Netlock — Content Security & Verification

Netlock Web Application — Requesting the Organisation Authentication Certificate for EESZT

A complete guide: how an organisation obtains in Netlock the organisation authentication certificate it uses to connect to EESZT — from creating the account and the organisation, through the legal representative's verification and power of attorney and the purchase with credits, to downloading the key — and how it replaces its old certificate with it.

Version 1.4 · 2026-11-12

Version history

Version	Date	Author	Changes
1.0	2026-11-09	Zoltán Deák (NETLOCK)	First edition.
1.1	2026-11-11	NETLOCK	Hungarian wording smoothed throughout; the content is unchanged.
1.2	2026-11-11	NETLOCK	Chapter 10: a new item on the deadline for switching (removed in 1.4).
1.3	2026-11-12	NETLOCK	Chapter 10: the switching item reworded; new footer (trust@netlock.com, +36 1 255 0792).
1.4	2026-11-12	NETLOCK	Chapter 10: the item on the deadline for switching is removed because it was wrong. The old system issues no EESZT certificates after 17 November 2026; a certificate that is still valid need not be replaced now, only switched before it expires.

About this document. This guide is self-contained: it holds every step needed to obtain the certificate. It is for the owner or administrator of the organisation who obtains the certificate, for the organisation's legal representative, who verifies their identity and grants the power of attorney on the organisation's behalf, and for the colleague who receives the key and the certificate. It covers payment with credits only. The guide also has a Hungarian edition.

Contents

1. Overview
- 1.1 What this guide covers
- 1.2 What you need
- 1.3 The steps

2. Netlock account and signing in
- 2.1 Creating an account
- 2.2 Setting up a second factor
- 2.3 Signing in

3. Creating the organisation
- 3.1 A new organisation
- 3.2 The setup checklist
- 3.3 Inviting a colleague

4. Entering and verifying the business details
- 4.1 Company data lookup
- 4.2 The verification outcome
- 4.3 The list of legal representatives

5. Legal representative verification and power of attorney
- 5.1 Why it is needed
- 5.2 Involving the legal representative
- 5.3 Starting the video identification
- 5.4 The video identification steps
- 5.5 Granting the power of attorney
- 5.6 Enabling organisational certificates
- 5.7 Authorisation status and deadlines

6. Written power of attorney when the legal representative cannot complete video identification

7. Buying credits and the certificate
- 7.1 Buying credits for the organisation
- 7.2 Buying the certificate with credits

8. Allowing the user to issue it

9. Receiving the key and the certificate

10. Switching from the old certificate

11. FAQ — errors, causes and solutions

1. Overview

1.1 What this guide covers

An organisation that connects to EESZT (the Hungarian Electronic Health Service Space) needs an authentication certificate. In the Netlock web application this is the **Organization authentication certificate**. The Store describes it as *"A client authentication certificate issued to your organization itself — it carries your organization's verified legal name and registration identifier, never a person's name."*

The certificate is issued with the ECC algorithm, which EESZT accepts. It is valid for two years, and its fee is paid every year.

The guide follows the whole path: from creating the Netlock account and the organisation, through verifying the business details, the legal representative's verification and power of attorney, the purchase with credits and allowing the user, to the colleague downloading the key and the certificate. At the end it describes how the organisation replaces its old certificate with the new one (chapter 10). It does not cover buying the certificate by card.

The key is created in the colleague's browser and never reaches Netlock: the colleague downloads it together with the certificate in a single password-protected PFX file (chapter 9).

> **NOTE** The certificate can be issued only after the organisation's legal representative has completed the quick online video identification and granted the power of attorney on the organisation's behalf (chapter 5). If they cannot do this, they may send a written power of attorney instead (chapter 6). Start with this step, and agree on it with the legal representative in good time.

1.2 What you need

- **A Netlock account** for everyone taking part: whoever creates the organisation, the legal representative and the colleague who receives the certificate (chapter 2). One person can hold several of these roles; if the legal representative does everything themselves, one account is enough.
- **The organisation's verified business details.** The organisation's tax number or company registration number is enough for this (chapter 4).
- **The legal representative**, for the video identification: a valid identity card or passport, a computer or phone with a camera and a microphone, good lighting, and about an hour without interruption (5.4). With joint representation this applies to every representative required.
- **Credits** on the organisation's balance for the certificate fee; credits are bought by card on the secure checkout page (chapter 7).
- Steps 3–4 and 7–8 are carried out by an owner or administrator of the organisation. The colleague who receives the certificate must be a member of the organisation (3.3).

1.3 The steps

Step	Who	Where	Chapter
1. Creating a Netlock account	everyone taking part	the **Create account** link on the sign-in page	2

Step	Who	Where	Chapter
2. Creating the organisation, inviting colleagues	whoever creates the organisation	**Settings** → **Organizations**, **Members**	3
3. Entering and verifying the business details	owner or administrator, then the Netlock Registration Authority	**Business Details**	4
4. The legal representative's video identification and power of attorney	the legal representative, then the owner or administrator	**Home**, **Certificates**	5 (or written power of attorney: 6)
5. Buying credits and the certificate	owner or administrator	**Store**	7
6. Allowing the user to issue it	owner or administrator	**Certificates**	8
7. Receiving the key and the certificate	the colleague	**Store**	9
8. Replacing the old certificate	the organisation and its IT partner	the EESZT connection, then an e-mail to Netlock	10

2. Netlock account and signing in

2.1 Creating an account

1. Open the Netlock sign-in page and click the **Create account** link (*"Don't have an account? Create account"*).
2. Fill in the form: **Email**, **Password**, **Confirm Password**, **Given name** and **Family name**. Enter your name as it appears on your identity document (*"Enter your name as it appears on your ID document."*). This matters most for the legal representative: the name is compared with the officers listed in the company register (4.3, 5.4).
3. Press **Create account**. You can also register with an Apple, Google or Microsoft account (**Sign up with**).
4. Confirm your e-mail address: open the link in the e-mail you receive. The link is valid for 30 minutes; if it has expired, ask for a new one with **Resend verification email**. If you cannot find the e-mail, check the spam folder too.

If you have been invited to an organisation, you can also create the account from the invitation link (3.3). In that case use the e-mail address the invitation was sent to.

2.2 Setting up a second factor

A Netlock account requires at least one second factor. At the first sign-in the **Secure your account** screen appears:

1. Accept the terms of use and the privacy documents (both checkboxes), then press **Set Up Now**.
2. Choose a method — **Passkey** (Face ID, Touch ID, Windows Hello or fingerprint), **Security Key** (a hardware security key), **Authenticator App** (for example Google Authenticator) or **SMS Code** (a code sent to your phone) — and follow the instructions on the screen.

Netlock may ask for the second factor again when the video identification starts (5.3), so the legal representative should have it at hand.

2.3 Signing in

1. Enter your e-mail address and press **Continue**.
2. Enter your password and press **Sign in**; if you registered with an Apple, Google or Microsoft account, choose it.
3. Enter your second factor.

If you have forgotten your password, use the **Forgot password?** link on the sign-in page. If you cannot enter your second factor, for example because you lost your phone, contact Customer Service (trust@netlock.com, +36 1 437 6655).

3. Creating the organisation

3.1 A new organisation

Creating an organisation is free.

1. Open **Settings → Organizations** and press **Create Organization**.
2. Fill in **Organization name**; the **Organization URL slug** is filled in from the name.
3. Press **Create a free organization**.

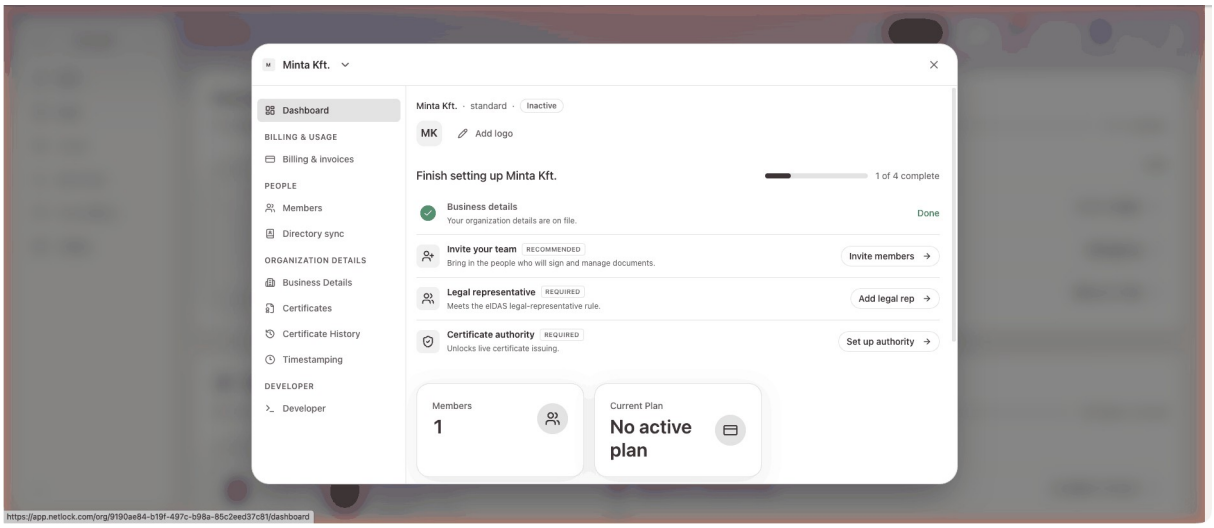
The organisation is created at once, and the application opens it on the **Business Details** page. Whoever creates the organisation becomes its owner. You switch between organisations with the organisation switcher at the top of the left-hand menu.

3.2 The setup checklist

On the organisation's **Dashboard** the *"Finish setting up your organization"* checklist shows what is still to do, each step with its own button:

- **Business details** (required) — chapter 4;
- **Invite your team** (recommended) — 3.3;
- **Legal representative** (required) — chapter 5;
- **Certificate authority** (required) — 5.6–5.7.

If you are an owner or administrator and also the organisation's legal representative, your own two steps appear on the list too: **Start your certificate registration** and **Grant your power of attorney**. Sections 5.3 and 5.5 describe them.



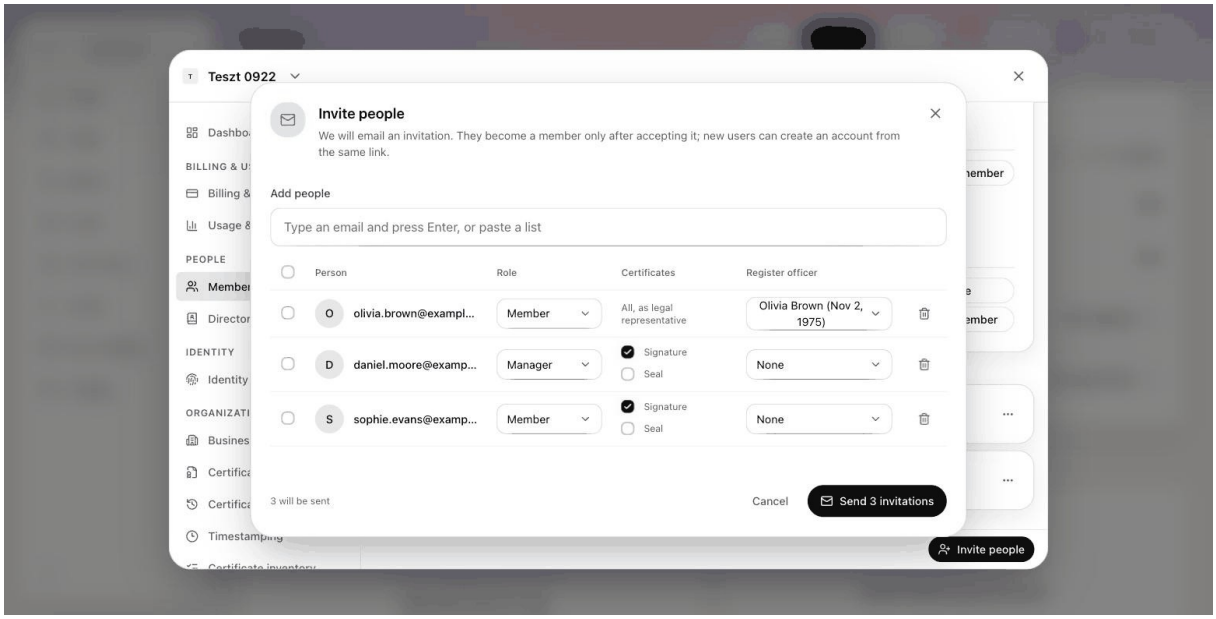
3.3 Inviting a colleague

Invite the colleague who will receive the certificate to the organisation, if that is not you. Invite the legal representative, if they did not create the organisation, after the business details have been verified (5.2).

