ADACOM

SECURITY BUILT ON TRUST

# FAQ FOR ADACOM QUALIFIED CERTIFICATES

## General Information

1. **What is a Key Pair?**
   In the terminology of Public Key Infrastructure (PKI), a key pair consists of a public key and a private key. These two keys are mathematically linked and provide asymmetric cryptography between them.
2. **What is a Public Key?**
   The public key is used to verify the electronic signature. It is associated with the private key and can be made publicly available.
3. **What is a Private Key?**
   The private key is used by the Subscriber to create an electronic signature. The private key is known only to the Subscriber and remains confidential.
4. **What is PKI (Public Key Infrastructure)?**
   PKI is a combination of software, cryptographic technologies, procedures, and services used for the creation, management, distribution, use, and revocation of digital certificates. It is a system that links public keys to users, each of whom has a specific role and unique identity.
5. **What is a Certification Authority (CA)?**
   A Certification Authority (CA) is a trusted third party responsible for issuing and managing digital certificates.
6. **What is a Qualified Signature Creation Device (QSCD)?**
   A Qualified Signature Creation Device (QSCD) is a secure device used to generate and store Qualified Electronic Signature Certificates. It must meet the evaluation criteria outlined in Annex II of Regulation (EU) No. 910/2014. Such devices include USB Tokens or remote QSCDs.

## Adacom e-shop

7. **How can I obtain a Qualified Signature Creation Device (QSCD)?**
   You can purchase a QSCD either online through ADACOM's e-shop at https://eshop.adacom.com , or by contacting the ADACOM sales department at +30 210 5193700.
8. **How will I know that my digital signature is about to expire?**
   One (1) month prior to your certificate's expiration, you will begin receiving notification emails at the address you provided during registration.
9. **What steps are required to renew my digital signature?**
   To renew your digital signature, visit https://eshop.adacom.com , or contact our commercial team directly at qc@adacom.com to place your new order. Once the payment has been completed, you will receive instructions for the technical steps as well as the identification procedure required for the new certificate issuance.

## AQS Portal Registration

10. **Do I have an account on the Adacom Portal?**
    You can easily check whether you already have an account on the Adacom Portal by attempting to register as a new user. If your details (such as email or ID number) are already associated with an active account, you will receive a message indicating that some of the information is already in use. In that case, proceed to log in to your existing account.
11. **What is my password for the Adacom Portal?**
12. If you don't remember your password, you can follow the password recovery procedure. Click Here to go to the login page and select **"Forgot your password"** below the **Sign In** button.

ADACOM
SECURITY BUILT ON TRUST

# FAQ FOR ADACOM QUALIFIED CERTIFICATES

13. **How should I complete the registration form?**
14. Your details must be entered exactly as they appear on the identification document you will use for verification (ID card or passport). You may enter your name in either Greek or Latin characters. The ID number must be entered in full (letters and numbers) and cannot be transliterated between alphabets. Pay special attention to entering your email address and mobile phone number correctly, as any mistake may prevent successful account activation.
15. **What does "Your Account is Disabled" mean?**
16. After submitting your registration form, a confirmation link will be sent to your email address. You must click this link to activate your account. If you try to log in without activating, you will see the message "Your Account is Disabled." Please check your inbox for the activation email. If you cannot find it or the link doesn't work, contact us at trust-support@adacom.net to request a new one.
17. **What is the OTP code required to log in?**
    The OTP (One-Time Password) is a 5-digit code you will receive each time you attempt to log in. It is required to access your account. The code will be sent to your email address from aqs-portal@adacom.com . Alternatively, you may wait two minutes and request a new OTP to be sent via SMS to your registered mobile number.

## Application on the AQS Portal

18. **I'm being asked for a Certificate Receipt Code. What is it and where can I find it?**
    The Certificate Receipt Code is a unique code generated when you placed your order. It contains information about the type of certificate you purchased and the identification method you selected. You will receive this code by email shortly after your order has been submitted and payment has been completed.
19. **I can't find the Certificate Receipt Code in my email.**
    The code, along with detailed instructions, is sent to the email address you provided during the ordering process shortly after payment. If you haven't received it, please contact our commercial team at qc@adacom.com to inquire about the status of your order.
20. **When submitting a new application, I receive the message "You already have an active certificate of this type." What should I do?**
    If you have an active certificate that you wish to renew, you must wait until the certificate is due to expire within a month or less. During that period, you should log in to your AQS portal account, go to "My Certificates," and submit the Certificate Receipt Code you received via email.
21. **What is the "Serial Number Type" and which one should I choose?**
22. The Serial Number field refers to a value that will be embedded in your certificate. You can enter either a random code with no personal information (automatically generated by the system), your Tax Identification Number (TIN), or your National ID/Passport Number, depending on the type of ID you selected. There are no strict requirements, but keep in mind that this value will be visible to anyone receiving a digitally signed document from you.
23. **What identification methods are available?**
    You can find all required documentation for identification here depending on the type of certificate you have acquired. You can also review all available identification methods and acceptable identification documents here
24. **Can I verify my identity by sending digitally signed documents?**

Yes, if you already hold a valid Qualified Electronic Signature Certificate, you may digitally sign the required identification documents and submit them either via email to lra@adacom.com or by uploading them through your AQS portal profile.

