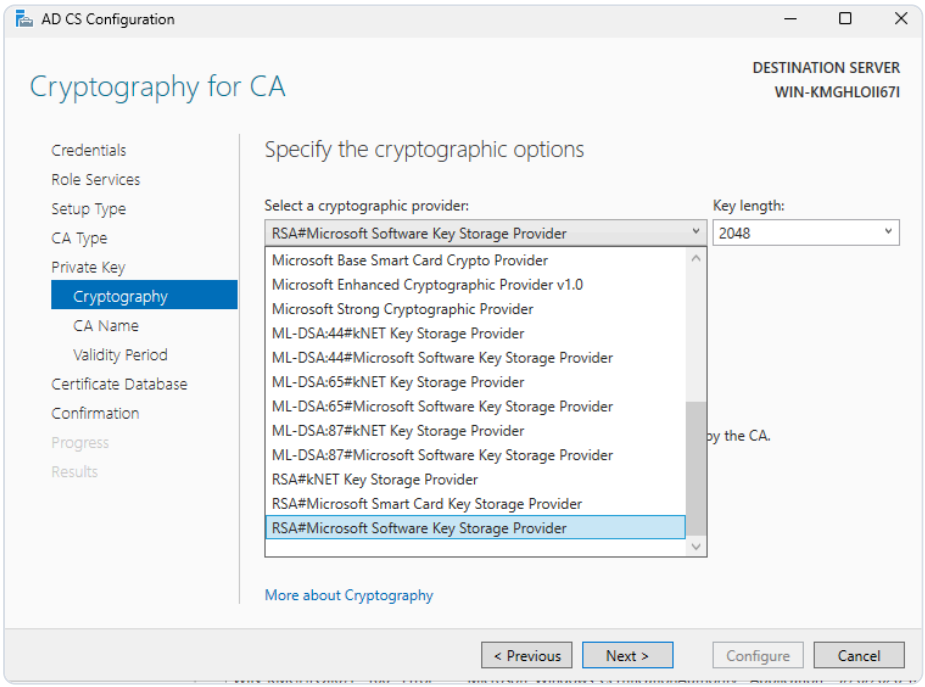

Figura 8. Lista de provedores criptográficos: `ML-DSA:44/65/87#kNET Key Storage Provider` ofertados à AC.

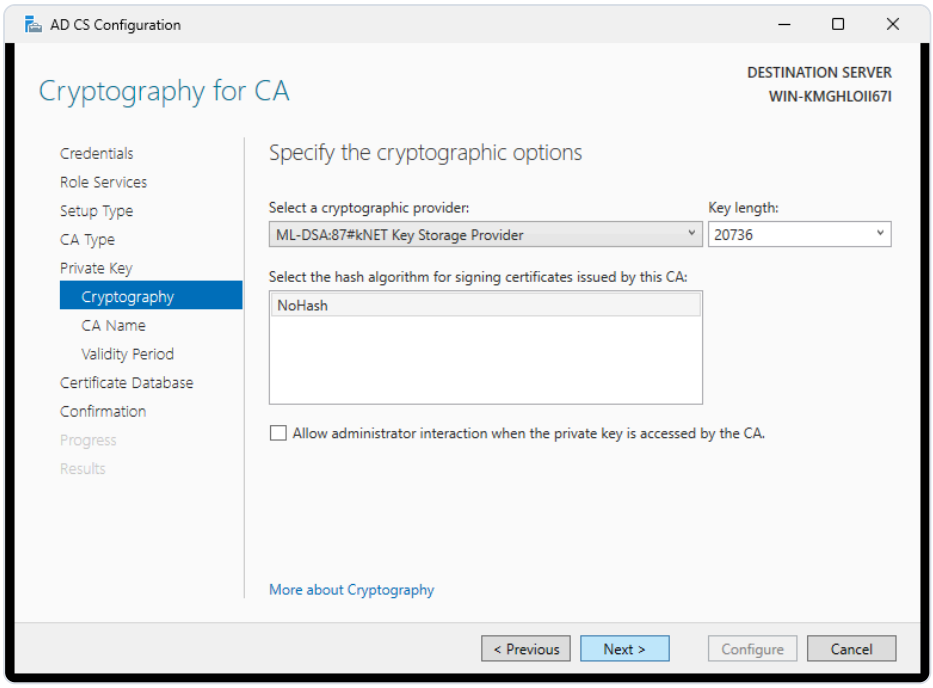

Figura 9. `ML-DSA:87#kNET Key Storage Provider` selecionado.

8. Defina o nome da AC (Figura 10), o período de validade do seu certificado (Figura 11) e a localização da base de dados e dos logs (Figura 12 — use os caminhos padrão a menos que sua política exija outro disco/volume).

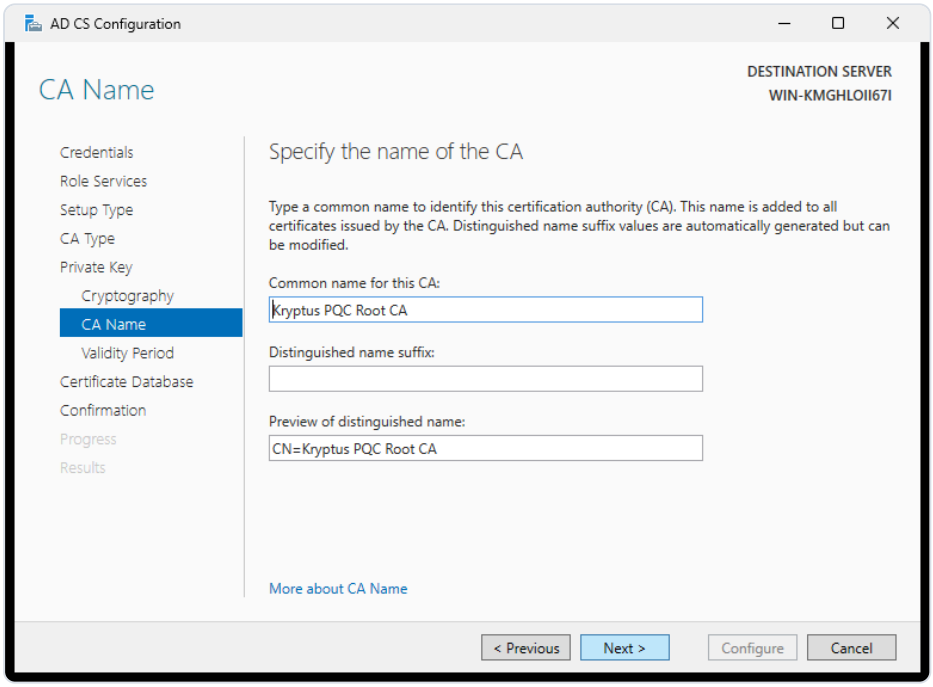

Figura 10. Nome comum da AC.

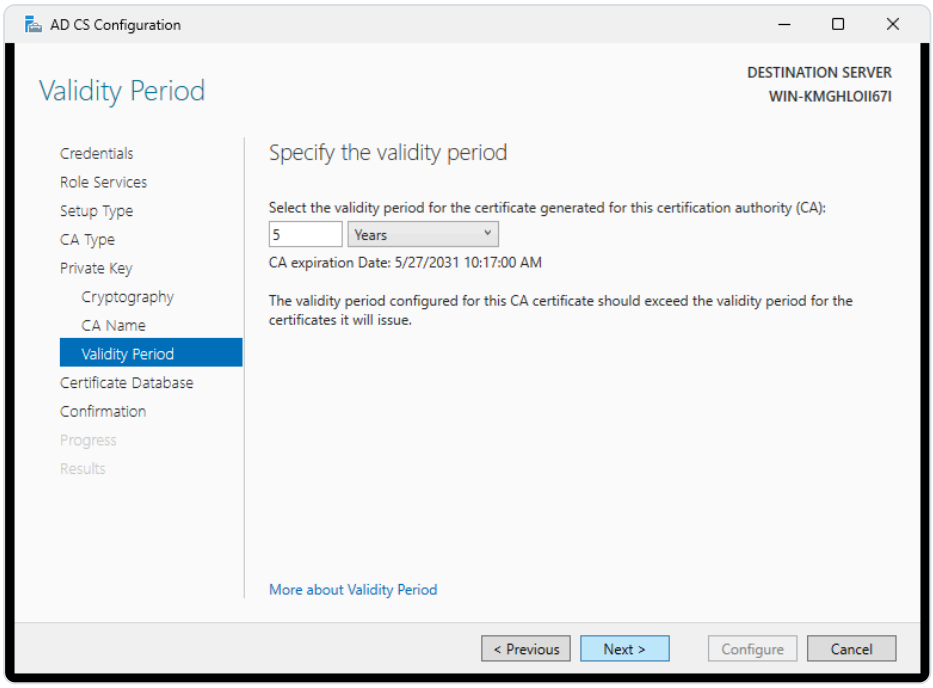

Figura 11. Período de validade do certificado da AC.

