BANCO DE ESPAÑA
Eurosistema

INFORMATION TECHNOLOGY COMMITTEE

ESCB-PKI PROJECT

ESCB-PKI REGISTRATION AUTHORITY APPLICATION

MOST COMMON ERRORS

VERSION 1.2

ECB-PUBLIC
15-November-2012

TABLE OF CONTENTS

TABLE OF ILLUSTRATIONS

Project name:	ESCB-PKI
Author:	ESCB-PKI Project team
File name:	ESCB-PKI - Common errors v.1.2.docx
Version:	1.2
Date of issue:	15.11.2012
Status:	Final
Approved by:	
Distribution:	

RELEASE NOTES

In order to follow the current status of this document, the following matrix is provided. The numbers mentioned in the column “Release number” refer to the current version of the document.

Release number	Status	Date of issue	Revisions
0.1	Draft	09.03.2012	Initial version
0.2	Draft	21.03.2012	Additional revision
1.0	Final	28.05.2012	First version
1.1	Update	27.07.2012	“Important Notice” added at the beginning of chapter 2
1.2	Update	15.11.2012	Added generic browser error

GLOSSARY AND ACRONYMS

Acronym	Definition
CA	Certificate Authority
CB	ESCB Central Bank (ECB or NCB)
CRL	Certificate Revocation List
ECB	European Central Bank
ESCB	European System of Central Banks, including the ECB and the NCBs of all States member of the European Union (whatever they use the Euro or not).
ESCB-PKI	European System of Central Banks - Public Key Infrastructure
IAM	Identity and Access Management
NCB	National Central Bank
PKI	Public Key Infrastructure
RO	Registration Officer

1. INTRODUCTION

This document aims at providing information of the most common errors you could find when you are managing ESCB-PKI certificates.

This first chapter introduces some concepts that could be useful to better understand how ESCB-PKI requests, certificates and sessions are handled. Next chapters will depict the usual errors; this document describes for every error the most probable causes and the actions you must undertake to solve it.

1.1. CERTIFICATE REQUEST STATE FLOW

The status of a certificate request can be:

– ***RO-Pending*** The RO shall still process the request

– ***User-Pending*** The user can generate and download the certificates. The RO has already handled the request and has allowed a remote download

– ***Completed*** The request has been processed and certificates have been generated

– ***Cancelled*** The request has been cancelled

– ***Expired*** The request has expired

The figure below shows the flow between the different statuses for a given request:

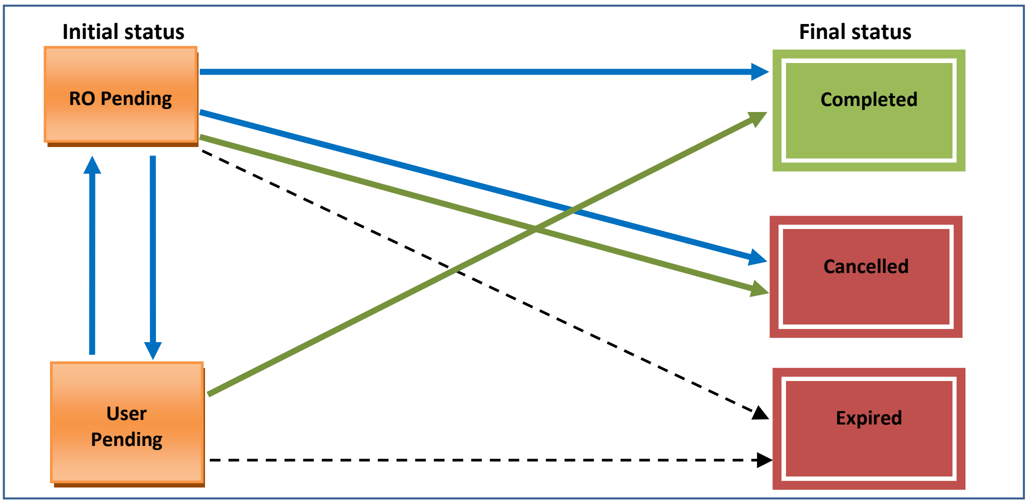


Figure 1 - Certificate requests status flow

Line convention:
Blue Actions performed by the Registration Officer
Green Actions performed by the end-user
Black Actions performed by ESCB-PKI periodic processes (under construction)