1. Open the **Members** page and press **Invite people**.
2. Type the colleague's e-mail address in the **Add people** field and press Enter.

3. Choose the role in the **Role** column. New rows start with the **Member** role; owners, admins and managers can receive the certificate without a separate permission, and a member is given permission (chapter 8).
4. Press **Send 1 invitation**.

The invitee receives an e-mail. Opening the link, they sign in, or create an account from the same link, and accept the invitation. Only then do they become a member of the organisation; until then the invitation is listed under **Pending Invitations**, where you can also send it again (**Resend Invitation**).

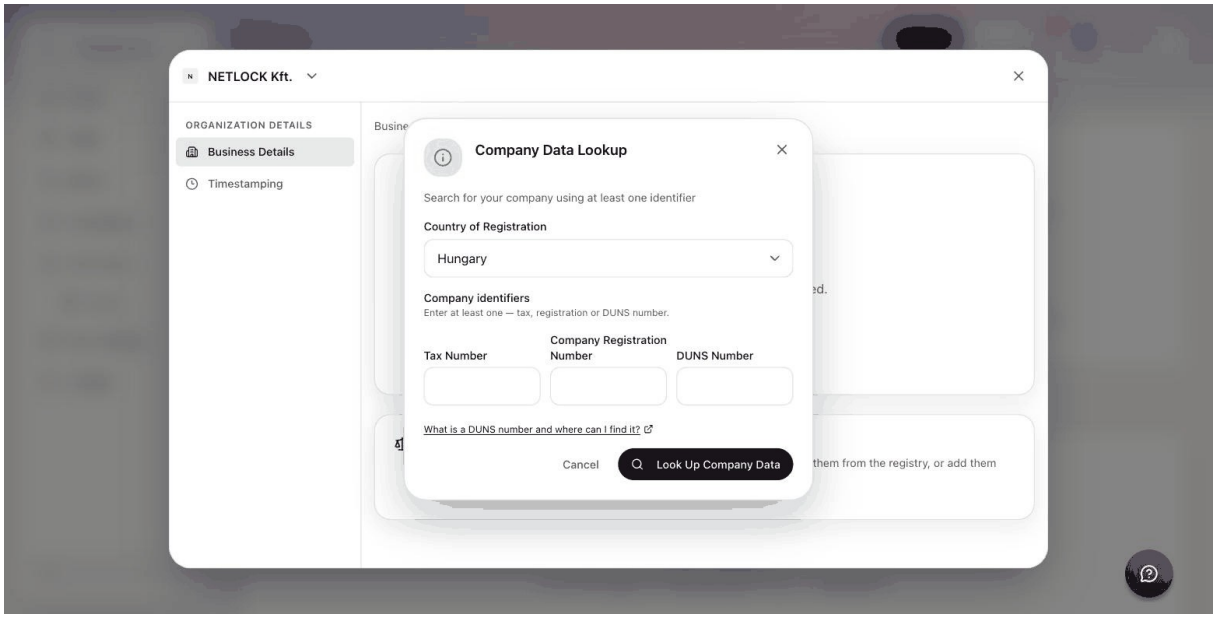


4. Entering and verifying the business details

The certificate carries the organisation's verified company data: its subject is the organisation's legal name and registration identifier. Nobody types these into the certificate; they are taken from the business details, and the certificate is issued only for a name verified for the organisation. The registration identifier follows the European standard (ETSI EN 319 412-1): for a Hungarian organisation `VATHU-` and the eight-digit core of the tax number; for another country `VAT`, the country code and its VAT number, or, without one, `NTR`, the country code and the registration number.

4.1 Company data lookup

1. Open the **Business Details** page, then the **Company Data Lookup** window.
2. Enter at least one identifier — **Tax Number**, **Company Registration Number** or **DUNS Number** — and the **Country of Registration**, then press **Look Up Company Data**.
3. If a match is found, press **Use This Data**. On the first lookup the data is saved at once, together with the legal representatives listed in the register, and sent for verification. If anything is missing, fill it in and press **Save Business Details**. If nothing is found, enter the data with **Enter Manually**.



4.2 The verification outcome

Once saved, the business details are verified. If the company cannot be verified automatically from the register (for example with data entered by hand, or when the representation cannot be derived from the register), the Netlock Registration Authority verifies it manually. A banner on the page shows the outcome:

The banner says	What it means
"Your company data has been submitted to the NetLock Registration Authority for manual verification."	Verification is in progress; wait for the outcome.
"The Registration Authority could not verify your	Correct the data and save it again;

The banner says	What it means
company data."	saving starts a new review.
"Your company data has been verified."	The organisation is verified; continue with chapter 5.

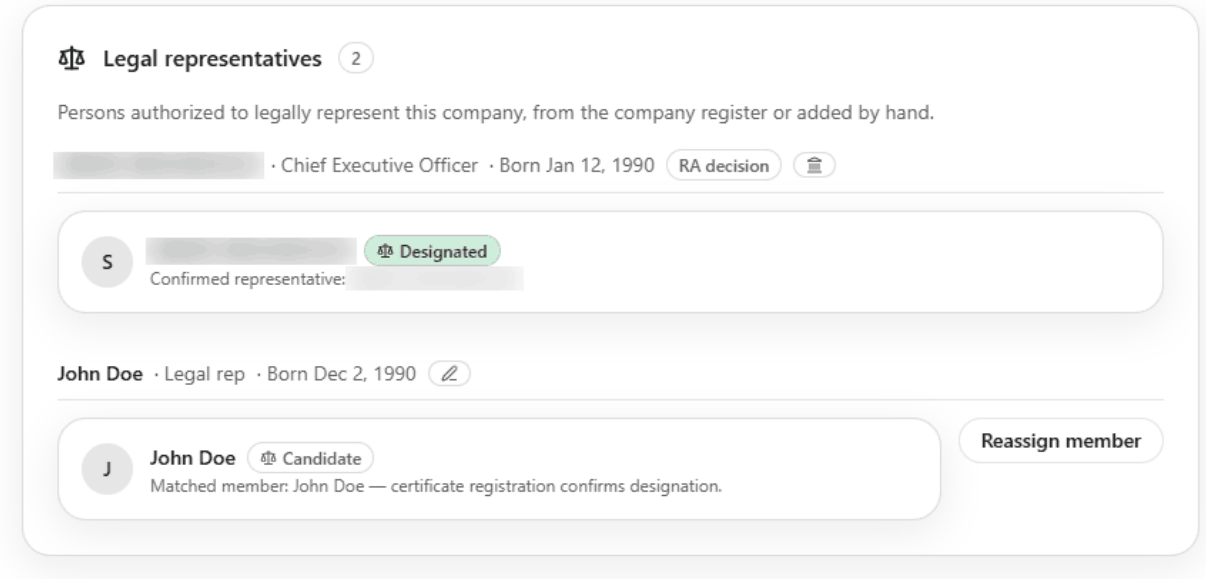
Verified business details are read-only. If you change them (**Edit**, then **Edit anyway**), the organisation is verified again, and new certificate requests wait until then. Once certificates have been issued, changing data that a certificate carries revokes every active certificate of the organisation; the application warns you with **Revoke all certificates to apply this change?**, and **Keep certificates** lets you back out.

4.3 The list of legal representatives

The **Legal representatives** part of the **Business Details** page lists the company's officers from the register, each with the type of representation: **Independent** or joint. Each row also shows who is linked to the officer in Netlock:

- **Candidate** — a member of the organisation matches the officer, but their designation is not confirmed yet. A member becomes a candidate if their account name matches the officer's name, if they accepted an invitation linked to the officer, or if an administrator assigned them to the officer (5.2).
- **Designated** — the legal representative has confirmed their identity with the video identification (5.4), or the Netlock Registration Authority has designated them.
- **Invitation pending** — the officer has been invited but has not accepted the invitation yet.

If the register records joint representation, the page shows the **Joint representation** label and this notice: *"This company has joint representation. Multiple legal representative authorizations are required to issue certificates."*



5. Legal representative verification and power of attorney

5.1 Why it is needed

A certificate in the organisation's name — the organisation authentication certificate used for EESZT is one — is issued only when the organisation's certificate authorisation is complete. For this the legal representative has to:

1. complete the quick online video identification, through which they receive their own organisation certificate free of charge (5.3–5.4), and
2. grant the power of attorney (PoA) on the organisation's behalf (5.5).

The legal representative must do this personally; nobody else can do it for them. With independent representation one legal representative is enough; with joint representation every representative required must do it.

Until the authorisation is complete, issuing the certificate is refused with *"Your organization's authorization is not complete yet: enough of its legal representatives must hold their own organization certificate. …"* You can buy the certificate before that, but it can be issued only after the authorisation, so wait with the purchase until then (chapter 7).

If the legal representative cannot complete the video identification, they may send a written power of attorney (chapter 6).

5.2 Involving the legal representative

The legal representative needs a Netlock account (chapter 2) and must be a member of the organisation.

If the legal representative created the organisation themselves, there is nothing to do: if their account name matches their name in the register, they appear on the **Legal representatives** list as **Candidate** once the business details are saved (4.3). The name match tolerates a missing middle name, title or married-name prefix in the account name, as long as at least two name words match. If they do not appear as a candidate, an owner or administrator assigns them (see **Assign member** below).

If someone else created the organisation, an owner or administrator invites the legal representative once the business details are verified:

1. On the **Legal representatives** list of the **Business Details** page, press **Invite** in the officer's row.
2. In the **Invite legal representative** window, enter the legal representative's e-mail address (**Email address**) and press **Send invitation**. You thereby confirm that the address belongs to the officer named in the register.
3. The legal representative receives an e-mail with the subject *"You've been invited as a legal representative of {organization}"*. Opening the link, they sign in, or create an account from the same link, then accept the invitation with **Accept Invitation**.

Until it is accepted, the row shows **Invitation pending**; afterwards the legal representative is a **Candidate**.