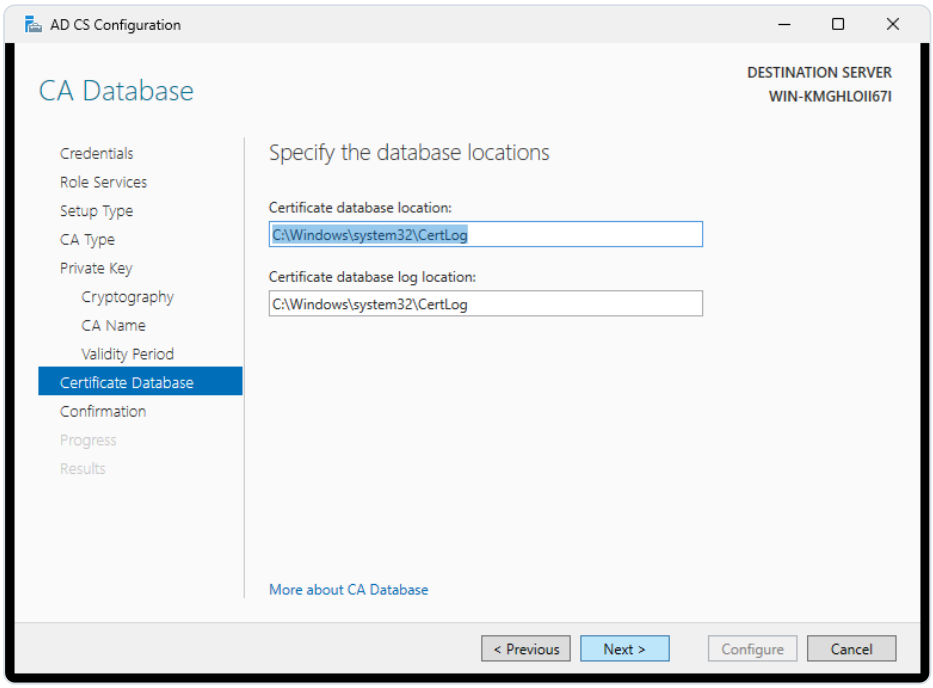

Figura 12. Página *Certificate Database*: localização da base e dos logs da AC.

9 Revise as configurações e clique em **Configure**: a chave ML-DSA é gerada no HSM e o certificado autoassinado da AC é produzido com ela (Figuras 13 e 14).

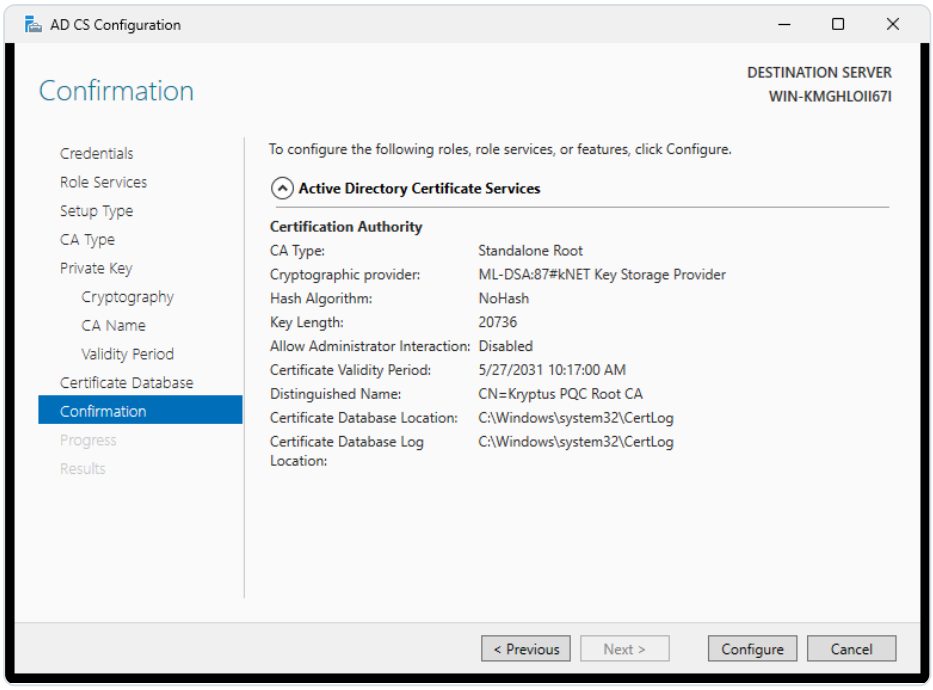

Figura 13. Revisão das configurações antes de criar a AC.

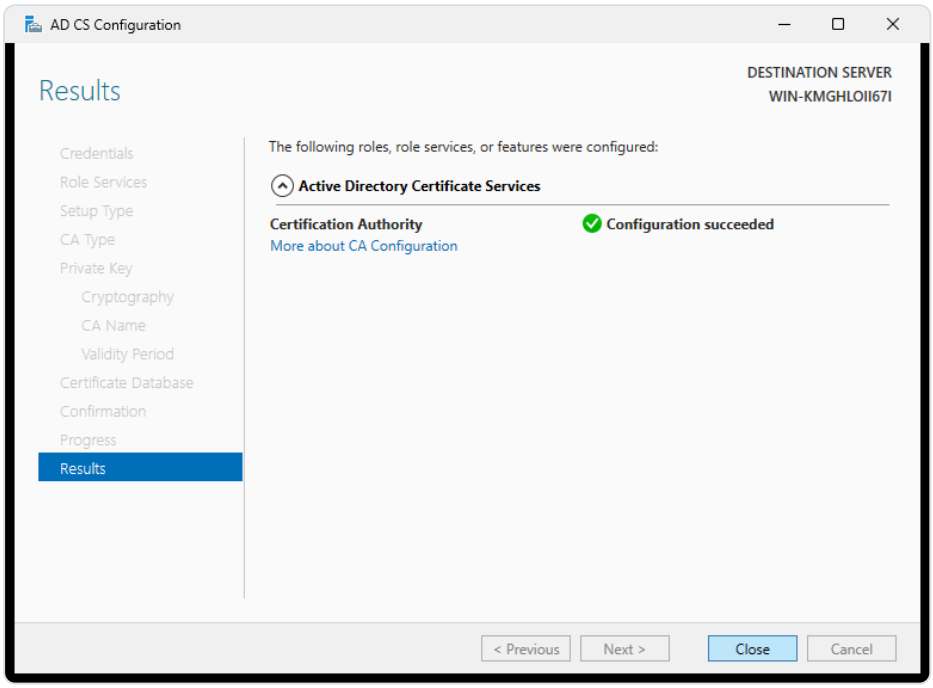

Figura 14. AC criada com sucesso.

10 Abra o console da Autoridade Certificadora (`certsrv.msc` ou *Server Manager → Tools → Certification Authority*) para confirmar que a AC está **em execução** (Figura 15). Para inspecionar o certificado emitido para a própria AC e o algoritmo usado, clique com o botão direito no nó da AC → *Properties → View Certificate → aba Details*: os campos *Signature algorithm* e *Public key* exibem **ML-DSA-87** (Figura 16).