Box convention:
Orange (Intermediate status) the request cannot remain in this status for a long period
Green (Final status) the request has been completed: certificates have been issued
Red (Final status) the request has been cancelled / expired: certificates have not been issued

1.2. CERTIFICATE STATE FLOW

The status of a certificate can be:

– ***Active***	Certificates are valid
– ***Revoked***	Certificates cannot be used any more
– ***Suspended***	Certificates have been temporarily invalidated
– ***Damaged***	Certificates have been replaced due to damage (e.g. broken token)
– ***Renewed***	Certificates have been replaced due to expiration
– ***Expired***	Certificates have expired

The figure below shows the flow between the different statuses for a given certificate:

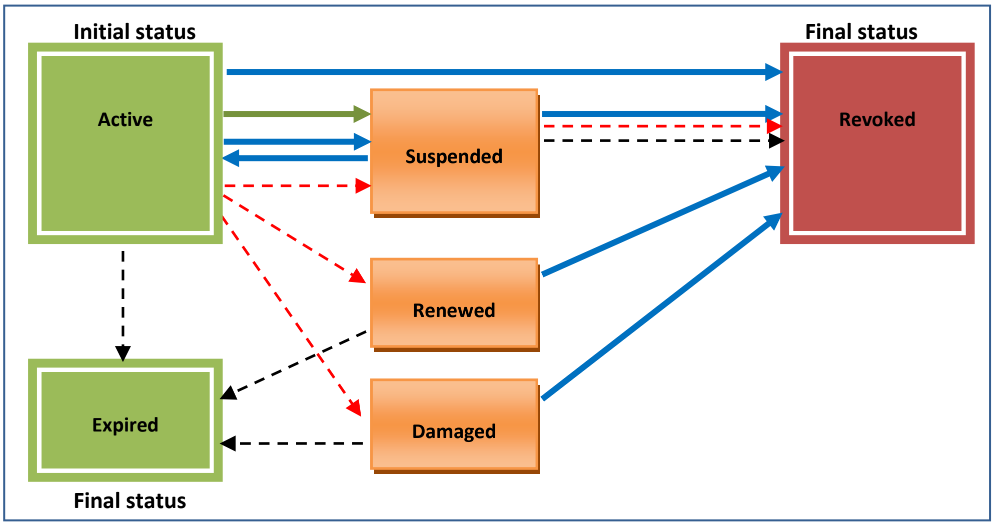


Figure 2 - Certificate package status flow

Line convention:

Blue	Actions performed by the Registration Officer
Green	Actions performed by the end-user
Black	Actions performed by ESCB-PKI periodic processes
Red	Action automatically executed as a result of a new certificate request due to: key compromise[1], expiration[2] or damage[3]

Box convention:

Orange	(Intermediate status) the certificate will not remain in this status for a long period
Green	(Stable status: initial or final) for a non-revoked certificate
Red	(Final status) for a revoked certificate

[1] Old certificates are initially suspended and afterwards, when the new certificate is issued, revoked

[2] Status of old certificates is changed to "renewed"

[3] Status of old certificates is changed to "damaged"

1.3. IAM LOGON: SSO AND BROWSER SESSION

It is very important to understand how IAM SSO works and how the browser (i.e. Internet Explorer) manages the sessions.

When you log-in to the IAM system (providing your identity & credentials) a new session is created (cookie session). This IAM session is linked to the browser session.