Note: This method can only be used once and only if the identification document (e.g., ID card or passport) remains valid and unchanged.
The Subscriber must confirm that their current certificate was originally issued through face-to-face verification. On the next renewal, in-person identification will be required.

25. **I received an email stating my application was approved. What are the next steps?**
    To issue and retrieve your certificate, refer to the guide sent to you via email from **aqs-portal@adacom.com** . Alternatively, you can find all our user guides here. The steps related to certificate pickup are detailed in Section 5.

## Remote Certificate Pickup

26. **What does "The QR code is invalid" mean?**
    If you scan the QR code displayed on your computer screen and receive this message, you are likely on step 2 of the process, which involves downloading and installing the Adacom Authenticator app on your mobile device. Click Next to proceed to step 3 and try scanning the new QR code that appears.
27. **I clicked "Enrollment" and I'm being asked for codes I don't know or have lost. What should I do?**
    If you have an active RSA account linked to a valid certificate, the portal will prompt you to activate your new certificate using the same account. To proceed, you will need both your **RSA code** and the **OTP (extended)** code from the *Adacom Authenticator* app on your phone.
    If you don't have one or both of these codes:
    1. Go to **My Certificates** and choose **Revoke** for your current certificate.
    2. Then go to **Remote Signature Accounts** and delete your active account.
    3. Finally, return to **Certificate Applications > Remote Certificate Applications** and repeat the enrollment process.

    This time the system will guide you to create a new RSA account and generate a new OTP code.

## Local Certificate Pickup

28. **I already have a digital signature. Which steps can I skip?**
    If your USB token already contains a digital signature, you may already have one or both of the required software drivers installed for certificate activation and retrieval.
    Check whether you have the following installed on your computer:
    - SafeNet Authentication Client Tools (Gemalto 5110 CC)
    - Bit4id xapp (Adacom USB Driver)

    If both are present, you can proceed directly to certificate installation. If either is missing, you can download and install them from here.
29. **I've forgotten or locked the user passwords for my token. How can I reset them?**
    If you've forgotten your token's user passwords or one of them has been locked due to repeated failed attempts, follow the steps outlined here to unlock your token and set new passwords. Note: These instructions assume you've kept the Default Administrator Password and Digital Signature PUK. If you've changed them, you'll need to enter the new credentials to proceed.

30. **I changed the Administrator and PUK codes and can't remember them. What can I do?**
    Unfortunately, if you no longer remember the updated Administrator Password or Digital Signature PUK, it is not possible to unlock your token. In this case, you will need to purchase a new e-Token device and revoke any active certificate stored on the old token, then reissue the certificate.
    To do so:
    - Visit the Adacom e-Shop to order a new token.
    - Contact customer support at trust-support@adacom.net for instructions on revocation and reissuance.
31. **During registration I get the message "Client Disconnected" and the process gets stuck at "Please Wait."**
    In this case, try refreshing the portal page and starting the registration process again.
    Keep in mind that the driver software runs for a limited time, during which the process must be completed.
    If you're unsure whether your credentials are correct, click here to reset them before restarting.
32. **During registration I receive the message: "Token Memory Full, Please delete Orphan Objects.**
    This means your token contains old certificates or failed issuance attempts ("orphan objects").
    You will need to clear them and restart the process. Follow the cleanup instructions here.
33. **I click "Launch Client" but the page doesn't respond.**
    First, check whether the **Bit4id xapp (Adacom USB Driver)** is installed on your computer. If not, download and install it from here. If the software is installed but the process still doesn't continue, it may be blocked by local or network-level security policies. In that case:
    - Contact your IT department to disable firewall restrictions, or
    - Try from a personal computer on a non-corporate network.

    Note: The registration needs to be completed only once. After that, you can sign documents from any computer.

## Using Remote Certificates

34. **How can I use my remote certificate to digitally sign documents?**
    The steps for digitally signing documents using your remote certificate are described in Section 7 of the user guide available here. To begin the signing process, visit: https://aqs-sign.adacom.com/
35. **I receive the message "Invalid Username or Password" when trying to log in. How do I log in and reset my credentials?**
    Your **username** was automatically generated by the system when your certificate was issued, and your **password** was set by you during **Step 3** of the issuance process.
    - The username **cannot be changed.**
    - You can **change your password** either:
      - From within the Adacom Portal at **Remote Signature Accounts > Change Password**, or
      - From the remote signature account login page, as long as you remember the current password.

    For security reasons, the password **cannot be recovered** without knowing the current one. If you don't remember your username or password, please contact **trust-support@adacom.net** for assistance.
36. **I receive the message "Account Locked due to many failed login attempts."**
    If your account is locked due to too many failed login attempts:
    1. Log in to your administrator account at: https://aqs-portal.adacom.com/aqs-portal/login.xhtml

2. Navigate to **Remote Signature Accounts > Unlock**
3. You will receive the message **"RSA Account Unlocked"**, and your login attempts will be reset.