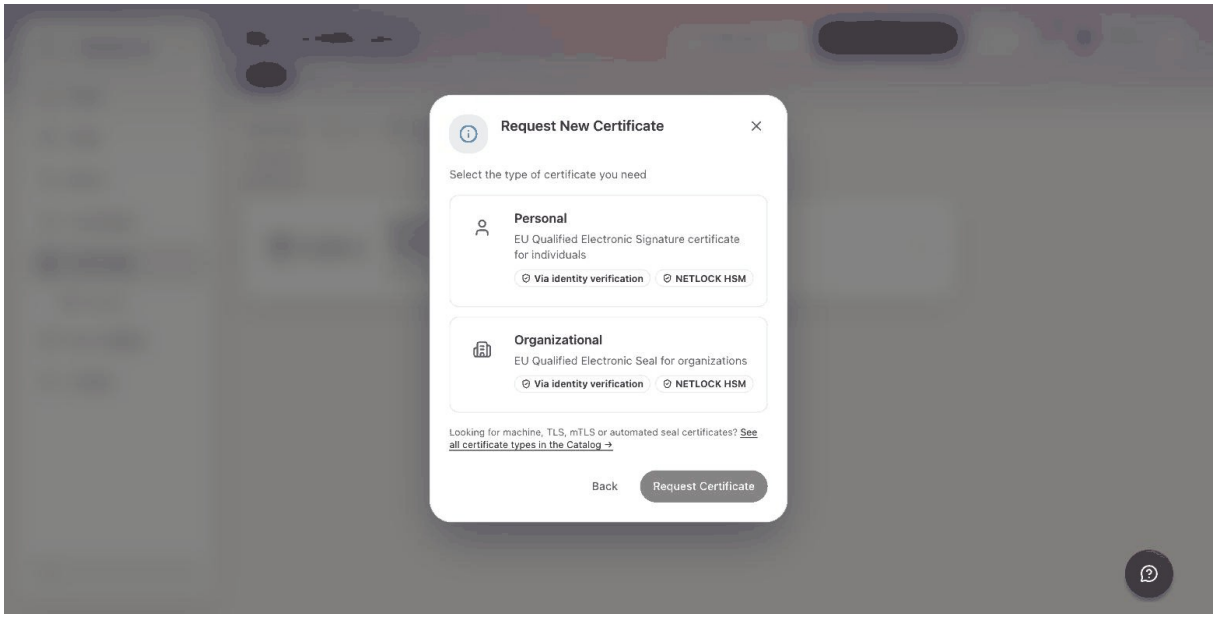
If the legal representative is already a member of the organisation, assign them with **Assign member** in the officer's row: choose the member, review the choice and press **Assign as candidate**.

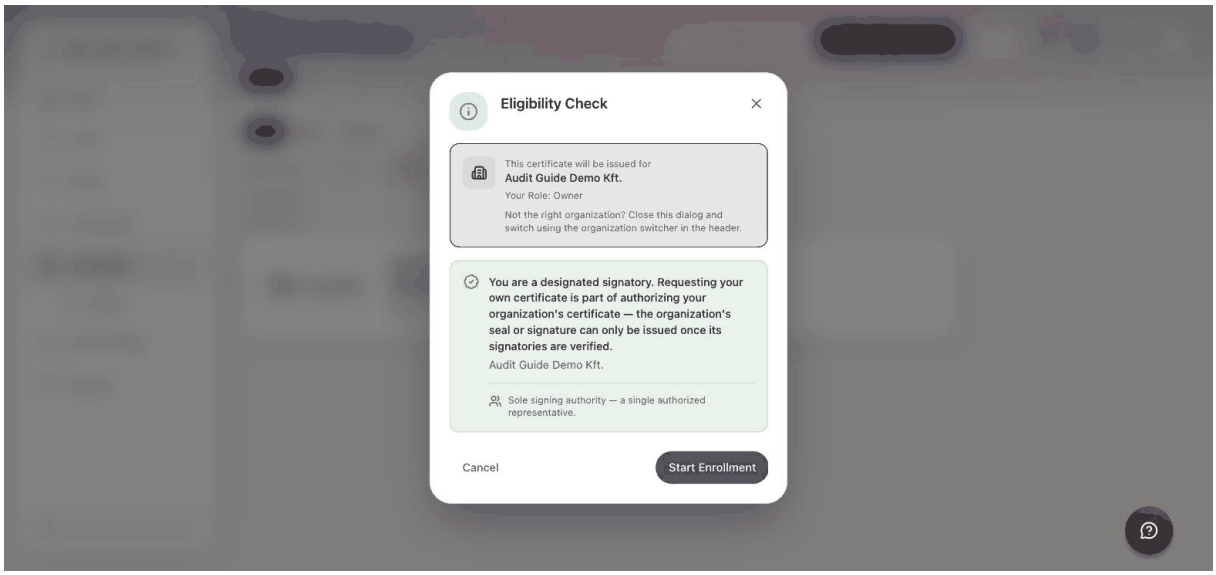
5.3 Starting the video identification

The legal representative completes the video identification with their own account, after the business details have been verified.

1. Sign in, and switch to the organisation with the organisation switcher.
2. On the **Home** page a *"{organisation} is waiting on you"* card shows two steps: **Start your certificate registration** and **Grant your power of attorney**. Press **Start registration**. If you are an owner or administrator of the organisation, you find the same step on the setup checklist (3.2).
    - Instead of the button, you can also start from the **Certificates** page with **Request Certificate**: in the **Request New Certificate** window choose the **Organizational** card.
3. The top of the window shows the organisation the certificate is issued for (*"This certificate will be issued for"*). If it is not the right one, close the window and switch organisation.
4. The **Eligibility Check** runs. If it passes, press **Start Enrollment**.
5. If your sign-in is not recent enough, Netlock asks for your second factor; enter it.

The video identification then opens with the **Organization certificate request** header.





5.4 The video identification steps

The video identification is the same remote identity check as for a personal certificate, only on the organisation's behalf: the header reads **Organization certificate request**, and the step bar has an extra **AUTHORIZE** stage. The screenshots in this section come from the personal request, so their header reads *Netlock Personal Certificate*; the screens are otherwise the same.

The step bar at the top of the screen shows where you are: **VERIFY**, **CHOOSE**, **INFO**, **SCAN**, **CONFIRM**, **SELFIE**, **AUTHORIZE** and **DONE**. On a phone the stages have no labels; a line above them names the current one, for example *4/8 · SCAN*. The header holds the **Exit** button (see *Stopping and continuing*).

Before you start

What you need	Details
A valid, original identity document	With a Hungarian document: an identity card (front and back) or a passport (photo page). For a document from another European country the identity card and the passport are usually offered too; for most other countries only the passport. A residence permit is not accepted. Neither is a photocopy or a picture on a screen: hold the original, physical document up to the camera. An expired document is refused.
A camera and a microphone	A computer or phone with a camera and a microphone. The check is recorded as video and audio.
Good light	Even, not too strong light, without direct sunlight on your face. Turn the screen brightness to maximum.
A quiet place and about an hour	The check must be finished within one hour of starting it.
A working second factor	Netlock may ask for it at the start (2.2).

Take off your glasses and anything else that covers your face.

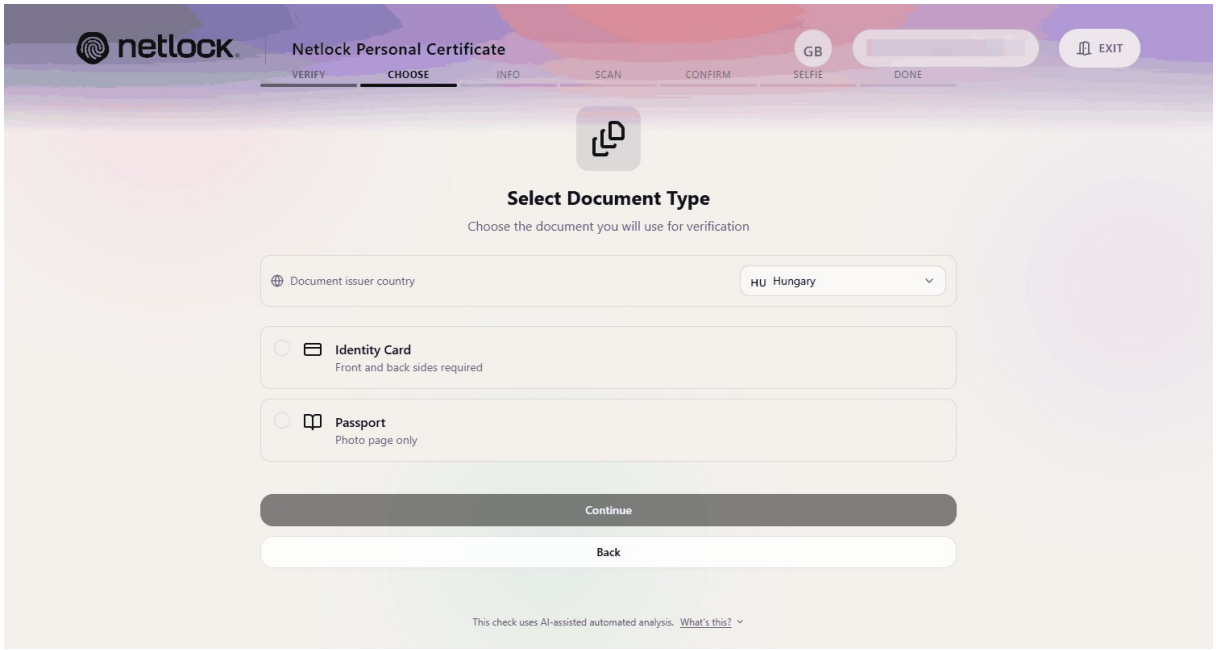
Step 1 — VERIFY: confirming your sign-in

1. On first opening, a **Cookie settings** banner asks whether Netlock may use analytics cookies. **Accept all** and **Reject all** both work; rejecting does not stop the identification.
2. If your sign-in is recent enough, the screen says *"Identity verified, continuing…"* and moves on by itself. If not, the Netlock sign-in page asks for your second factor; enter it, and the flow continues automatically.

Step 2 — CHOOSE: choosing the document

On the **Select Document Type** screen:

1. Check the **Document issuer country**. Netlock fills it in; if your document was issued by another country, open the list, type the first letters of the country and choose it.
2. Choose the document: **Identity Card** (*"Front and back sides required"*) or **Passport** (*"Photo page only"*). The grey **DÁP · coming soon** card cannot be chosen yet.
3. Press **Continue**.

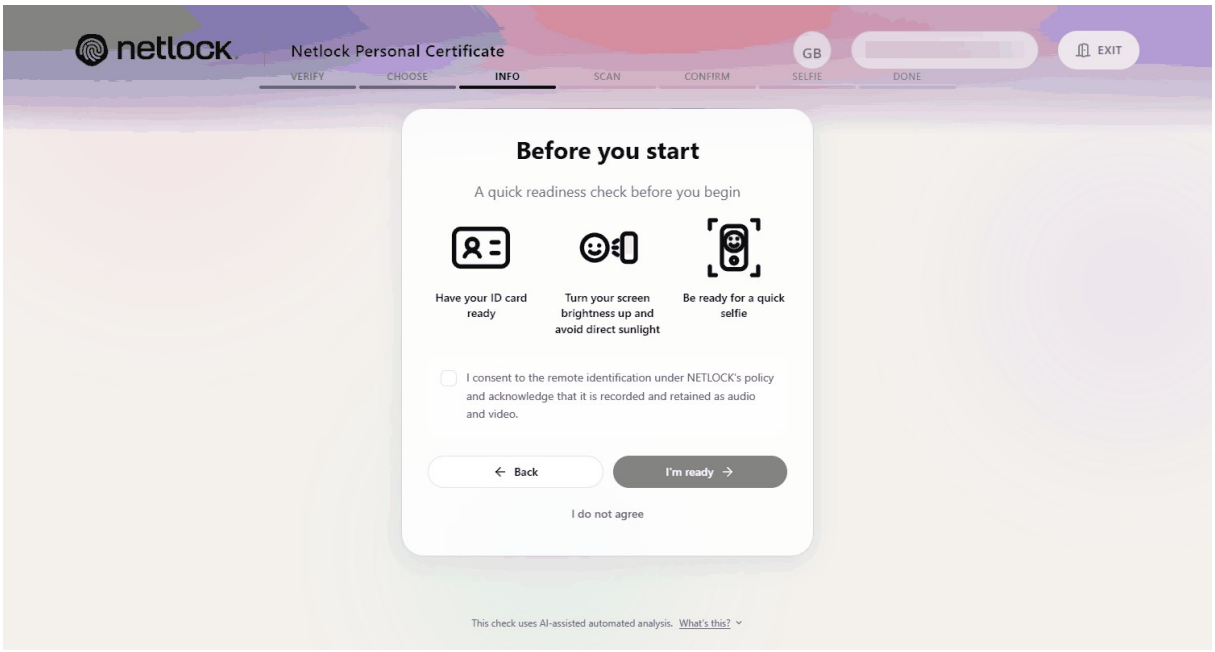


Step 3 — INFO: getting ready and consent

The **Before you start** screen shows three reminders: have the document at hand (*"Have your ID card ready"* or *"Have your passport ready"*), *"Turn your screen brightness up and avoid direct sunlight"*, and *"Be ready for a quick selfie"*.