This means that once you have been authenticated by the IAM WAM to access to one application:

- If you remain within the same browser session, IAM will not authenticate you again the next time you select another application protected by the IAM WAM, therefore, the access to the new application will be done with the same credentials you presented before.
- Only if the new application needs stronger credentials (i.e. you have authenticated using a software certificate and the new application requires advanced certificates) you will be requested to authenticate again.
- If you need to use different credentials for two applications that require the same level of authentication (i.e. both use standard certificates), you must open a new browser session:
    - In IE7 you will need to open a new explorer, but
    - In IE8 (or above) you will need to explicitly choose to open a new session (by default IE8 and IE9 will not open new session)

1.4. ESCB-PKI APPLICATION SESSION AND LOG-OFF

Apart from the IAM session the ESCB-PKI system creates another session associated to the application. Two different sessions may be created:

- One associated to the tool used by ESCB-PKI Registration Officers and other ESCB-PKI roles (e.g. Key Recovery Officer, etc.), that is, people that have been granted a role in the system
- Another one associated to the tool used by ESCB-PKI subscribers

When you log-off from the ESCB-PKI application, your ESCB-PKI session cookie will be invalidated to avoid the risk of being used without your control. If you want to access to the ESCB-PKI tool later, you must open a new browser session and re-authenticate.

2. ACCESS TO THE ESCB-PKI APPLICATION NOT GRANTED

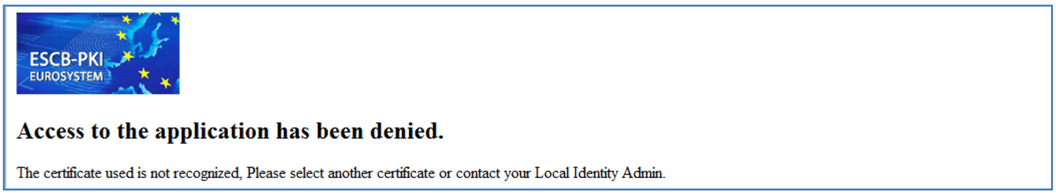
IMPORTANT NOTICE

Please, take into account that once you receive an Access error (any of the errors described below in this chapter) you MUST CLOSE THE BROWSER SESSION AND OPEN A NEW ONE (see paragraph 1.3 IAM logon: SSO and Browser session) before trying again.

Even though you had put in place the corrective actions, you will receive the same error if you DO NOT open a new browser session.

1. *IAM: Certificate not recognised*

IAM error:



Access to the application has been denied.

The certificate used is not recognized, Please select another certificate or contact your Local Identity Admin.

Reason:

Your certificate is not associated to a valid user-id in the IAM directory. Three main reasons can cause this error:

a) You are not using the correct certificate.

b) Your certificate is not associated to your IAM account yet (Note: the ESCB-PKI application sends your certificates to IAM when you receive the "*Certificate issuance confirmation*" e-mail).

c) Your certificate is not yet registered in your browser (Note: the certificates are registered the first time you open your browser with your card inserted in the reader).

Action:

a) Verify that you are using the correct certificate (issued by a CAF compliant PKI).

b) Verify that your certificate is associated to your account in the IAM directory[4].
   If you are using an ESCB-PKI certificate:
   - If you have just obtained your certificate wait until you receive the "*Certificate issuance confirmation*" e-mail containing the serial numbers of the certificates issued[5] and try again.
   - If you have received this e-mail and the certificate(s) is(are) not published in the IAM IDM, contact your Local Help Desk to communicate the error to the ESCB-PKI coordinating service desk.

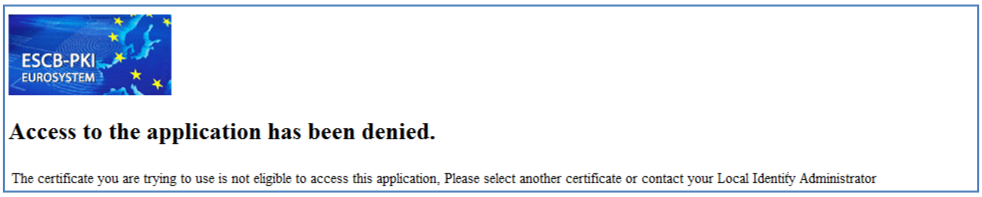
c) Close the browser session, open a new session and try again. Verify that your certificate is registered in your browser.

[4] Use IAM IDM tool.

[5] The ESCB-PKI sends this message at the same time it publishes your certificates in the IAM IDM directory.

2. *IAM: Certificate not eligible*

IAM error:



Access to the application has been denied.