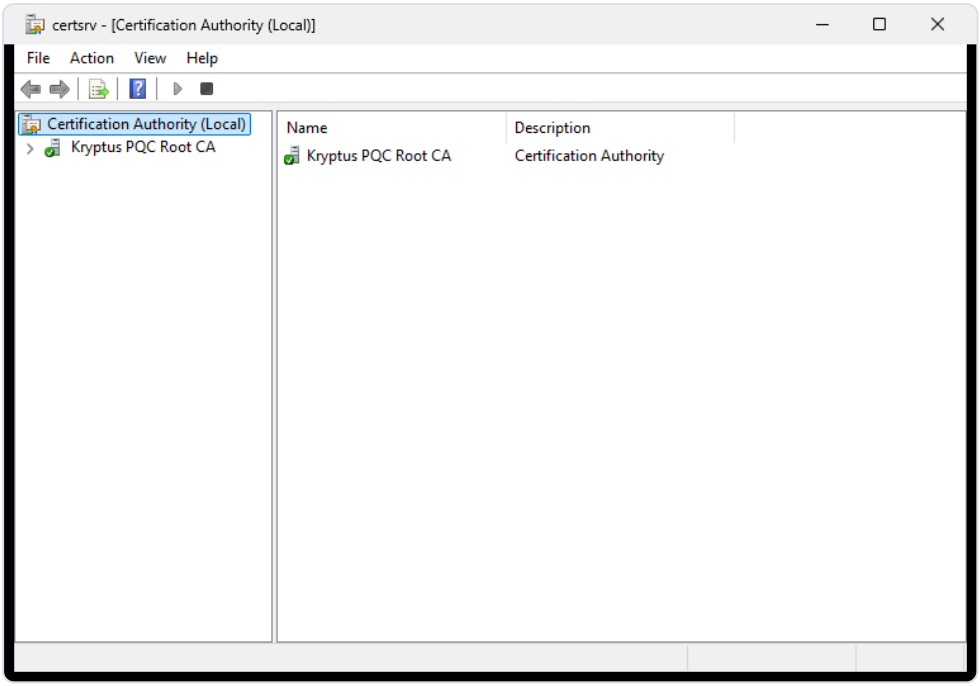

Figura 15. `certsrv.msc` : a AC *Kryptus PQC Root CA* em execução.

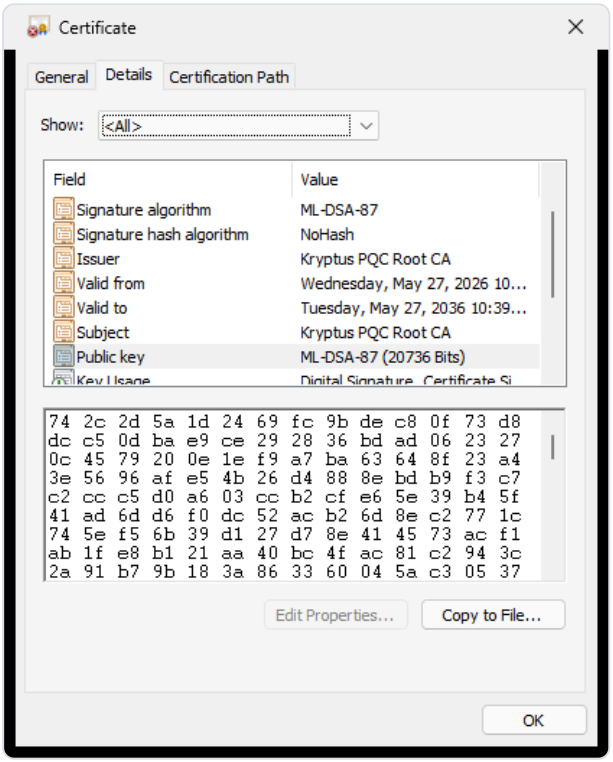

Figura 16. Detalhes do certificado da AC: *Signature algorithm* e *Public key* em **ML-DSA-87** (20736 bits).

11 Verifique que a chave de assinatura da AC reside no HSM:

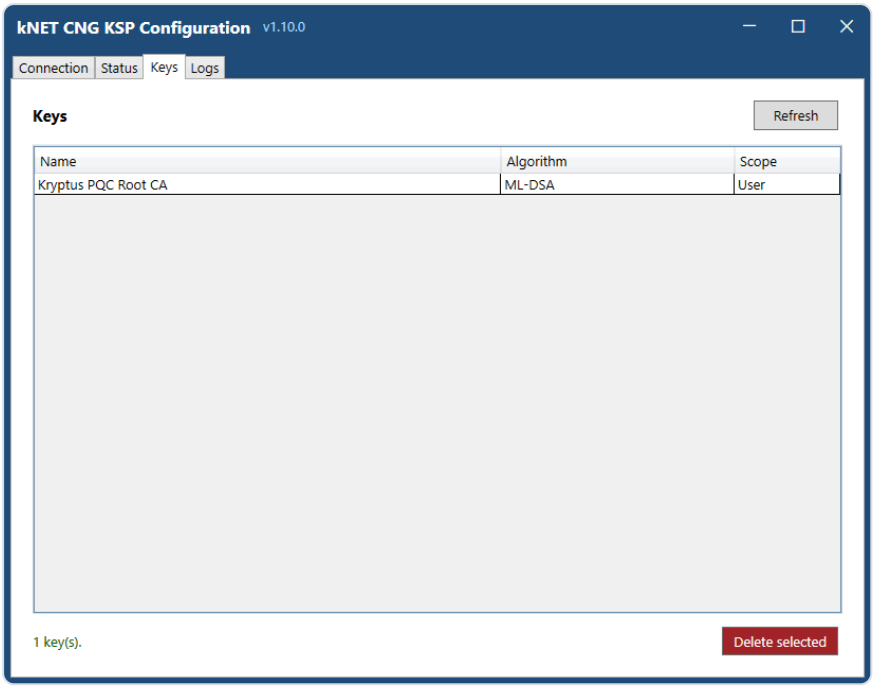

Figura 17. A chave da AC listada no HSM pela ferramenta do KSP.

3.3.2 Pela linha de comando (CLI)

A criação da AC também pode ser feita por linha de comando. Os blocos a seguir reproduzem a saída real dos comandos executados em laboratório (resumida nos trechos mais longos); o nome do servidor foi anonimizado como `<server-name>`.

5 Criar a AC ML-DSA-87.

```
PS> Install-AdcsCertificationAuthority `
      -CAType             StandaloneRootCA `
      -CACommonName       "Kryptus PQC Root CA" `
      -CryptoProviderName "ML-DSA:87#kNET Key Storage Provider" `
      -HashAlgorithmName  NoHash -KeyLength 20736 `
      -ValidityPeriod     Years -ValidityPeriodUnits 10 -Force

ErrorId ErrorString
------- -----------
      0          # ErrorId 0: instalação concluída com sucesso
```

6 Confirmar a AC e o algoritmo ML-DSA-87.

```
PS> certutil -CAInfo
CA name: Kryptus PQC Root CA
CA type: 3 -- Stand-alone Root CA
    ENUM_STANDALONE_ROOTCA -- 3
CA cert[0]: 3 -- Valid
CRL[0]: 3 -- Valid
DNS Name: <server-name>
CertUtil: -CAInfo command completed successfully.

PS> certutil -dump ca.cer          # ca.cer = certificado exportado da AC
Signature Algorithm:
    Algorithm ObjectId: 2.16.840.1.101.3.4.3.19 ML-DSA-87
Public Key Algorithm:
    Algorithm ObjectId: 2.16.840.1.101.3.4.3.19 ML-DSA-87
Public Key Length: 20736 bits
```

3.4 Emitir, revogar e publicar certificados (LCR)

Com a AC pronta, o ciclo de vida dos certificados (emissão, revogação e publicação de LCR) pode ser conduzido pela interface gráfica ou pela linha de comando. Em ambos os caminhos, a chave da folha é gerada e permanece dentro do HSM, e todas as assinaturas (certificado e LCR) usam a chave ML-DSA da AC no hardware.

3.4.1 Pela interface gráfica (GUI)

O fluxo completo pela GUI: gerar a requisição com a chave no HSM (snap-in *Certificates*, passos 1 a 6) e operar o ciclo de vida no console da AC (`certsrv.msc` , passos 7 a 11).

1 No snap-in *Certificates* (`certmgr.msc` para o usuário ou `certlm.msc` para a máquina), clique com o botão direito em *Personal* → *All Tasks* → *Advanced Operations* → *Create Custom Request* (Figura 18).