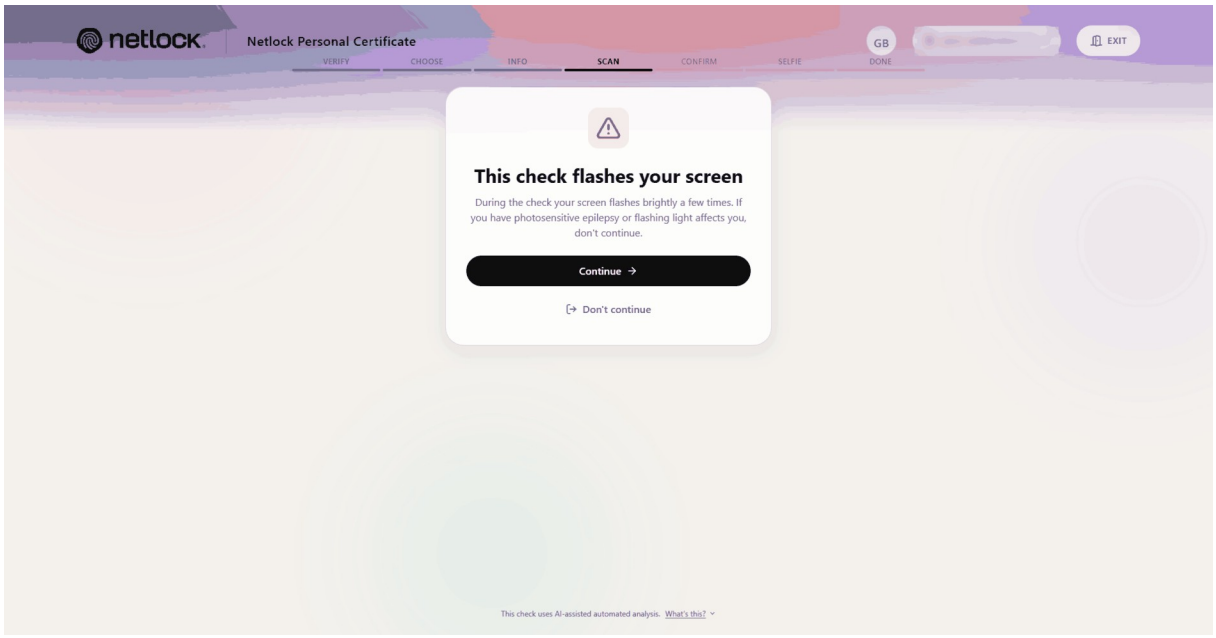
1. Tick the consent: *"I consent to the remote identification under NETLOCK's policy and acknowledge that it is recorded and retained as audio and video."*
2. Press **I'm ready**. Until the box is ticked, the button cannot be used.

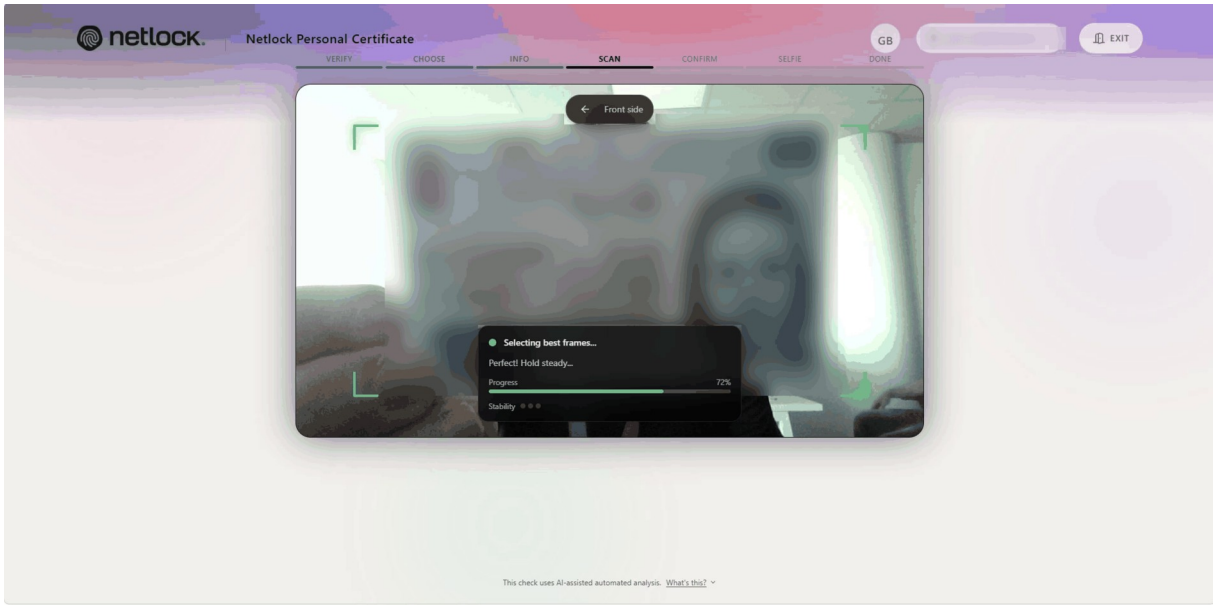
If you choose **I do not agree**, the identification ends here and no certificate is issued (*You chose not to go ahead*).



Step 4 — SCAN: scanning the document

1. **Flashing warning.** Before the first camera step a card says *"This check flashes your screen"* — the screen flashes brightly a few times during the check. If you have photosensitive epilepsy or flashing light affects you, choose **Don't continue**. Otherwise press **Continue**.
2. **Camera.** The browser asks for permission to use the camera: allow it. If the screen says the camera is blocked (*"Camera access is blocked…"*), that there is no camera (*"No camera was found on this device."*), or that another app is using it, allow it in the browser settings or close the other app, then try again.
3. **The front of the document.** The screen asks: *"Show the front side of your document"*. Hold the document flat inside the frame. The **Progress** bar fills and the **Stability** dots light up as the picture improves. On a phone, turn it sideways when the screen asks (**Turn your phone sideways**).
4. **Hold still.** You do not need to press anything: once the document is steady and sharp, the application captures it by itself (*"Hold steady..."*, *"Capturing..."*). For the security check it may ask you to tilt the document slightly (*"Gently tilt the document a little"*), and for an identity card to rock it slowly so the hologram catches the light (*"Slowly rock the ID left and right so the hologram catches the light"*).
5. **The back.** For an identity card the screen then shows **Flip your card**: show the back the same way. For a passport only the photo page is scanned.
6. **Analysis.** While Netlock reads and checks the document, the screen shows *"Analyzing your document..."*. If the picture gets stuck, the screen says what is wrong (for example it is too dark, or the document is not fully inside the frame), and **Retake** restarts the side.





Scanning tips. The messages on the screen help; the most common ones:

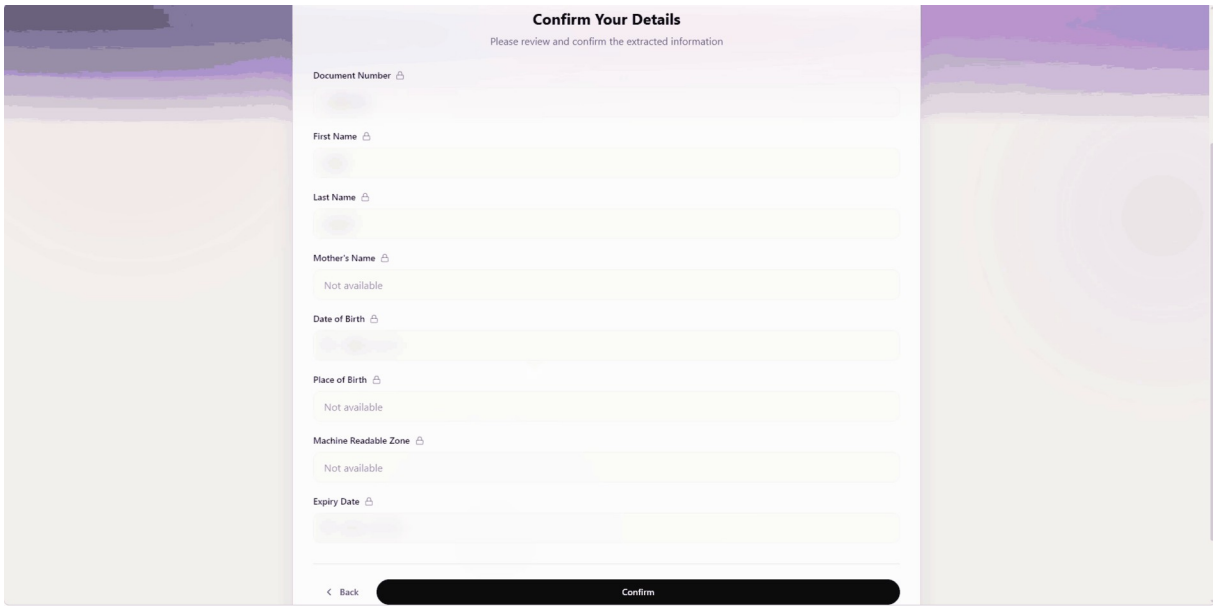
What to do	The message you may see
Light the document evenly, without glare or shadow.	*"It's too dark. Move to a brighter place", "It's too bright. Avoid direct light", "There's glare on the document. Tilt it slightly away from the light"*
Keep the whole document flat inside the frame.	*"Move the document closer", "Move the document a little further away", "Make sure all four corners of the document are visible", "Straighten the document"*
Hold the device steady, or lay the document on a flat surface.	*"The picture is blurry. Hold the document steady"*
Show the original document, not a photocopy or a picture on a screen.	*"This looks like a screen. Show the physical document"*
Keep the photo and the text	*"Make sure the photo is clearly visible"*

What to do	The message you may see
readable.	

Step 5 — CONFIRM: confirming the details

The **Confirm Your Details** screen shows the data read from the document: **Document Number**, **First Name**, **Last Name**, **Mother's Name**, **Date of Birth**, **Place of Birth**, **Machine Readable Zone** and **Expiry Date**. For Hungarian documents the data comes from the document and the official register. The fields cannot be edited.

1. Review the data.
2. If it is correct, press **Confirm**.
3. If something is wrong, scan the document again: press **Back**, then answer **Scan your document again?** with **Yes, scan again**.