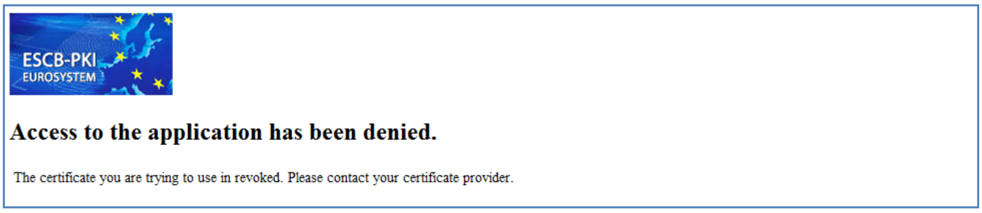
The certificate you are trying to use is not eligible to access this application, Please select another certificate or contact your Local Identify Administrator

Reason:
You are trying to access to https://ra.pki.escb.eu/epkmain using a software certificate.

Action:
You must use an advanced certificate (smart card).

3. *IAM: Revoked Certificate*

IAM error:



Access to the application has been denied.

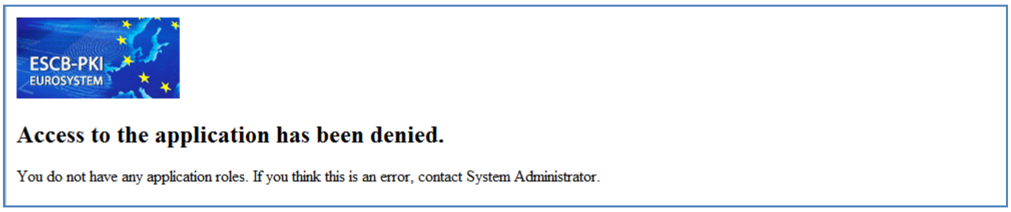
The certificate you are trying to use in revoked. Please contact your certificate provider.

Reason:
You are using a revoked (or suspended) certificate.

Action:
Verify you are using the correct certificate.
If your certificate is suspended you must reactivate it.
If your certificate is revoked you must request a new certificate.

4. *IAM: No roles*

IAM error:



Access to the application has been denied.

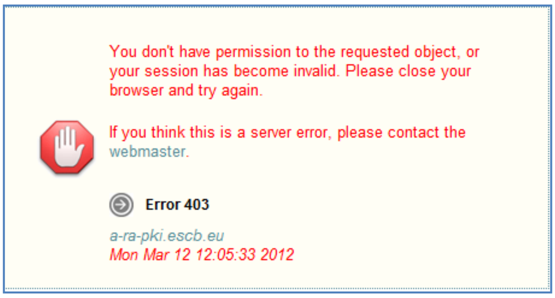
You do not have any application roles. If you think this is an error, contact System Administrator.

Reason:
You are trying to access to https://ra-pki.escb.eu/epkmain but you have not been granted any role in the ESCB-PKI system.

Action:
If you think you must have a role, please verify it looking for your Roles in the IAM IDM.
If you have being granted an ESCB-PKI role and you can't access to the application, please contact the IAM Coordinating service desk.

5. *ESCB-PKI session invalidated*

ESCB-PKI error:



You don't have permission to the requested object, or your session has become invalid. Please close your browser and try again.

If you think this is a server error, please contact the webmaster.

Error 403

a-ra-pki.escb.eu
Mon Mar 12 12:05:33 2012

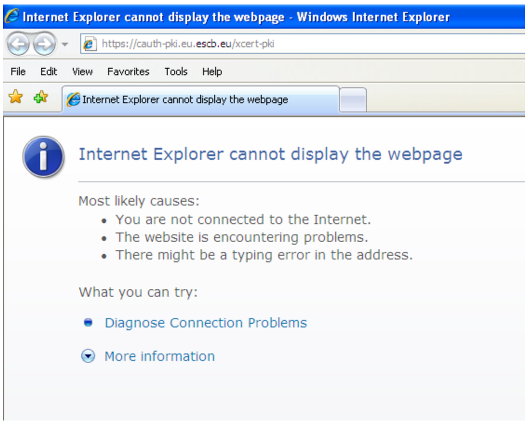
Reason 1:
You will receive this message if you have logged-off from the ESCB-PKI application and afterwards you try to access to the application again from the same browser session.