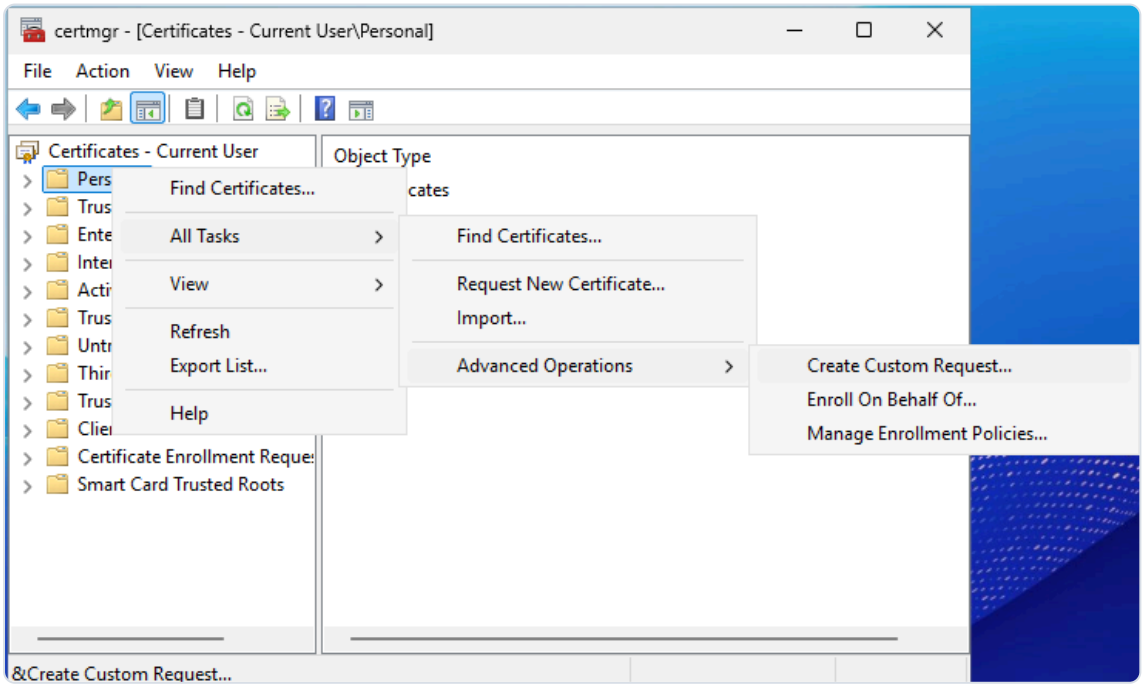

Figura 18. Início do pedido em *Personal* → *All Tasks* → *Advanced Operations* → *Create Custom Request*.

2. Em *Select Certificate Enrollment Policy*, escolha **Proceed without enrollment policy** (requisição custom, sem política do AD) (Figura 19).

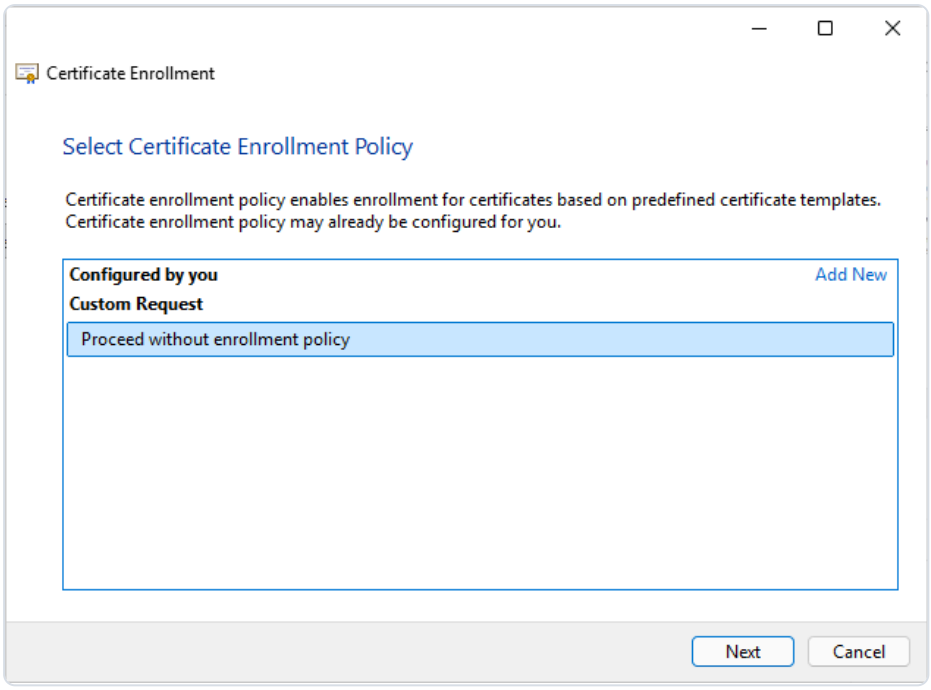

Figura 19. *Custom Request*: **Proceed without enrollment policy**.

3. Em *Custom request*, selecione o template **"(No template) CNG key"** e o formato **PKCS #10** (Figura 20). O KSP é um provedor CNG, então a opção precisa ser *CNG key*, não *Legacy key*.

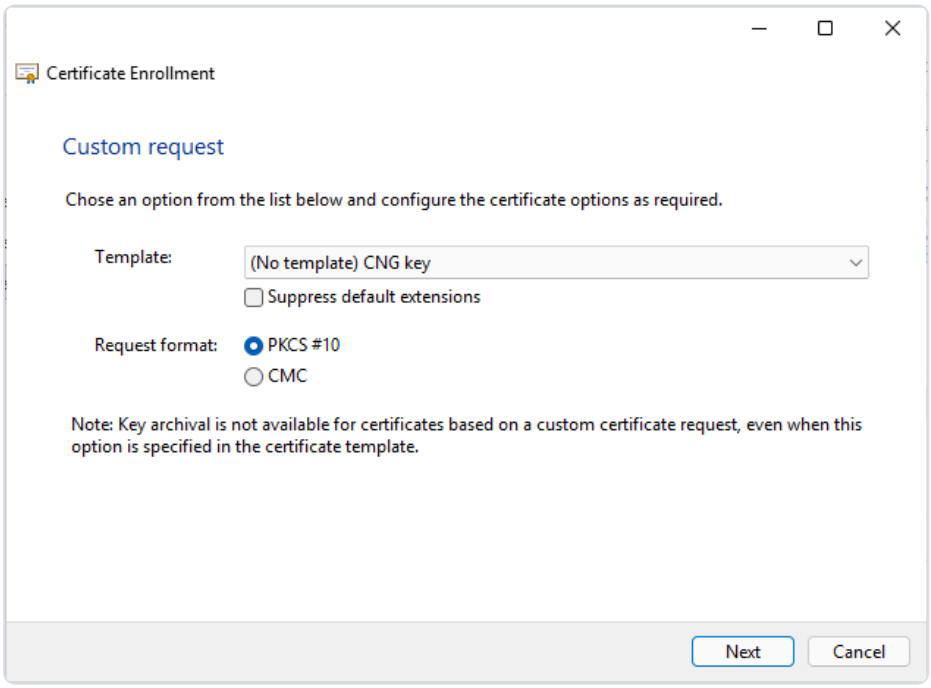

Figura 20. Template **(No template) CNG key** e formato **PKCS #10**.

4. A tela *Certificate Information* resume o pedido; clique em *Details* → *Properties* para configurá-lo (Figura 21). Na aba *Subject*, informe o titular (ex.: `CN=...`) (Figura 22); na aba *Extensions*, ajuste o *Key usage* (ex.: *Digital signature*) (Figura 23).

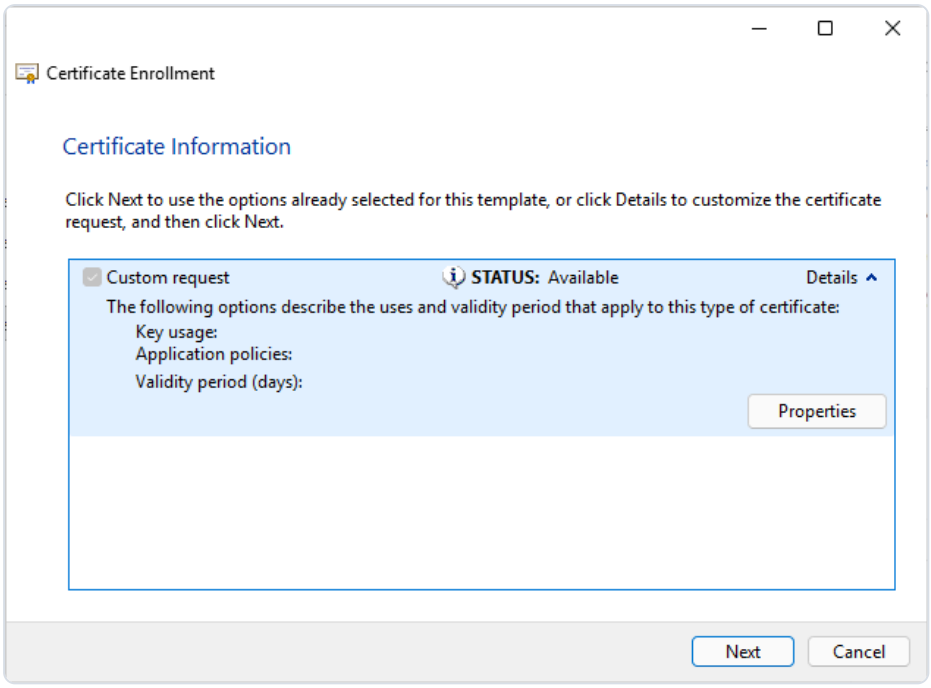

Figura 21. *Certificate Information* antes de configurar: clique em *Details* → *Properties*.