Automatic checks and the name check

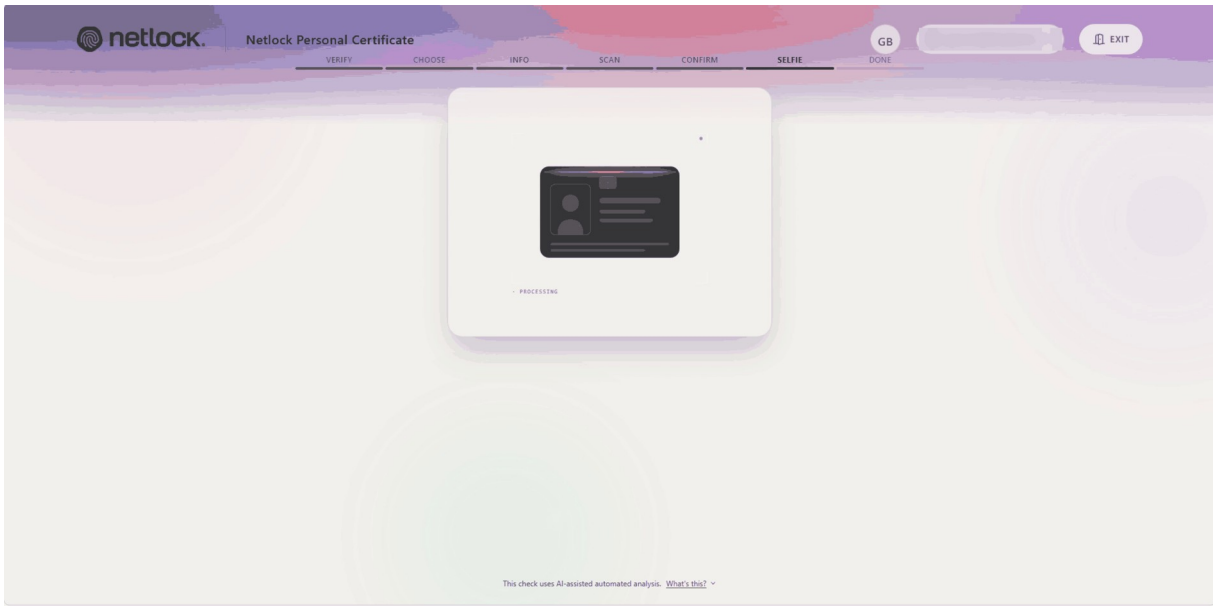
After **Confirm**, Netlock runs its checks without asking; they have no stage on the step bar, and while they run the screen shows only an animation. There is nothing to do; wait.

- **Verifying Your Information**: for a Hungarian document, the document number and the personal data are compared with the official register.
- **The legal representative name check**: Netlock compares the name and date of birth on the document with the company's registered officers.

Outcome of the check	What happens
The legal representative is among the officers.	The flow continues.
The match is uncertain (for example the name is close to the registered one and the date of birth matches), or the list of officers is not available.	The flow continues, and a staff member reviews the request.
The legal representative is not among the officers.	The **Certificate request declined** screen says *"You aren't listed as a legal representative of*

Outcome of the check	What happens
	this organization." No certificate is issued; chapter 11 says what to do.

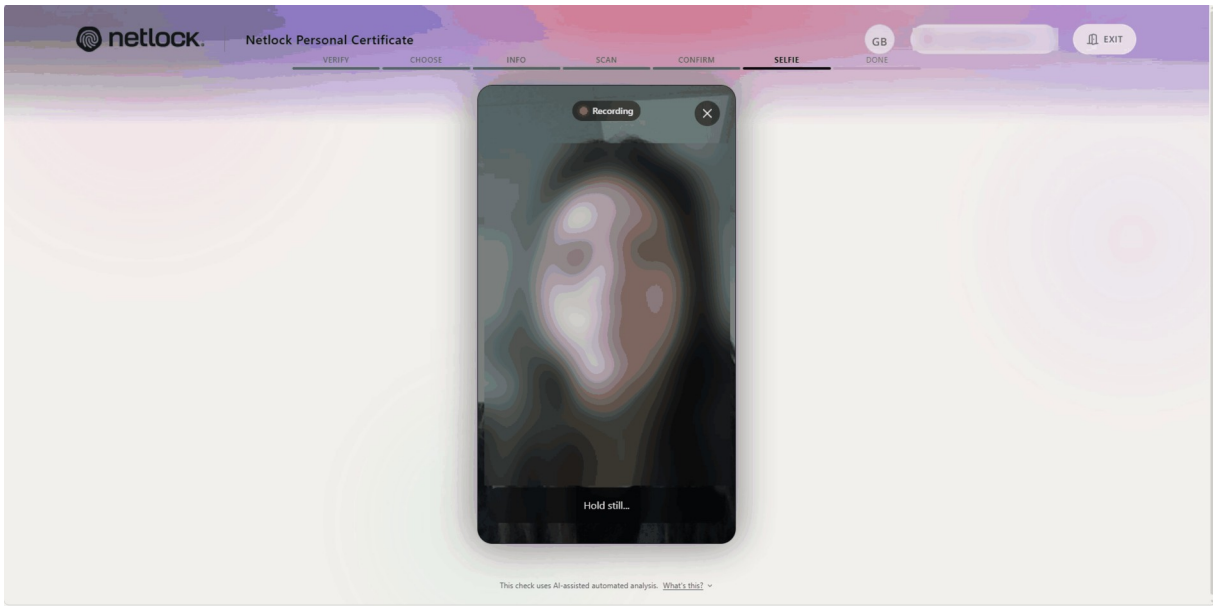
If a check does not accept the scanned document, the **We couldn't verify your ID** screen sends you back to the scan.



Step 6 — SELFIE: selfie and liveness check

1. **Brightness.** Before the camera opens, a card asks: **Set your screen brightness to maximum**. The check uses a quick screen flash to confirm that a real person is in front of the camera; on a dim screen the flash may be too weak. Turn the brightness to maximum, then press **Continue**.
2. **The camera.** On a phone, hold it upright at eye level; the camera opens only in portrait (**Turn your phone upright**). Look into the camera.
3. **The oval frame.** Keep your face inside the oval frame. The screen tells you what to adjust, for example *"Look straight at the camera with your whole face in view"*, *"Only one face should be visible"*, *"Move closer to the camera"*, *"Move back from the camera"*, *"Hold your head straight"*, *"Hold still..."*. The small indicators — **Position**, **Distance**, **Lighting**, **Head** — change to *"Looking good — hold still"* when everything is right.
4. **Follow the instructions.** The check may ask for a short movement, or for a short text to be read aloud: do it calmly and clearly. The browser may then ask for permission to use the microphone: allow it. If the screen shows **Microphone error**, allow the microphone in the browser settings or close the other app using it, then press **Retry microphone**.
5. **Lighting.** Just before the flash, Netlock checks the light on your face. If it is too strong (**Too much direct light on your face**) or too weak (**It's a bit too dark**), change the lighting — move out of direct sunlight, close the curtains, or switch on a lamp facing you — then press **I've adjusted – try again**.
6. While Netlock analyses the recording, the screen shows *"Verifying your identity..."*.

After the selfie you cannot go back to the earlier steps.



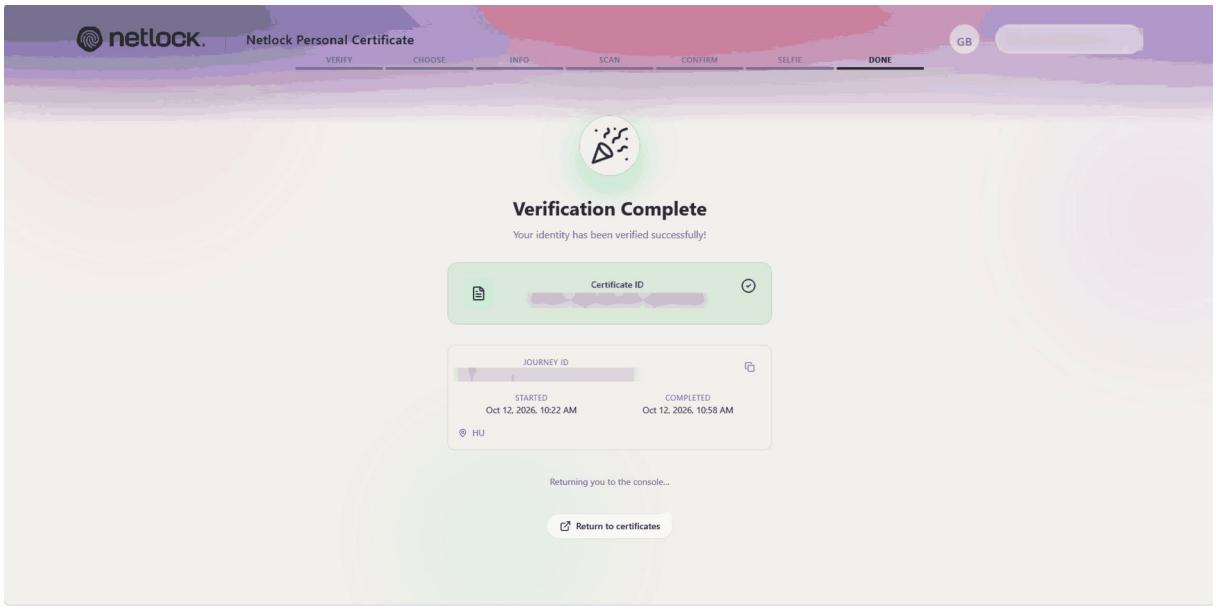
Step 7 — AUTHORIZE: the power of attorney

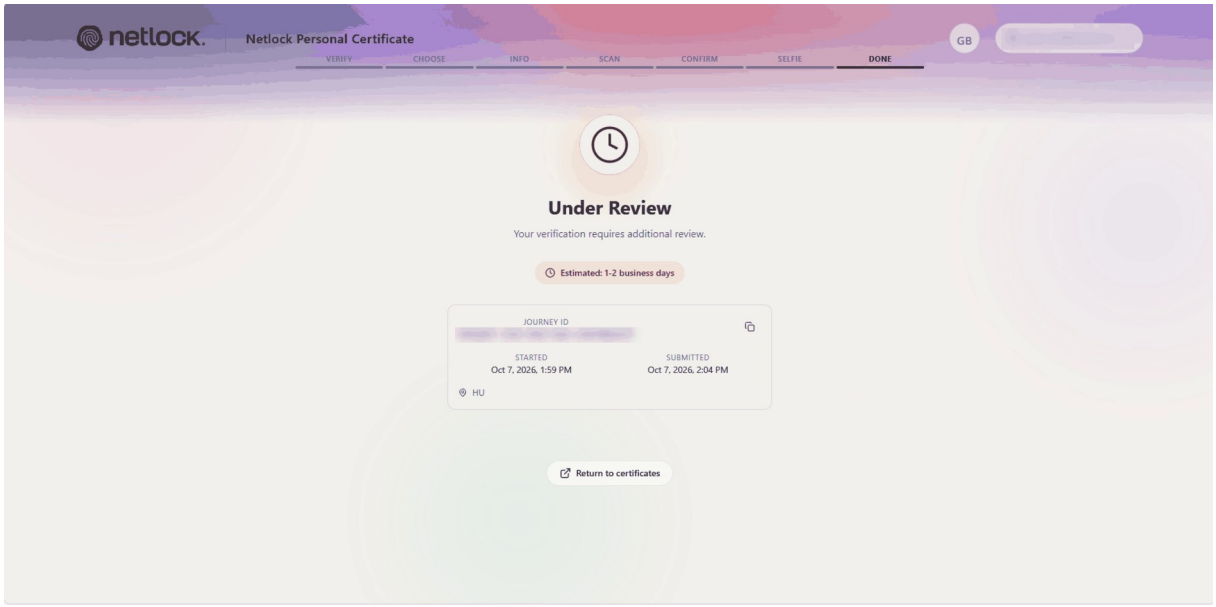
After the selfie the screen asks for the power of attorney. Section 5.5 describes the declaration and the buttons; to grant it, choose **I grant the Power of Attorney**.