Action 1:
Open a new browser session to access to the ESCB-PKI application. Another option is that you close all the instances of your browser and open a new one.

Reason 2:
If you receive this error after having closed all the instances of your browser, as described above, another reason of this error is that your user account have not been propagated correctly to the ESCB-PKI system when it was created in the IAM infrastructure.

Action 2:
Contact your local Help Desk to communicate the error to the ESCB-PKI coordinating service desk.

6. *Generic browser error*



Internet Explorer cannot display the webpage - Windows Internet Explorer

https://cauth-pki.eu.escb.eu/xcert-pki

Internet Explorer cannot display the webpage

Most likely causes:
- You are not connected to the Internet.
- The website is encountering problems.
- There might be a typing error in the address.

What you can try:

Diagnose Connection Problems

More information

Reason 1:
The ESCB-PKI application has requested to present a client certificate to authenticate and you have not got selected one

Action 1:
Obtain your authentication certificate and select it while accessing the application

Reason 2:
The PIN of your cryptographic token is locked

Action 2:
Unlock the PIN of your cryptographic token

3. CERTIFICATE REQUEST REJECTED

7. *Certificate request rejected*

E-mail:

Dear ESCB-PKI user,

Unfortunately, your certificate request has been rejected because there is another request that has not been completed yet.

Please complete the existing request or contact your Registration Officer to cancel it.

Reason:

You have requested new certificates but you already have another request in pending status (status “ro-pending” or “user-pending”).

Action:

You may either complete the existing request or cancel it and afterwards make the new request.

8. *New certificate request rejected*

E-mail:

Dear ESCB-PKI user,

Unfortunately, your request for new certificates has been rejected because you already have got valid certificates.

Please initiate a new request and select a more appropriate operation (e.g. renewal for certificate expiration)

Reason:

You requested a “new certificate” and you already have a valid certificate. A valid certificate is an “active” or “suspended” certificate.

Action:

If you need new certificates because your old keys:

- Have been compromised; make a request indicating the reason: LOST CERTIFICATE.
- Have been damaged; make a request indicating the reason: REPLACED TOKEN / UNRECOVERABLE CERTIFICATE.
- Are closed to expire; make a request indicating the reason: CERTIFICATE EXPIRATION.

9. *Certificate renewal request rejected*

E-mail:

Dear ESCB-PKI user,

Unfortunately, your request for the renewal of your certificates has been rejected because you either have not got certificates or they are not about to expire.

For your information, ESCB-PKI certificates can be renewed only during their last 100 days of life.

Please initiate a new request and select a more appropriate operation (e.g. renewal for replaced token or unrecoverable certificate)

Reason:

You have indicated in your request the reason: CERTIFICATE EXPIRATION, but certificates can only be renewed during their last 100 days of life.

Action:

If you do not have any certificate, make a request indicating the reason: NEW CERTIFICATE.

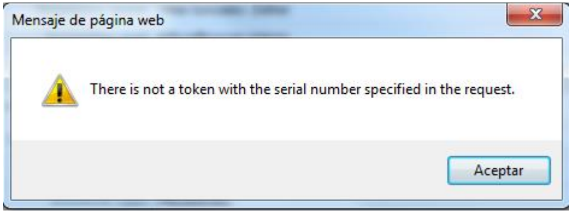
If you need new certificates because your old keys:

- Have been compromised; make a request indicating the reason: LOST CERTIFICATE.
- Have been damaged; make a request indicating the reason: REPLACED TOKEN / UNRECOVERABLE CERTIFICATE.

4. CERTIFICATE GENERATION MOST COMMON ERRORS

10. There is not a token with the serial number specified in the request

EPK application error:



Mensaje de página web

There is not a token with the serial number specified in the request.

Reason:

You are in the process of generating advanced certificates and

a) The smart card is not correctly inserted in the reader.

b) The smart card used is not the one indicated in the request.