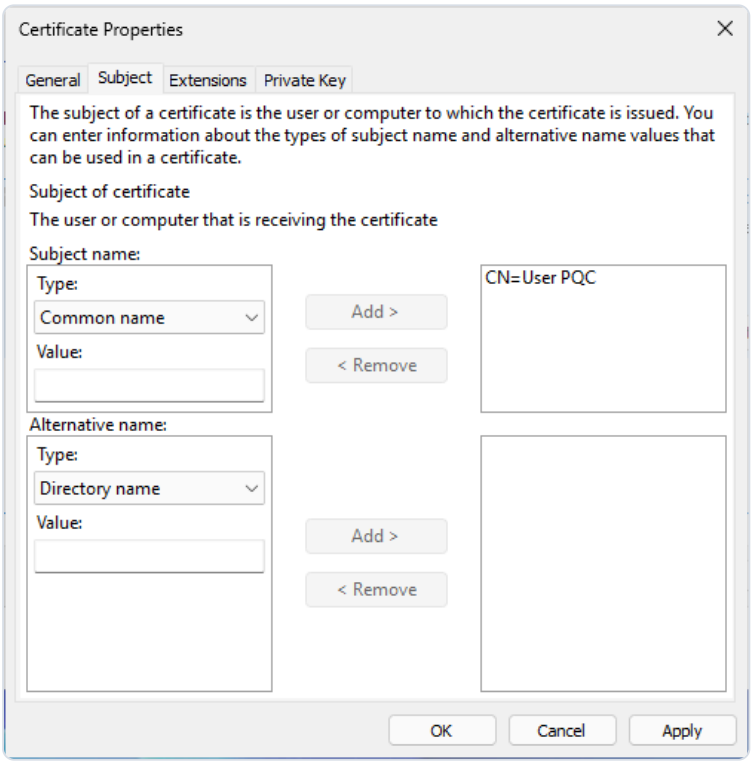

Figura 22. Aba *Subject*: nome do titular do certificado.

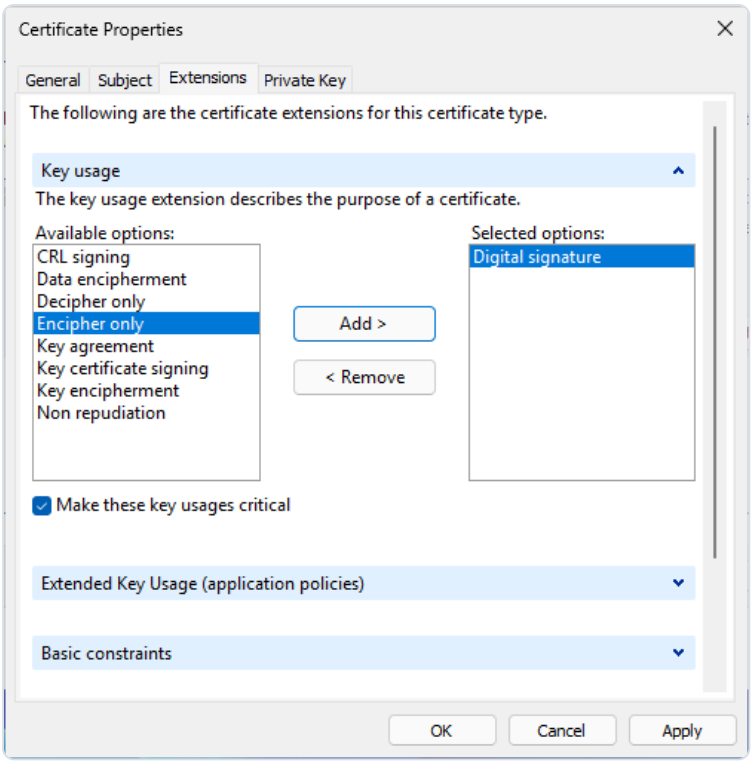

Figura 23. Aba *Extensions*: *Key usage* do certificado (ex.: *Digital signature*).

5 Na aba *Private Key* → *Cryptographic Service Provider*, marque o conjunto desejado do **kNET Key Storage Provider**, por exemplo `ML-DSA:65, kNET Key Storage Provider` (Figura 24). É essa escolha que faz o par de chaves **nascer dentro do HSM**.

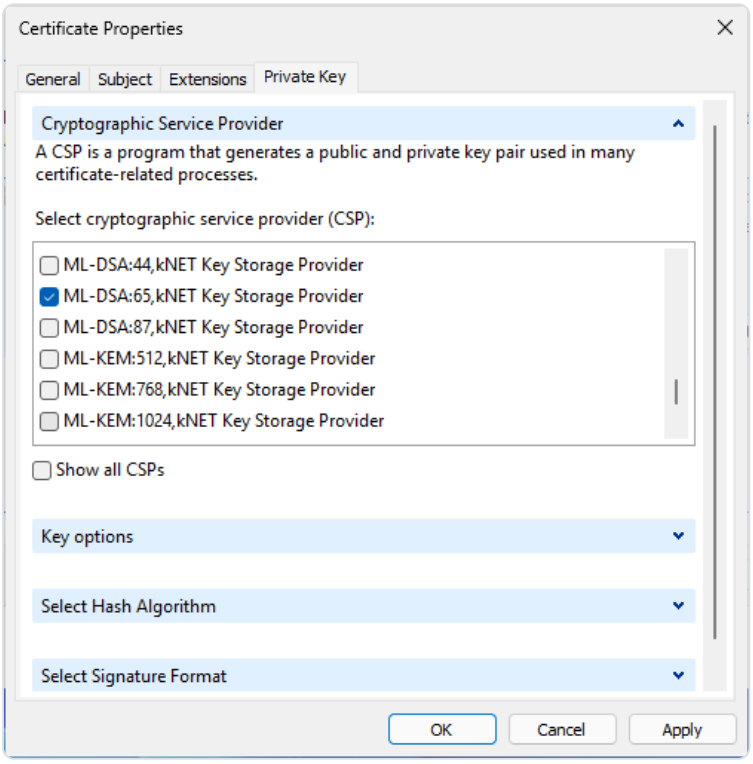

Figura 24. Provedor `ML-DSA:65, kNET Key Storage Provider` selecionado: a chave é gerada no HSM.

6 De volta à tela *Certificate Information*, agora com as opções aplicadas (Figura 25), conclua salvando a requisição (`.req`) em **Base 64** (Figura 26). A chave privada já está no HSM; o arquivo carrega apenas o pedido (CSR).

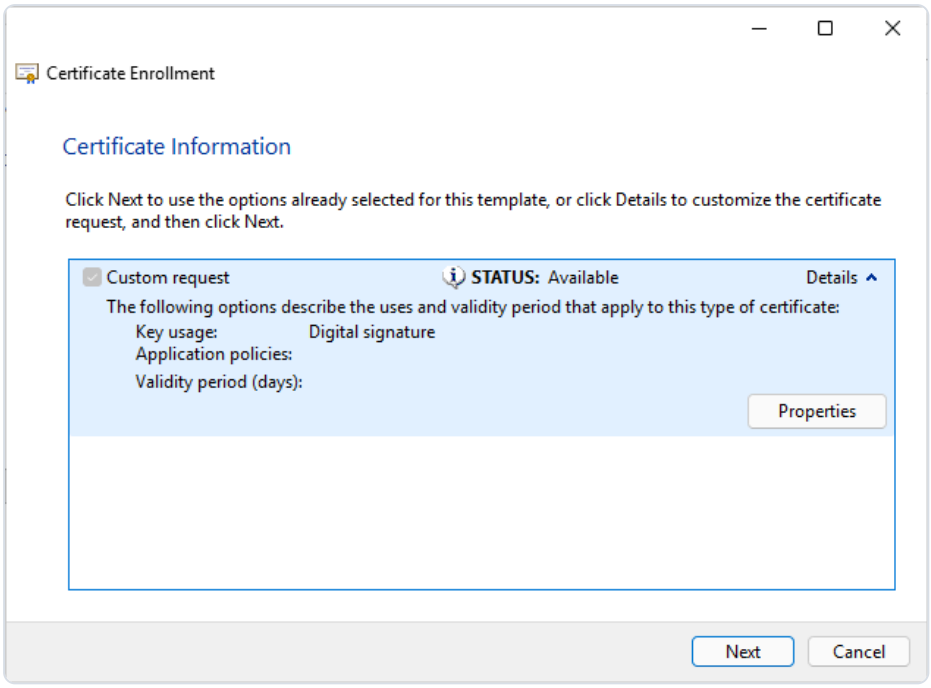

Figura 25. *Certificate Information* após a configuração do pedido.