Step 8 — DONE: the outcome

At the end of the check the outcome screen appears. **Return to certificates** takes you back to the web application.

- **Verification Complete** — *"Your identity has been verified successfully!"* The screen also shows the **Certificate ID** and the **Journey ID**; you can copy the latter with the button next to it. Note both in case you need to contact Customer Service. The legal representative's own certificate then appears as **Active** on the **Certificates** page, and they become **Designated**.
- **Under Review** — *"Your verification requires additional review."* There is nothing to do: a registration officer reviews the request and may e-mail you if a further document is needed. The screen also shows the expected time, usually **Estimated: 1-2 business days**. You receive an e-mail about the decision; until then the request waits on the **Certificates** page as **Under manual review**.
- **Verification Failed** — *"We were unable to verify your identity."* A red card names the step that failed, the reason and what to do. **Start New Verification** takes you back to the web application: start the new request from the **Certificates** page (5.3). **Contact Support** opens an e-mail to Customer Service with the Journey ID as the subject.





If a camera step fails

The document scan and the selfie each allow at most three attempts. If an attempt fails, a screen explains it and offers the next step:

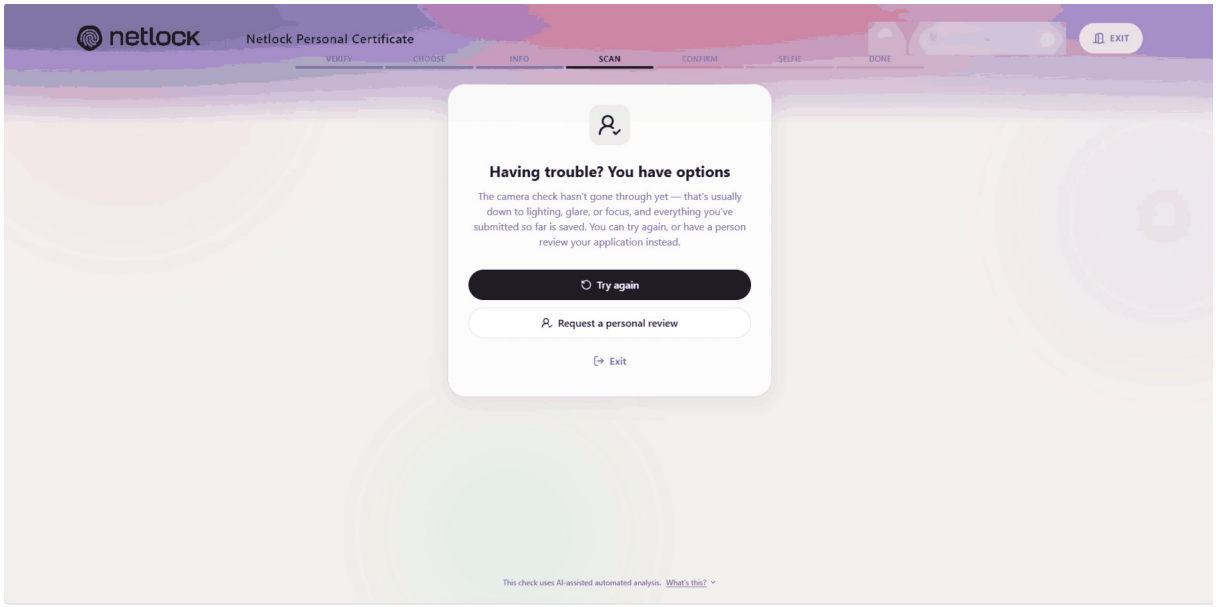
Screen	What it says, and what you can do
Let's try that again	A short message names the reason (for example the document picture was blurry, or the face did not match the photo on the document). **Try again** opens the camera again.
Connection problem	The connection was lost before the check finished. Check the network and try again.
Capture paused	You closed the camera; **Resume** continues where you left off.
Camera unavailable	Check the camera permissions and try again.

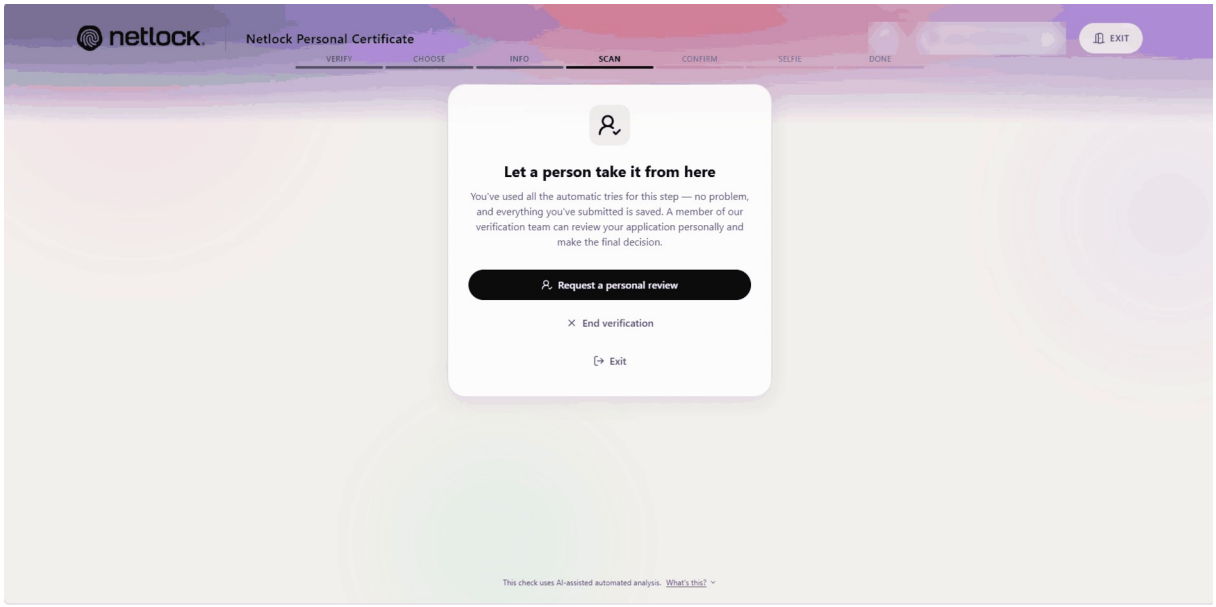
A staff member can take over. If the attempts keep failing, the screen is titled **Having trouble? You have options**. This is usually down to lighting, glare or focus, and everything

you have submitted so far is saved. You can choose **Try again**, **Request a personal review** or **Exit**.

When all three attempts are used up, the screen is titled **Let a person take it from here** and offers **Request a personal review** or **End verification**. **End verification** closes the request, and it cannot be resumed later; when asked to confirm, **Keep going** still takes you back.

If you ask for a personal review, the screen confirms it (**Review requested**). Then finish the remaining steps — including the power of attorney — so that the staff member has all the data. The flow ends with the **Your request is with our team** screen; you usually receive the outcome by e-mail within 1–2 business days.

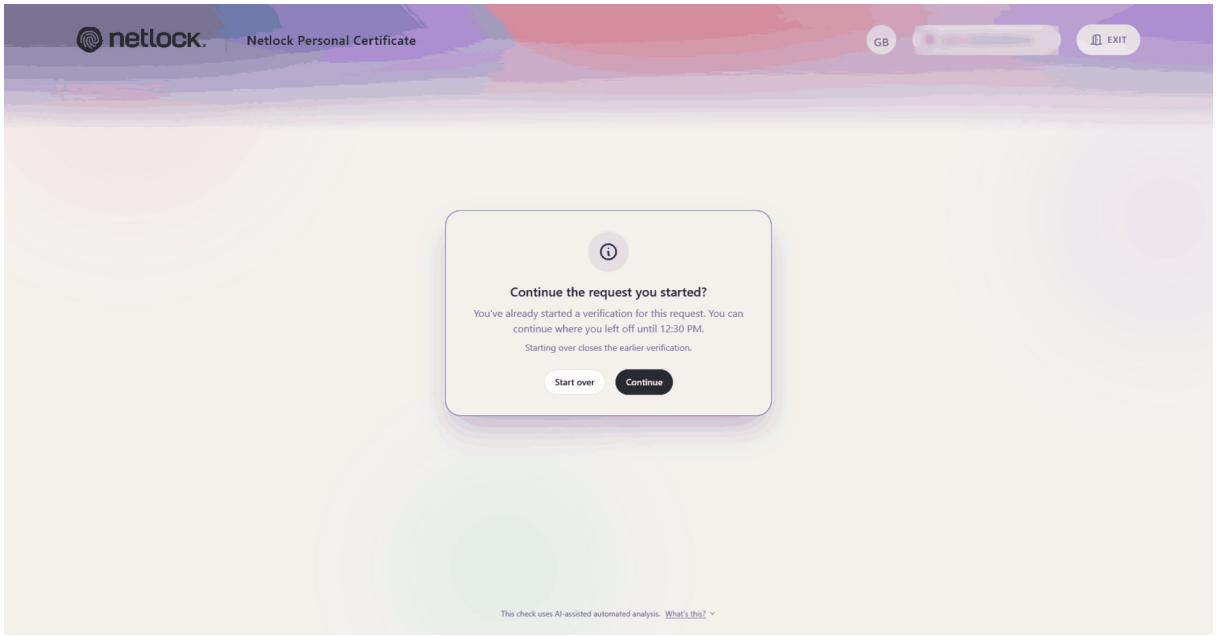




Stopping and continuing

Exit asks **Exit verification?** — the check you started is not lost until it expires. Confirm with **Exit** to leave; **Cancel** keeps you in the check.

If you stopped before submitting and start the same request again from the **Certificates** page within one hour of starting it, Netlock offers to continue: **Continue the request you started? Continue** picks up where you left off; **Start over** begins a new check. A check that is already under review is not offered.



What happens next. If the request passed without a staff review, the legal representative's own organisation certificate is issued and they become **Designated**. If a staff member reviews it, you receive an e-mail about the decision. The next step is the power of attorney (5.5), if it has not been granted yet, then enabling organisational certificates (5.6).