Action:

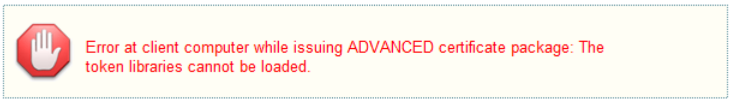
a) Verify that you have the smart card correctly inserted in the reader

b) If the serial number indicated in the request was mistaken, you can correct it. Take into account that the modification of the serial number of the token can only be done if the status of the request is still ro-pending. If the status of the request is user-pending[6] you must:

- contact your Registration Officer to change back the request to the ro-pending status,
- modify the SN of the request,
- print and sign the new terms and conditions document, and
- send it again to your Registration Officer.

11. Client error downloading certificates

EPK application error:



Error at client computer while issuing ADVANCED certificate package: The token libraries cannot be loaded.

Reason:

Typically you will receive this message if you are using the wrong driver for your smart card reader.

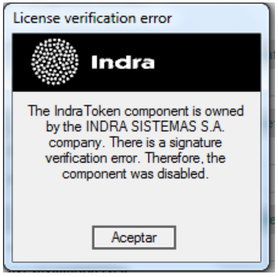
Action:

Verify that you have the correct version of your driver (the last version valid for your operating system) and try again.

[6] This implies that you have already send the terms and conditions document with the wrong serial number

12. *License verification error*

EPK application error:



License verification error

The IndraToken component is owned by the INDRA SISTEMAS S.A. company. There is a signature verification error. Therefore, the component was disabled.

Reason:

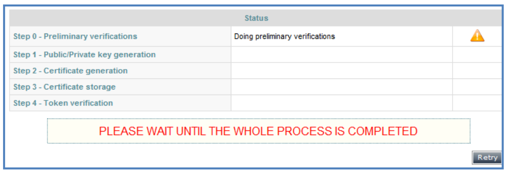
You will receive this message if you have not installed the ESCB-PKI production CA certificates.

Action:

Verify that you have installed the Production Root and Subordinate CAs certificates and try again. Instructions to install the CAs are available in the ESC-PKI Website (Support tab).

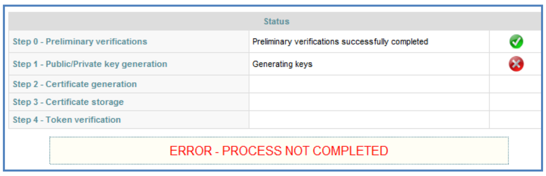
13. *Error generating the keys*

EPK application error:



Status		
Step 0 - Preliminary verifications	Doing preliminary verifications	⚠
Step 1 - Public/Private key generation		
Step 2 - Certificate generation		
Step 3 - Certificate storage		
Step 4 - Token verification		

PLEASE WAIT UNTIL THE WHOLE PROCESS IS COMPLETED



Status		
Step 0 - Preliminary verifications	Preliminary verifications successfully completed	✓
Step 1 - Public/Private key generation	Generating keys	✗
Step 2 - Certificate generation		
Step 3 - Certificate storage		
Step 4 - Token verification		

ERROR - PROCESS NOT COMPLETED

Reason:

Typically you will receive this message if

a) You have removed the token from the reader while the keys were being generated.

b) You are using an old version of the driver of your smart card reader.

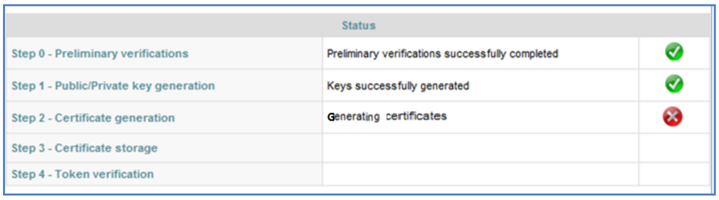
Action:

a) Re-insert the card and try again.

b) Verify that you have the correct version of your driver and try again.