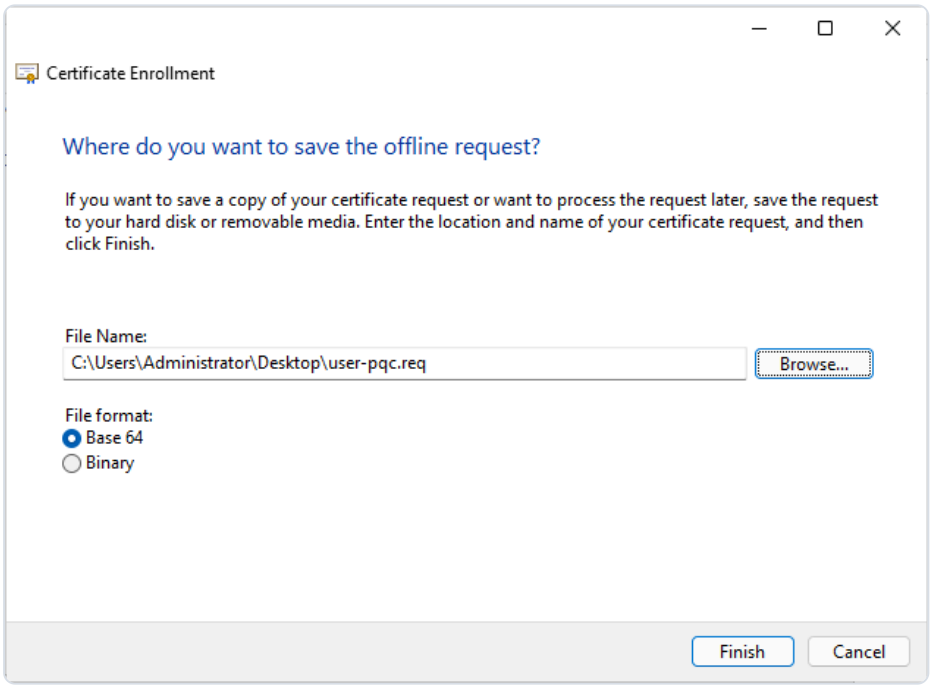

Figura 26. Requisição salva em **Base 64** (`.req`).

7 No console da AC (`certsrv.msc`), botão direito no nó da AC → *All Tasks* → *Submit new request* e selecione o `.req` (Figura 27). Numa AC *standalone*, o pedido entra como pendente.

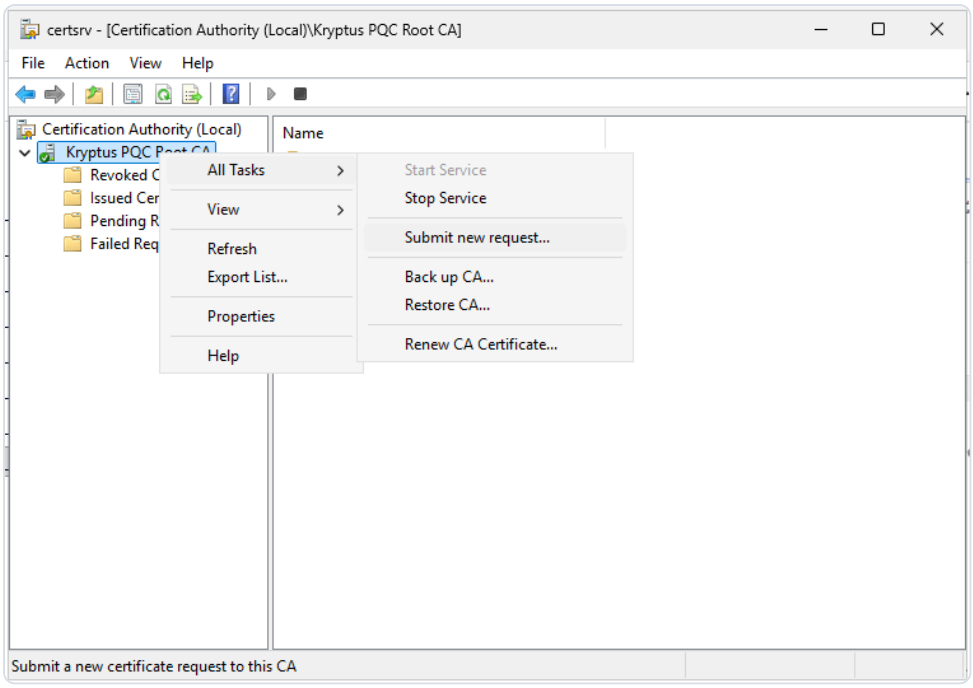

Figura 27. *All Tasks → Submit new request*: envio do CSR à AC.

8 Em *Pending Requests*, botão direito no pedido → *All Tasks* → *Issue* para emitir (Figura 28). O certificado passa para *Issued Certificates*, de onde pode ser exportado e inspecionado: a folha emitida tem chave pública **ML-DSA-65** e foi assinada pela AC com **ML-DSA-87** (Figura 29).

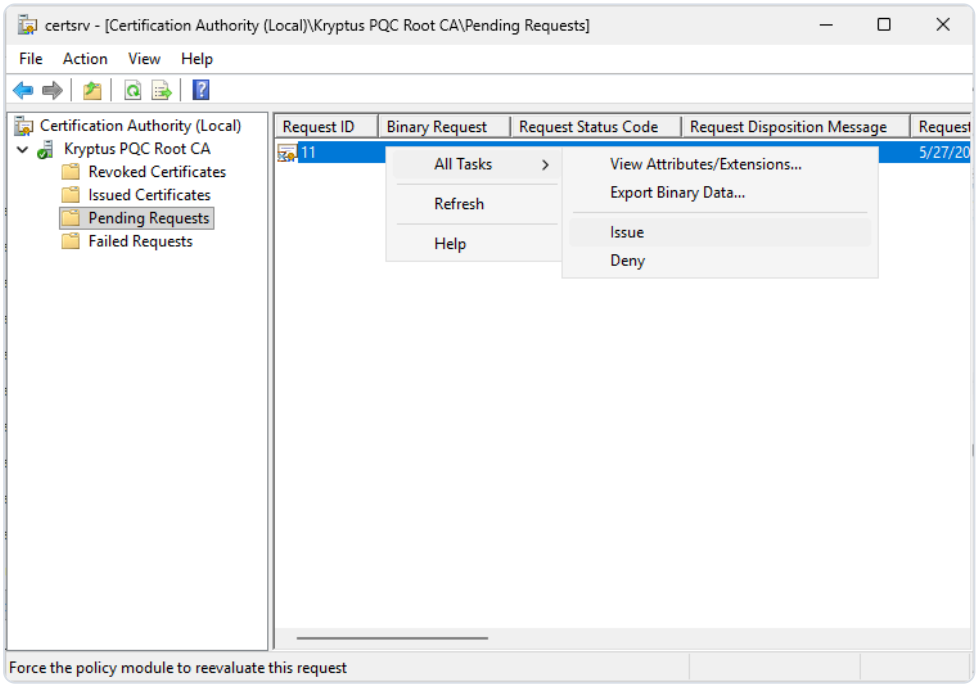

Figura 28. Aprovação do pedido pendente em *All Tasks → Issue*.

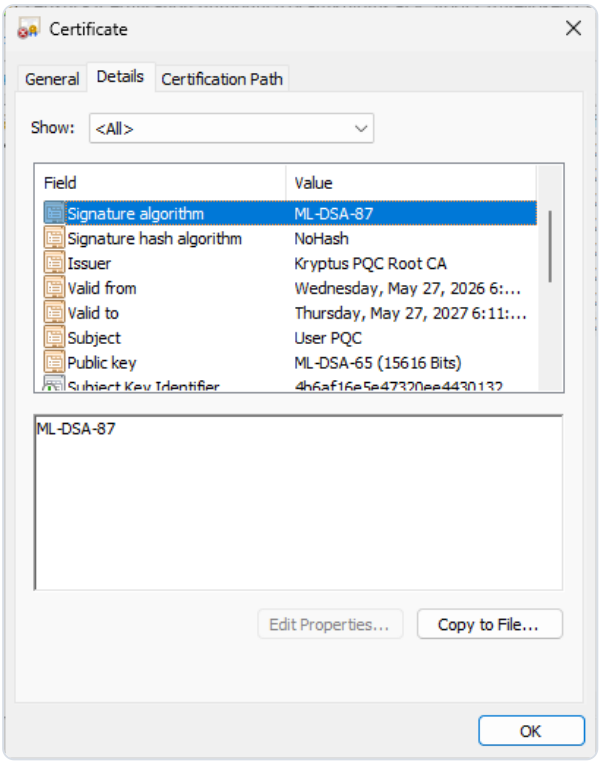

Figura 29. Certificado emitido: *Public key* **ML-DSA-65** e *Signature algorithm* **ML-DSA-87**.