5.5 Granting the power of attorney

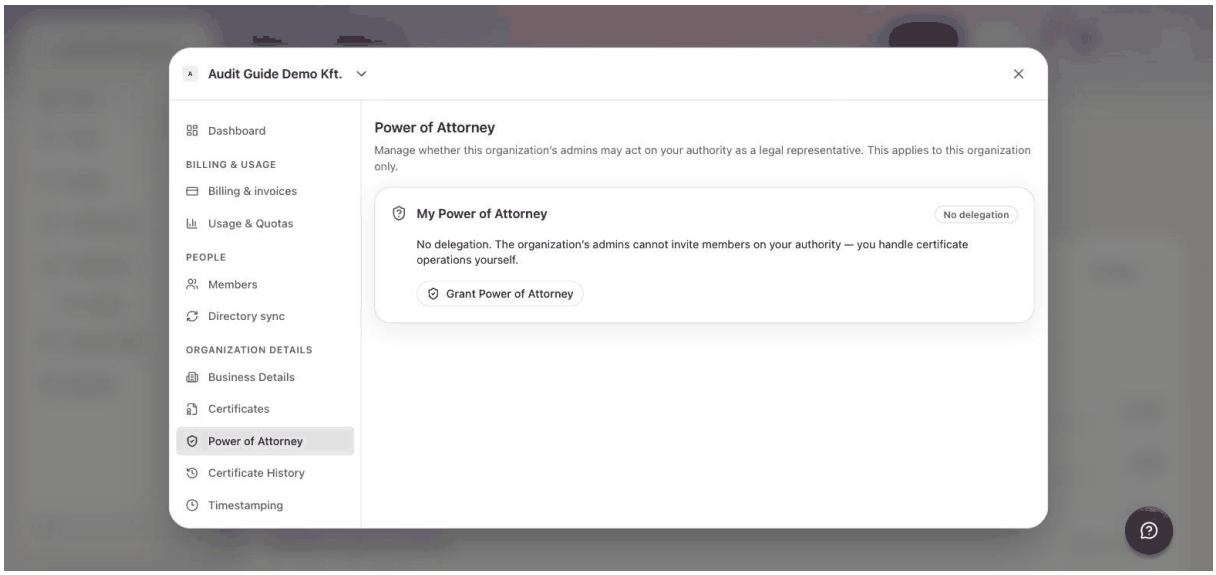
With the power of attorney the legal representative authorises the organisation to request and manage certificates on their authority. It can be granted in two places.

In the AUTHORIZE step of the video identification. The screen shows the declaration, filled in with the organisation's name: *"As a legal representative of {organisation}, you authorize the organization to issue qualified electronic certificates to its members under your Power of Attorney. …"* To the question **Do you grant this Power of Attorney?** choose **I grant the Power of Attorney**. If you chose **Not now**, grant it later in the web application.

In the web application, once you are **Designated**:

1. Open the organisation's **Power of Attorney** page; the **Grant authority** button on the **Home** page takes you straight there.
2. On the **My Power of Attorney** card, press **Grant Power of Attorney**.
3. Read the declaration and press **Grant**.

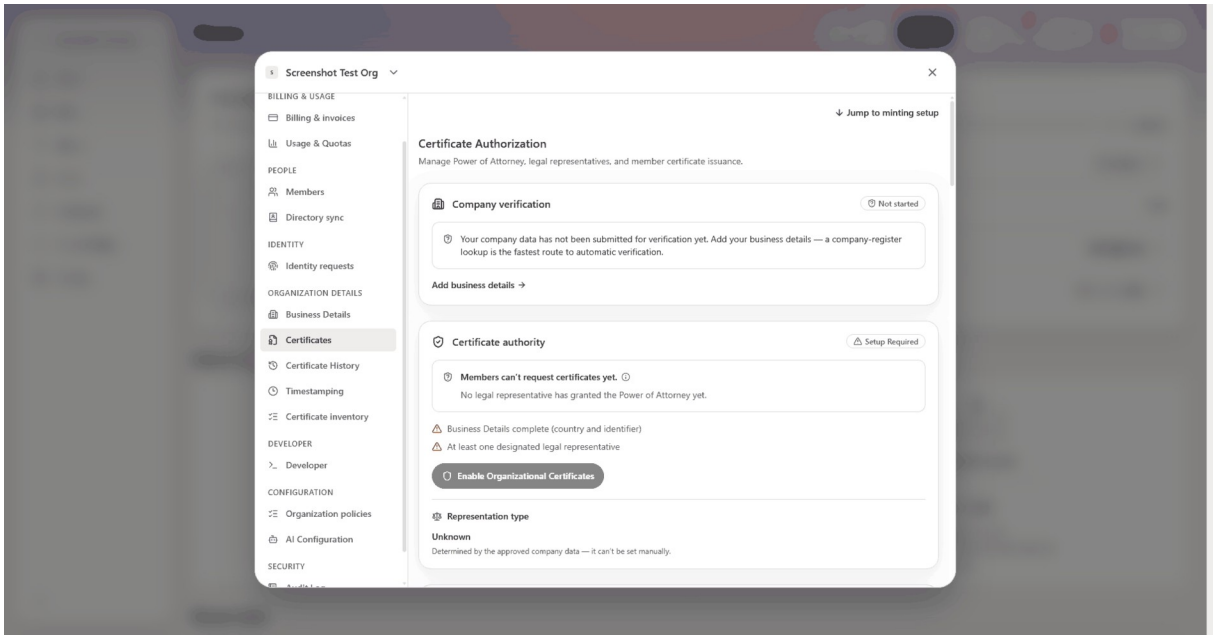
The card then shows **Delegated**, with the date it was granted. The legal representative can withdraw the power of attorney here at any time (**Withdraw delegation**); certificates already issued stay valid.



5.6 Enabling organisational certificates

Once there is a designated legal representative, an owner or administrator enables organisational certificates:

1. Open the organisation's **Certificates** page; the **Set up authority** button in the **Certificate authority** row of the setup checklist also takes you there.
2. Check the prerequisites: **Business Details complete (country and identifier)** and **At least one designated legal representative** (with joint representation, as many as the company's representation rules require).
3. Press **Enable Organizational Certificates**. While a prerequisite is missing, the button cannot be used and says *"Complete all prerequisites first"*.



5.7 Authorisation status and deadlines

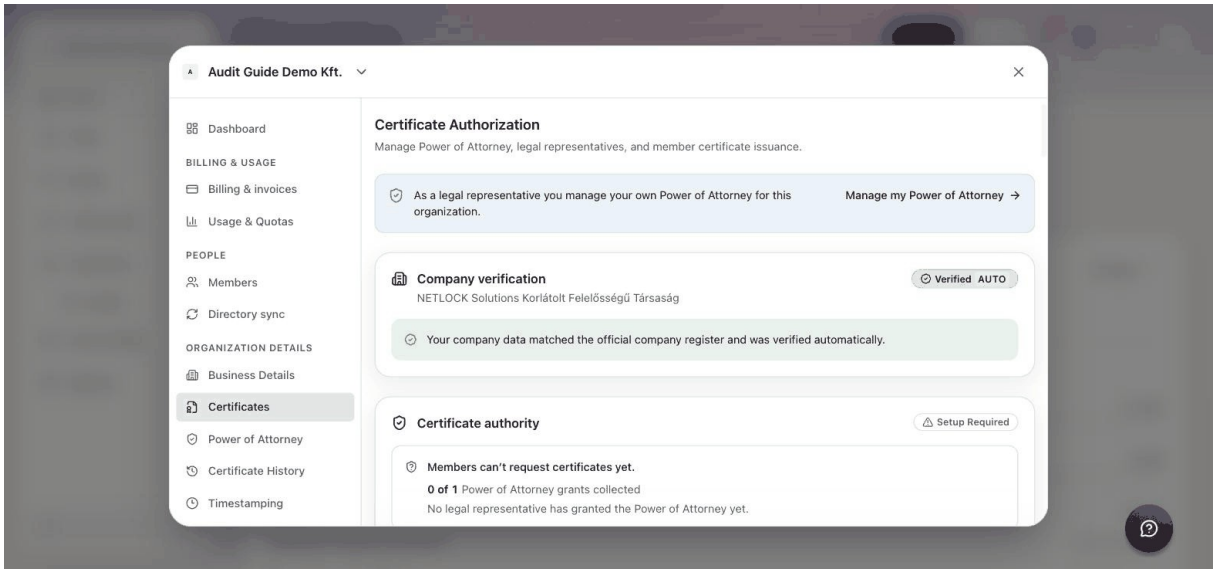
The **Certificate authority** card on the **Certificates** page shows where the authorisation stands:

Status	What it means	What to do
Setup Required	Organisational certificates are not enabled yet.	Carry out the steps in section 5.6.
Signatory Designated, **Pending Signatory Certificate**	The authorisation is waiting for the legal representative's own certificate.	The legal representative finishes the video identification (5.3–5.4).
Pending Authorization, **Partially Authorized**	The authorisation is waiting for the power of attorney; with joint representation, not all of them have been collected yet.	The legal representative, or the other representatives, grant the power of attorney (5.5).
Authorized	The authorisation is complete.	Continue with the purchase (chapter 7).
Revoked	The authorisation was revoked, or a deadline passed.	An owner or administrator restarts it with **Re-initiate Authorization**.
Authorization Paused	A designated representative dropped out; issuing new certificates is paused, existing ones stay valid.	Another legal representative carries out the steps in sections 5.3–5.5.

With joint representation the card also shows how many powers of attorney have been collected (**Power of Attorney grants collected**, for example *1 of 2*).

Deadlines. From the moment the authorisation waits for the legal representative's certificate, they have 30 days for the video identification; after that the power of attorney must be granted within 14 days (with joint representation, every further power of attorney within 14 days too). In the last seven days the card warns, for example: *"Certificate registration deadline in {days} day(s). Please complete the required steps."* If a deadline passes, the authorisation is revoked (**Revoked**) and has to be restarted.

An authorisation that has once become complete stays in force even if the legal representative's own certificate later expires or is revoked; it ends only if the legal representative withdraws the power of attorney.



6. Written power of attorney when the legal representative cannot complete video identification

If the legal representative cannot complete the video identification, they may authorise a member of the organisation to request the certificate with a written power of attorney instead. The Netlock Registration Authority then completes the organisation's authorisation on the basis of the power of attorney.

1. **The authorised person.** Decide who handles the certificate on the organisation's behalf. They need a Netlock account (chapter 2) and must be a member of the organisation (chapter 3); it can be the person who created the organisation.
2. **The business details.** An owner or administrator enters the business details and has them verified (chapter 4).
3. **The content of the power of attorney.** The document states:
    - the organisation's name, tax number and registration number (for example its company registration number);
    - the legal representative's name and position;
    - the authorised person's name, and the e-mail address they registered with in Netlock;
    - the subject of the authorisation: requesting and managing the organisation authentication certificate in the organisation's name, used for EESZT, on the Netlock platform;
    - the date and the legal representative's signature. With joint representation, every representative required signs it.
4. **Signing and sending it.** Send the power of attorney by e-mail to **trust@netlock.com**, with the organisation's name and "EESZT – meghatalmazás" (power of attorney) in the subject, in one of these two ways:
    - signed by hand and scanned, together with the legal representative's specimen signature (*aláírási címpéldány*); or
    - signed with a qualified electronic signature.
5. **Acceptance.** The Netlock Registration Authority checks the power of attorney and lets you know the outcome by e-mail. Once it is accepted, the **Certificate authority** card on the organisation's **Certificates** page shows **Authorized** (5.7). Then continue with the purchase (chapter 7).

7. Buying credits and the certificate

The certificate is bought from the organisation's credits. It is valid for two years, and its fee is paid every year. The current price in credits is shown on the certificate's card in the Store and in the **Options** step of the order.

> **NOTE** Buy only once the **Certificate authority** card shows **Authorized** (5.7). Buying earlier is possible, but issuing is refused until then.

The organisation can spend the credits on other Netlock services too: signing and sponsored signing in the organisation's workspace, storage blocks and timestamping.

7.1 Buying credits for the organisation

If the balance turns out to be too low while buying, you can open the credit purchase from the order window too.

1. Open **Store → Credits** and choose **Buy credits**.
2. The window asks who the credits are for: choose **For the organization** — *"The credits go to the organization's balance, for anyone here to spend."*
3. Choose a credit pack, or enter the number of credits with **Custom amount**, within the range shown in the window.
4. Press **Continue to checkout** and pay on the secure checkout page.