14. *Error generating certificates*

EPK application error:



Status		
Step 0 - Preliminary verifications	Preliminary verifications successfully completed	✓
Step 1 - Public/Private key generation	Keys successfully generated	✓
Step 2 - Certificate generation	Generating certificates	✗
Step 3 - Certificate storage		
Step 4 - Token verification		

Reason:

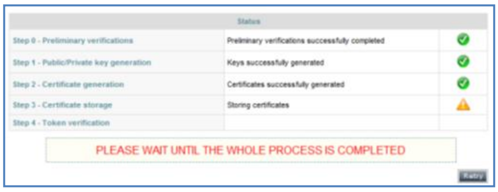
You shouldn't receive this message. Should this happen, contact your local Help Desk to communicate the error to the ESCB-PKI coordinating service desk.

Action:

If the certificates haven't been generated (you didn't receive an ESCB-PKI e-mail containing the serial number of the certificate) you can try again. But, if the certificates have been issued you must generate a new request with reason: LOST CERTIFICATE.

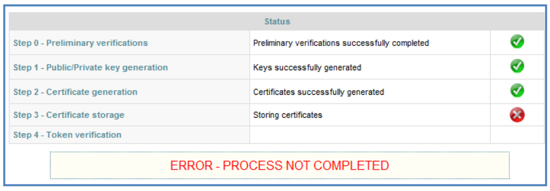
15. Error storing certificates

EPK application error:



Status		
Step 0 - Preliminary verifications	Preliminary verifications successfully completed	✓
Step 1 - Public/Private key generation	Keys successfully generated	✓
Step 2 - Certificate generation	Certificates successfully generated	✓
Step 3 - Certificate storage	Storing certificates	⚠
Step 4 - Token verification		

PLEASE WAIT UNTIL THE WHOLE PROCESS IS COMPLETED



Status		
Step 0 - Preliminary verifications	Preliminary verifications successfully completed	✓
Step 1 - Public/Private key generation	Keys successfully generated	✓
Step 2 - Certificate generation	Certificates successfully generated	✓
Step 3 - Certificate storage	Storing certificates	✗
Step 4 - Token verification		

ERROR - PROCESS NOT COMPLETED

Reason:

Typically you will receive this message if

a) You removed the token from the reader while the keys were being stored.

b) Your smart card has not enough space to store the certificates generated[7].

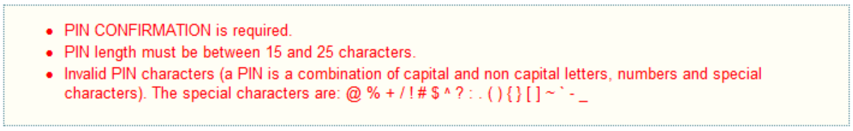
Action:

a) Verify that you have the smart card correctly inserted in the reader and try again.

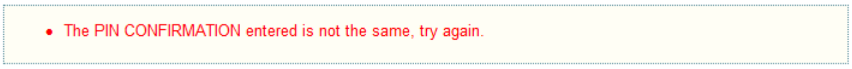
b) If your card is full you must clean your smart card (i.e. deleting keys and certificates you don't need) and then make a new request.

16. Invalid PIN downloading standard certificates

EPK application error:



- PIN CONFIRMATION is required.
- PIN length must be between 15 and 25 characters.
- Invalid PIN characters (a PIN is a combination of capital and non capital letters, numbers and special characters). The special characters are: @ % + / ! # $ ^ ? : . ( ) { } [ ] ~ ` - _



- The PIN CONFIRMATION entered is not the same, try again.

Reason:

a) You have selected a PIN not compliant with the security rules.

b) The value entered in the PIN confirmation entry does not match the PIN.

Action:

a) Select and type a PIN compliant with the security rules:

- – PIN length must be between 15 and 25 characters
- – PIN is a combination of capital and non-capital letters, numbers and special characters (special characters are: @ % + / ! # $ ^ ? : . ( ) { } [ ] ~ ` - _)

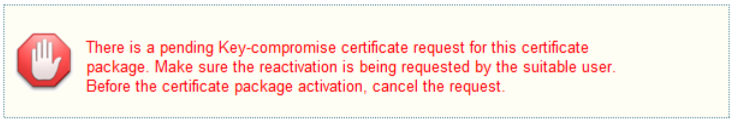
b) Ensure that you type the same value in the PIN confirmation entry.