You can then try logging in again at https://aqs-sign.adacom.com

**37. Can I customize the appearance of my digital signature?**

Yes. The aqs-sign platform allows you to personalize how your digital signature appears on documents.To configure your signature: Log in at https://aqs-sign.adacom.com, click your name in the top-right corner select My Signatures. You can choose from the following options:

- Sketch: Draw your signature with a mouse or touchscreen
- Type: Type your name or custom text and select a font
- Upload: Use an image file of your handwritten signature or stamp

**38. I changed mobile device and the Adacom Authenticator shows the message "No QR codes have been scanned." How can I recover my OTP?**

To recover your OTP on a new device, you need to scan the QR code that was displayed on your computer during the certificate issuance.

If you no longer have this code saved, your certificate will need to be revoked and reissued.

Please send your request to trust-support@adacom.net to receive personalized instructions.

**39. I'm trying to upload a document for signing, but the process fails or I get a generic error.**

First, check the file type and file name:

- Files should preferably be in PDF format (or alternatively Word format).
- Make sure the filename contains only Latin characters (no Greek letters, symbols, or special characters).

Rename the file and try again.

**40. After entering my password and extended code, I get an error and the signature process fails.**

Check whether your password is being auto-filled by your browser. If so:

- Delete the saved entry from your browser's keystore, or
- Try using a different browser for signing.

If the issue persists, it may be due to an **unsynchronized OTP code**. To synchronize your OTP with the server time, follow the steps outlined here.

# Using Local Certificates

**41. How can I use my digital signature stored on a USB Token?**

You can find our PDF guide with step-by-step instructions for signing documents using Adobe Acrobat Reader DC here. If you plan to participate in public tenders, we recommend setting up **timestamping** through the Acrobat Reader menu by following the instructions provided here.

**42. I sign a document and get the message "Signature Validity Unknown." What should I do?**

This message from Adobe Acrobat usually indicates that your trust lists need to be updated.

Follow the steps in the guide here. To update your trust settings. Afterward, restart Acrobat Reader and open the signed document again. If the issue persists, contact us at trust-support@adacom.net

**43. Can I customize how my signature appears on a document?**

Yes. Acrobat offers several customization options: Open Acrobat and go to Edit > Preferences > Signatures > Creation & Appearance > More > New In the "Configure Signature Appearance" window, you can: Upload a scanned signature or stamp image (PDF file) under Configure Graphic > Imported Graphic > File Choose which textual information appears under Configure Text Name your custom

appearance in the Title field. Click OK, then close and reopen Acrobat to apply the new appearance. From now on, you will see your custom appearance listed in the Appearance dropdown, alongside "Standard Text

44. **My token is locked. How can I unlock it?**
    To unlock your token and reset your passwords, click here to access the relevant guide.

# Class1/2

45. **How should I fill in the application details?**
    For Class 1 certificates, there are no restrictions on the display name.
    You may choose a name that reflects the identity under which you will be signing (preferably your full name in Latin characters).
    For Class 2 certificates, stricter validation is applied to the organization name and identification number (Tax ID or GEMI number).These fields must exactly match the information on the company's official documents, and verification is performed through the GEMI platform. If you wish to use a name that does not appear in GEMI, you must provide additional documentation to support the requested name.
46. **The link for retrieving my certificate says "Invalid." What should I do?**
    The certificate download link has a limited lifespan.
    If the link has expired, please contact us at **trust-support@adacom.net** to request a new one.
47. **The steps shown on my screen during certificate pickup seem unfamiliar. What do they refer to?**
    These steps relate to importing your certificate into the Firefox browser keystore. This is optional and only relevant if you plan to use your certificate for encrypted email exchange or e-invoicing (Class 2 only). If this does not apply to you, you can ignore those steps and follow the instructions you received from aqs-portal@adacom.com.
48. **I followed the guide, but I'm not sure if my certificate was successfully installed. How can I check?**
    If you're using a Windows 8 or newer PC, you can check your certificate in Microsoft Edge: Go to Settings > Privacy, search, and services > Security > Manage Certificates. Search for a certificate whose expiration date is 365 days after issuance (i.e., when you completed the guide steps)
49. **I think I completed all the steps but I can't find my certificate. What should I do?**
    Please contact us at **trust-support@adacom.net** so we can verify whether your certificate was successfully issued.
50. **I found my certificate but can't send encrypted or signed emails. Are there extra steps required?**
    Yes. To use your certificate for email signing and encryption, you must configure your email client to recognize the certificate. You can find the setup instructions for Microsoft Outlook here If you're using a different email client, please refer to its documentation for **S/MIME certificate integration**.
51. **I can send signed emails, but when I try to encrypt them, I receive an error saying one or more recipients do not have a valid encryption certificate. What should I do?**
    To send encrypted email, you must have the recipient's public key stored in their contact entry in your email client. The easiest way to add it in Microsoft Outlook is:
    - Locate a previously signed email from the recipient
    - Right-click on their name and select Add/Edit Contact
    - Ensure their certificate appears under the Certificates tab and click Save and Close

    When composing a new encrypted email, choose the recipient from your saved contacts