The credits appear on the organisation's balance once the payment arrives, and they are valid for 12 months from the date they are credited.

Owners and administrators can buy credits for the organisation. A member needs the **Can buy credits for the organization** permission, which an owner or administrator can turn on in the member's row on the **Members** page.

7.2 Buying the certificate with credits

The certificate type is available to every organisation by default. If the Store card shows **Request access** instead of **Buy**, the type is not enabled for the organisation: ask for it to be enabled with that button.

1. Open the **Store** and click the **Organization authentication certificate** card.
2. In the overview window press **Buy**. If the organisation already holds an allowance for this certificate, you buy more places with **Add quota**.
3. In the **Add certificates** step, which the window also labels **Options**:
    - in the payment selector, choose the price in credits;
    - in the **Certificates** field, enter how many certificates you buy. The step explains: *"You can hold as many valid certificates at a time as you subscribe to. Revoking one frees its place for a new certificate."* Buy as many as the number of valid certificates you need at the same time;
    - the summary shows the total in the **Total credits** row.
4. Press **Review Order**. The **Review your order** step shows how many credits are taken from the organisation's balance and the current balance (*Your balance*).
5. Press **Confirm Purchase**.

If the balance does not cover the purchase, the button is inactive and reads *"Not enough credits — this purchase needs {n} credits."* Buy credits with the **Buy credits** link (7.1), then continue the order.

The allowance you bought is shown under **Certificate allowances** on the **Usage & Quotas** page.

8. Allowing the user to issue it

Owners, admins and managers can issue the certificate without a separate permission. If another member receives it, an owner or administrator allows them:

1. Open the organisation's **Certificates** page and click the **Jump to minting setup** link.
2. In **Who can issue certificates**, find the **Organization authentication certificate** row and set it to **Specific people**.
3. Click the *Granted to {granted} of {total}* link that appears under the row: the list of members opens.
4. Click the colleague's row. **Grant** at the end of the row changes to **Can issue**. Clicking again takes the permission back.

In the same row, **Everyone** gives the right to every member, including those who join later; **Admins only** clears the permissions given to members. Both ask for confirmation.

9. Receiving the key and the certificate

This step is carried out by the colleague who receives the certificate. The key is created in their browser, so they should do it on the device where the downloaded files can be kept safely.

1. Sign in and switch to the organisation with the organisation switcher at the top of the left-hand menu.
2. Open the **Store**, click the **Organization authentication certificate** card, and in the overview window press **Issue certificate**. The **Issue a certificate** wizard opens.
3. **Certificate type**: the certificate is selected; press **Continue**.
4. **Key**: choose **Generate a key in your browser (recommended)**: *"A fresh key is created on this device. It is never sent to NETLOCK — you download it once, together with the certificate."* You can also upload a CSR of your own; it may carry an EC key or an RSA key of 4096 bits, and an RSA-PSS key is refused.
5. **Names**: there is nothing to fill in. The **Issued to** row shows the organisation's verified legal name, which cannot be edited here. **Name this certificate** is optional (up to 100 characters, for example *EESZT – production*): the name heads the certificate list, becomes the PFX file's friendly name, and names the downloaded files.
6. **Issue**: the **Seats** row of the summary shows that the certificate takes one place from the allowance bought and how many places remain. Press **Issue certificate**.

On the **Certificate issued** screen, download the files. **Do not close the panel until you have downloaded the key:** *"The private key exists only in this browser tab. Download it now — it cannot be recovered after you close this panel."*

1. **Password for the PFX file**: the password protects the PFX file; NETLOCK never sees it and cannot recover it. You have two options:
    - **Use a strong generated password**: copy the password, or tick **I have saved this password** — the download cannot start until you do. The password is shown only here;
    - **Choose my own password**: at least 12 characters, with lower- and upper-case letters and a digit. Do not use accented letters, because some programs cannot open a file with such a password.
2. Press **Download PFX file**. The file holds the private key, the certificate and the issuing CA chain together; if the chain is not available, only the key and the certificate, and the window says so.
3. Under **Other formats** you find **PFX for older systems (.pfx)** for macOS 14 and earlier, Adobe Acrobat and older Windows, and the certificate-only files, such as **Certificate, DER (.cer)** and **Certificate, PEM (.pem)**.

The certificate can then be opened with the **View it in your certificate console** link; **Done** closes the wizard.

> **NOTE** Keep the PFX file and its password. Netlock cannot replace either: if they are lost, the certificate has to be revoked and a new one issued (chapter 11).

10. Switching from the old certificate

This chapter is for organisations that currently use an EESZT certificate issued in the old system.

Who needs to request a new certificate?

- **Organisations whose certificate expires after 17 November 2026.** After that date the old system no longer issues EESZT certificates; a new certificate can be requested only on the Netlock platform. Start the switch in good time, because the legal representative's verification and power of attorney also take time (chapter 5). For certificates issued in the old system we send a notice 30 days before they expire. A certificate that is still valid does not need to be replaced now: switch to the new one before it expires.
- **Organisations whose details have changed.** If details in the certificate — for example the organisation's name, registered office or tax number — change, the existing certificate cannot be modified. A new certificate has to be requested on the Netlock platform.

The steps of the switch

1. **Request the new certificate** on the Netlock platform (chapters 2–9).
2. **Put the new certificate in place of the old one** in the EESZT connection, the same way as the old one was set up. Usually the IT partner who serves the organisation can help with this.
3. **Once the new certificate works, let us know** at trust@netlock.com. Give the organisation's name and tax number, and attach the old certificate's .cer file or give its serial number. On that basis we revoke the old certificate and record the change in the billing details.

NOTE Do not ask for the old certificate to be revoked until you have received the new certificate and set it up in the EESZT connection. You cannot sign in to EESZT with a revoked certificate, and a revocation cannot be undone.

11. FAQ — errors, causes and solutions

Problem (what you see)	Cause	What to do
When issuing the certificate: *"Your organization's authorization is not complete yet: enough of its legal representatives must hold their own organization certificate. …"*	The legal representative has not completed the video identification or has not granted the power of attorney; with joint representation, not every representative required has done so.	Check the status of the **Certificate authority** card on the **Certificates** page and complete the missing step (5.3 –5.7). If the legal representative cannot complete the video identification, send a written power of attorney (chapter 6).
When issuing, the application says that the organisation's authorisation has been revoked, or: *"This organization's certificate authorization expired before it was completed. An administrator must re-initiate it before certificates can be requested."*	The authorisation was revoked, or the deadline for the video identification (30 days) or for the power of attorney (14 days) passed.	An owner or administrator restarts it with **Re-initiate Authorization** on the **Certificate authority** card, and the legal representative completes the missing step (5.7).
During the video identification: *"You aren't listed as a legal representative of this organization."*	The name or date of birth on the document does not match the company's registered officers.	An administrator checks the **Legal representatives** list on the **Business Details** page (4.3); then the legal representative starts the video identification again (5.3). If the data is correct, contact Customer Service.
On the **Home** page or the **Certificate authority** card: *"Certificate registration deadline in {days} day(s). …"* or *"PoA authorization deadline in {days} day(s). …"*	The deadline for the video identification or for the power of attorney is near.	The legal representative completes the step before the deadline (5.3–5.5).
On the **Business Details** page the legal representative's row does not show **Candidate**.	The account name does not match the name in the register, or the legal representative has not accepted the invitation yet.	An administrator invites them from the officer's row (**Invite**), or assigns the member (**Assign member**) (5.2).
Enable Organizational Certificates cannot be used: *"Complete all prerequisites first"*.	The business details are incomplete, or there is no designated legal representative yet.	Finish verifying the business details (chapter 4) and the legal representative's video identification (5.4).
You sent the written power	The Registration Authority	Wait for the reply by e-mail;

Problem (what you see)	Cause	What to do
of attorney, but the **Certificate authority** card does not show **Authorized** yet.	has not processed the power of attorney yet, or it was incomplete.	if none arrives, contact Customer Service (trust@netlock.com, +36 1 437 6655) (chapter 6).
The wizard says *"Minting for this certificate is delegated — ask an organization admin to grant you issuance access."*	The colleague has not been allowed to issue the certificate yet.	An owner or administrator allows them (chapter 8).
The wizard says *"Not included in your organization's plan yet — an organization admin can add it from the Store."*	The organisation has not bought this certificate yet.	An owner or administrator buys it (7.2).
The wizard says *"Ask an organization admin to add quota for this certificate."*	Every place bought is taken by a valid certificate.	An owner or administrator buys another place with **Add quota** (7.2), or revokes a certificate no longer in use.
The wizard says *"Your organization isn't entitled to this certificate type yet — it must be enabled for your organization before it can be issued."*	The certificate type is not enabled for the organisation.	An owner or administrator asks for it to be enabled with **Request access** on the certificate's card in the Store (7.2), or contacts Customer Service.
The wizard says *"Your organization's business details (legal name and registration identifier) must be set before a certificate can be issued."*	The organisation has no business details.	An owner or administrator enters them and has them verified (chapter 4).
After issuing: *"The certificate authority declined this request. This certificate carries your organization's verified name, so its subject was filled in automatically — there is nothing to correct in this form. Contact support and quote the reference below."*	The certification authority did not accept the organisation's name in the certificate; this happens when the name is not among the names verified for the organisation.	Check on the **Business Details** page whether the banner says *"Your company data has been verified."* (4.2). If it does, contact Customer Service and quote the reference shown under the message.
In the **Review your order** step of the order: *"Not enough credits — this purchase needs {n} credits."*	The organisation's credit balance does not cover the purchase.	Buy credits for the organisation with the **Buy credits** link (7.1), then confirm the order.
The wizard says *"There aren't enough credits to issue this certificate. Once the*	The organisation's credit balance does not cover the issue.	An owner or administrator buys credits (7.1), then the colleague starts issuing again.

Problem (what you see)	Cause	What to do
balance covers it, start again from your certificate list; anything that did go through is listed there."		
The credit purchase window says *"Your account is not allowed to buy credits for the organization, and nothing was charged."*	As a member, only someone with a separate permission can buy credits on the organisation's behalf.	An owner or administrator buys them, or turns on **Can buy credits for the organization** for the member on the **Members** page (7.1).
Buy is inactive: *"You do not have permission to complete this action. Ask an organization admin."*	Your account cannot buy on the organisation's behalf.	An owner or administrator makes the purchase (7.2).
The banner on the **Business Details** page: *"Your company data has been submitted to the NetLock Registration Authority for manual verification."*	The Registration Authority is still verifying the business details.	Wait for the outcome; continue with the next steps after the verification (4.2).
The PFX file or its password is lost, or the panel closed before the key was downloaded.	The key was created only in the colleague's browser and Netlock does not know the password, so neither can be replaced.	An owner or administrator revokes the certificate: on the **Certificates** page, select it, choose **Revoke**, give the reason and type the confirmation `REVOKE 1`. This frees the place, and the colleague issues a new one (chapter 9).
An older Windows, macOS 14 or Adobe Acrobat does not open the PFX file.	The default PFX file uses newer encryption that these programs do not know.	When downloading, choose **PFX for older systems (.pfx)** under **Other formats** (chapter 9). If the panel is already closed, the key cannot be downloaded again: revoke the certificate and issue a new one.
The old certificate has been revoked, and you cannot sign in to EESZT.	The revocation was asked for before the new certificate was set up.	A revocation cannot be undone. Request and set up a new certificate as soon as possible (chapters 2–9); if you get stuck, contact Customer Service (trust@netlock.com, +36 1 437 6655).