9 Para **revogar**, em *Issued Certificates*, botão direito no certificado → *All Tasks* → *Revoke Certificate* (Figura 30); escolha o motivo e confirme (Figura 31).

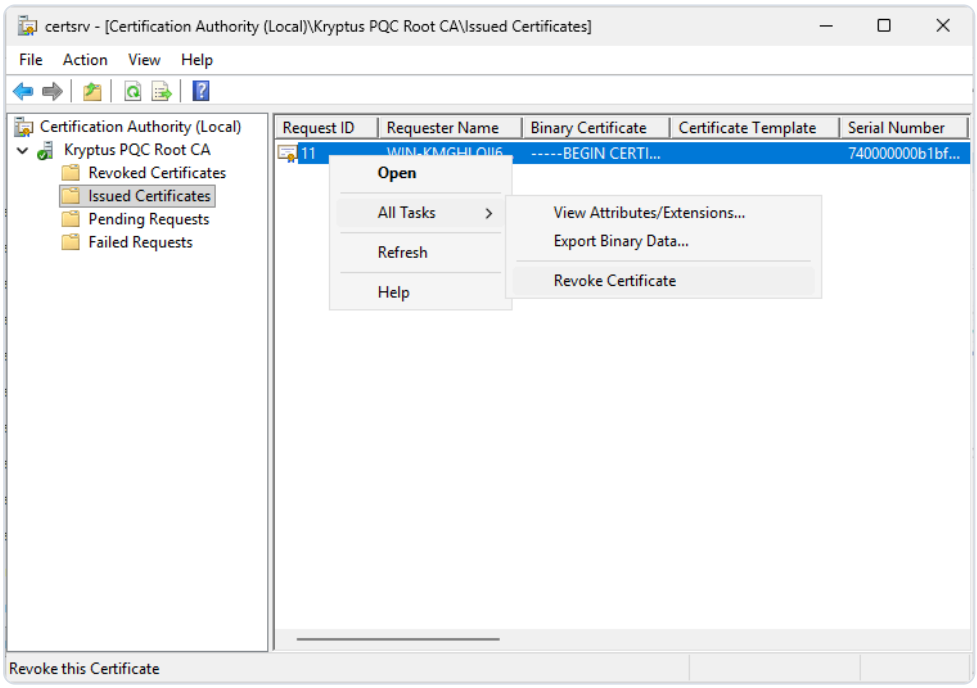

Figura 30. *All Tasks → Revoke Certificate.*

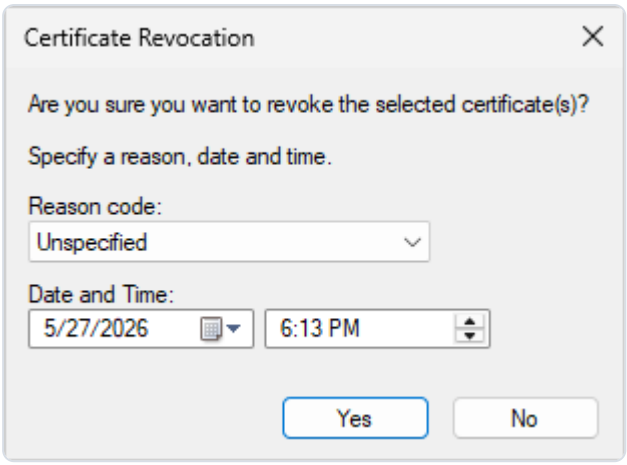

Figura 31. Diálogo de revogação: *Reason code* e data/hora.

10 Para **publicar a LCR**, em *Revoked Certificates*, botão direito → *All Tasks* → *Publish* (Figura 32) e escolha **New CRL** (Figura 33).

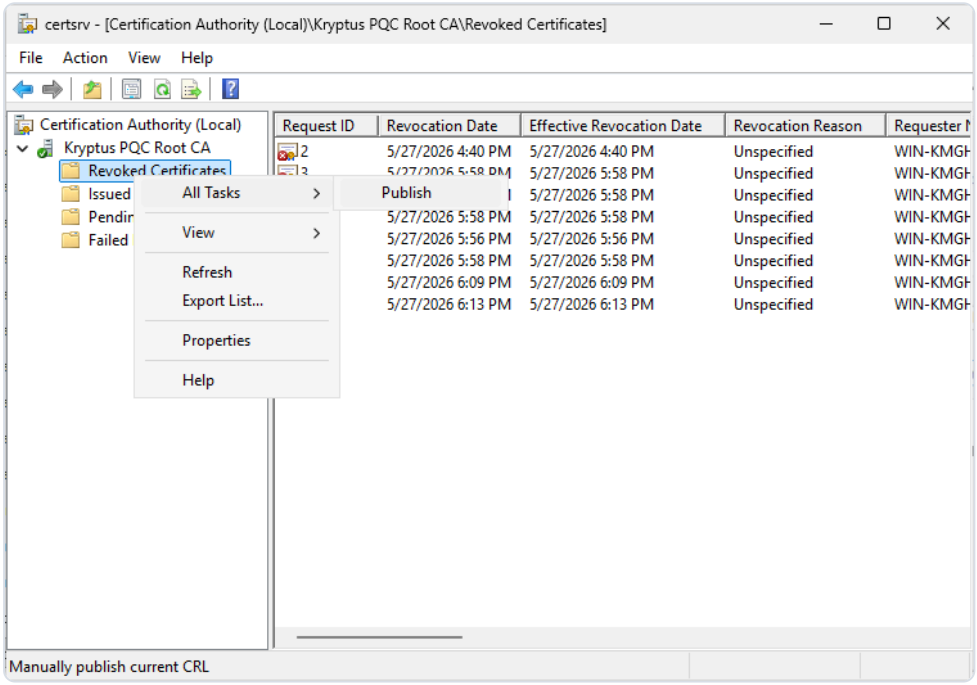

Figura 32. *All Tasks* → *Publish*: geração de nova LCR.

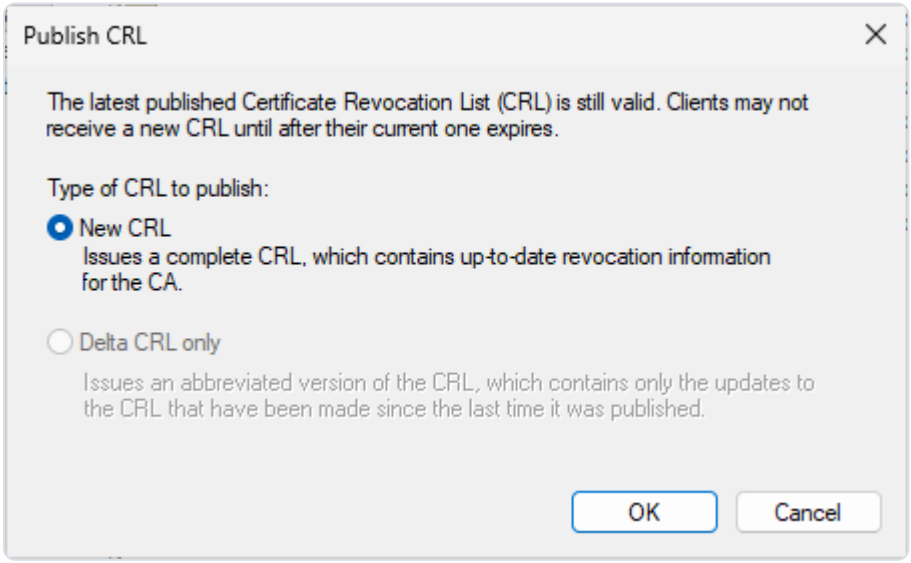

Figura 33. *Publish CRL*: **New CRL**.

11 A LCR também é assinada com a chave ML-DSA da AC. Em *Revoked Certificates → Properties → View CRLs → View CRL*, o campo *Signature algorithm* exibe **ML-DSA-87** (Figura 34).

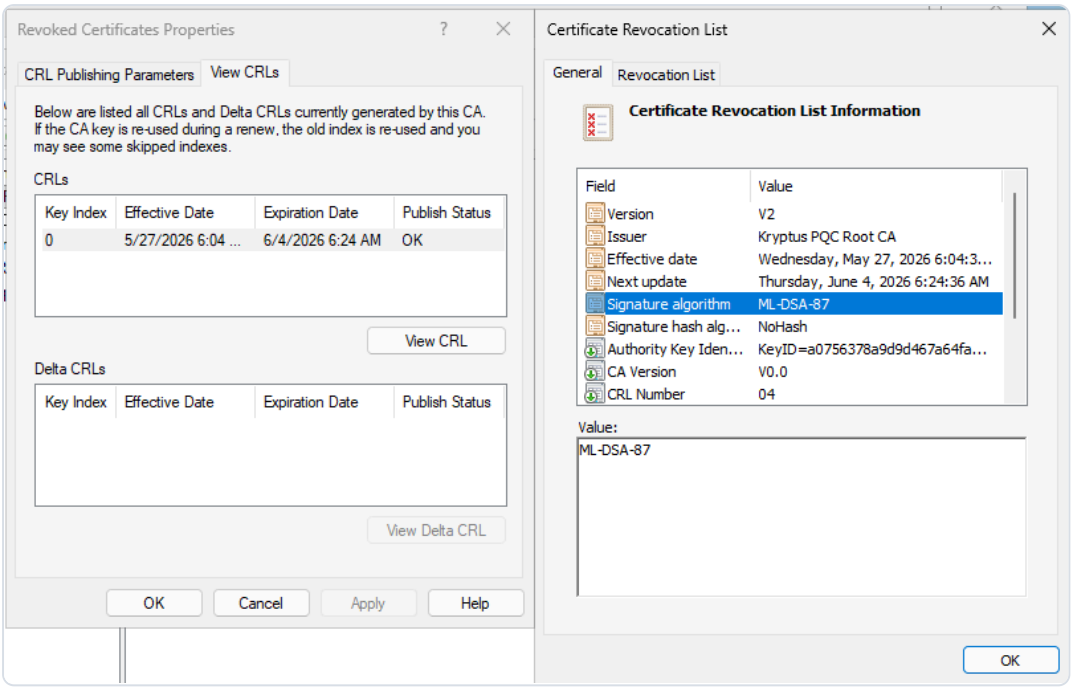

Figura 34. Detalhes da LCR: *Signature algorithm* em **ML-DSA-87**.

3.4.2 Pela linha de comando (CLI)

As mesmas operações por linha de comando (saída real, resumida nos trechos mais longos; servidor anonimizado como `<server-name>`):

1 Emitir um certificado (folha ML-DSA-65).

```
# leaf.inf: solicitação de uma folha pós-quântica no HSM
[NewRequest]
Subject      = "CN=pqc-server.exemplo.local"
RequestType  = PKCS10
ProviderName = "kNET Key Storage Provider"
KeyAlgorithm = ML-DSA-65
MachineKeySet = TRUE
KeyUsage     = 0x80

PS> certreq -q -new -f leaf.inf leaf.req
CertReq: Request Created
PS> certreq -q -config "<server-name>\Kryptus PQC Root CA" -submit leaf.req leaf.cer
RequestId: 2
RequestId: "2"
Certificate request is pending: Taken Under Submission (0)
PS> certutil -resubmit 2                # o operador da AC aprova
Certificate issued.
CertUtil: -resubmit command completed successfully.
PS> certreq -q -config "<server-name>\Kryptus PQC Root CA" -retrieve 2 leaf.cer
RequestId: 2
RequestId: "2"
Certificate retrieved(Issued) Issued  Resubmitted by <server-name>\Administrator
```

O certificado emitido forma uma **cadeia 100% pós-quântica**: chave da folha ML-DSA-65, assinada pela AC com ML-DSA-87.

```
PS> certutil -dump leaf.cer
Serial Number: 740000000234fa2471b0af215a000000000002
Signature Algorithm:
    Algorithm ObjectId: 2.16.840.1.101.3.4.3.19 ML-DSA-87
Issuer:
    CN=Kryptus PQC Root CA
Subject:
    CN=pqc-server.exemplo.local
Public Key Algorithm:
    Algorithm ObjectId: 2.16.840.1.101.3.4.3.18 ML-DSA-65
Public Key Length: 15616 bits
```

2. Revogar e publicar a LCR (CRL).

```
PS> certutil -revoke 740000000234fa2471b0af215a000000000002
Revoking "740000000234fa2471b0af215a000000000002" -- Reason: Unspecified
CertUtil: -revoke command completed successfully.
PS> certutil -CRL
CertUtil: -CRL command completed successfully.  # LCR assinada com ML-DSA-87
```

3. Verificar a cadeia e a revogação.

```
PS> certutil -verify leaf.cer
ChainContext.dwErrorStatus = CERT_TRUST_IS_REVOKED (0x4)

CertContext[0][0]: dwInfoStatus=102 dwErrorStatus=4
  Issuer: CN=Kryptus PQC Root CA
  Subject: CN=pqc-server.exemplo.local
  Serial: 740000000234fa2471b0af215a000000000002
  Element.dwErrorStatus = CERT_TRUST_IS_REVOKED (0x4)
    CRL 03:
    Issuer: CN=Kryptus PQC Root CA

CertContext[0][1]: dwInfoStatus=10c dwErrorStatus=0
  Subject: CN=Kryptus PQC Root CA   # raiz autoassinada ML-DSA-87
  Element.dwInfoStatus = CERT_TRUST_IS_SELF_SIGNED (0x8)

The certificate is revoked. 0x80092010 (-2146885616 CRYPT_E_REVOKED)
Leaf certificate is REVOKED (Reason=0)
CertUtil: -verify command completed successfully.
```

4. Considerações Finais

Computadores quânticos criptograficamente relevantes ameaçam os algoritmos assimétricos clássicos (RSA, ECDSA, Diffie-Hellman). O risco é imediato mesmo antes de tais máquinas existirem, por causa do ataque "harvest now, decrypt later": dados e assinaturas capturados hoje podem ser quebrados no futuro. Por isso a migração precisa começar agora.

Esse movimento é coordenado por governos. Nos EUA, o NIST publicou os padrões (FIPS 203/204/205) e a NSA, pela suíte **CNSA 2.0**, exige criptografia pós-quântica nos Sistemas de Segurança Nacional, com transição preferencial até 2030-2033 e plena até **2035**. A Casa Branca (NSM-10) e o OMB orientam as agências federais a migrar no mesmo horizonte. Na Europa, a Comissão Europeia recomendou, em 2024, que os Estados-membros adotem um **roteiro coordenado** de transição para a PQC, favorecendo esquemas híbridos e com metas em torno de 2030 para sistemas de alto risco e 2035 de forma ampla, apoiada por guias nacionais como os do BSI (Alemanha) e da ANSSI (França). A mensagem é convergente: planejar e iniciar a migração agora.

A transição pós-quântica saiu do plano teórico e chegou à PKI corporativa do Windows. Com a KB5087539 e o provedor CNG da Kryptus, é possível, **hoje**, operar uma Autoridade Certificadora ML-DSA com a chave de assinatura protegida no **ASI-HSM AHX5 kNET**, unindo resistência quântica e segurança de hardware. Recomendamos iniciar pelos pilotos de hierarquia paralela e pelo mapeamento dos pontos da sua PKI que precisarão de assinatura pós-quântica.

Referências

1. Microsoft's quantum-resistant cryptography is here (SymCrypt, 2024)
2. Post-Quantum Cryptography Comes to Windows Insiders and Linux (2025)
3. Post-Quantum Cryptography APIs Now Generally Available on Microsoft Platforms
4. What is ML-DSA support in AD CS? (Microsoft Learn)
5. Configure a certification authority to use ML-DSA (Microsoft Learn)
6. Configure certificate templates for ML-DSA (Microsoft Learn)
7. Atualização KB5087539 (12/05/2026, build 26100.32860)
8. NIST FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), agosto de 2024
9. NIST FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA), agosto de 2024
10. NIST FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA), agosto de 2024
11. NIST CAVP: validação da implementação criptográfica do ASI-HSM AHX5 kNET (Kryptus)
12. NSA: Commercial National Security Algorithm Suite 2.0 (CNSA 2.0), transição PQC dos Sistemas de Segurança Nacional dos EUA
13. Comissão Europeia: Recomendação (UE) 2024/1101 sobre um roteiro coordenado de transição para a criptografia pós-quântica (11/04/2024)