[7] This is a very rare situation. Typically this could happen in the acceptance environment when you store multiple certificates in the same card. The ESCB-PKI smart-card can store up to 11 certificates, taking into account that initially 3 certificates are stored and that, in normal circumstances, 1 extra certificate will be added every 3 years (the old encryption certificate is not deleted when renewing certificates), it will take more than 20 years to reach the number of 11 certificates in the same smart-card.

5. CERTIFICATE MANAGEMENT MOST COMMON ERRORS

17. *Error reactivating a certificate*

EPK application error:



There is a pending Key-compromise certificate request for this certificate package. Make sure the reactivation is being requested by the suitable user. Before the certificate package activation, cancel the request.

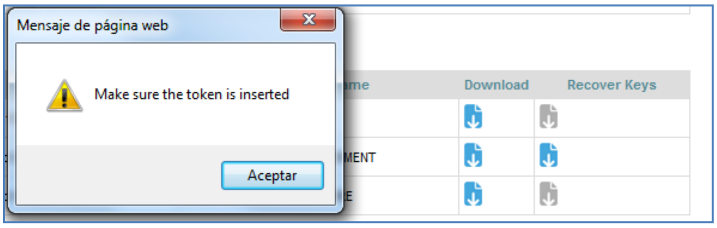
Reason:
You are trying to reactivate a suspended certificate and there is a pending request to replace this certificate due to key compromise.

Action:
Ensure that the user requesting the certificate reactivation is the owner of the certificate. If he really wants to reactivate the old certificate:

- Cancel the pending request, and afterwards
- Reactivate the certificate.

18. *There is not a token in the reader*

EPK application error:



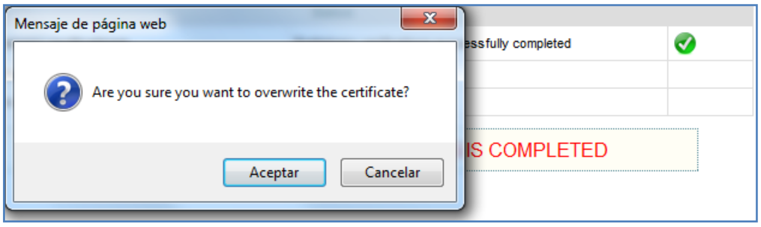
Make sure the token is inserted

Reason:
You selected the "encryption key recovery" option to recover old encryption certificate but you have not inserted a smart card in the reader or the smart card is not correctly inserted.

Action:
Verify that you have the smart card correctly inserted in the reader and try again.

19. *Duplicated encryption key*

EPK application error:



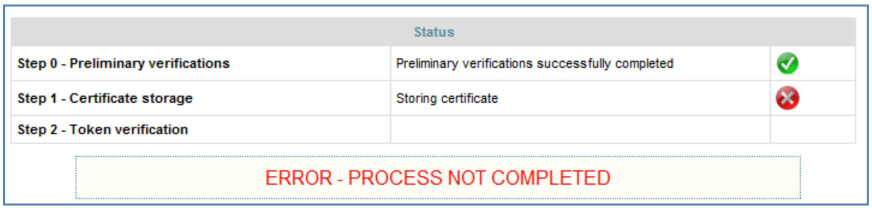
Are you sure you want to overwrite the certificate?

Reason:
You have requested to recover an encryption key and you already have it installed in your token.

Action:
You can cancel the request or, if you want to replace the copy installed in your smart card because it was damaged, you can continue.

20. Error storing certificates

EPK application error:



Status		
Step 0 - Preliminary verifications	Preliminary verifications successfully completed	✓
Step 1 - Certificate storage	Storing certificate	✗
Step 2 - Token verification		

ERROR - PROCESS NOT COMPLETED

Reason:

Typically you will receive this message when

a) You removed the token from the reader while the keys were being stored.

b) Your card has not enough space to store the certificates generated[8].

c) You are using a smart card with a different serial number from the one selected in the previous screen.

Action:

a) Verify that you have the smart card correctly inserted in the reader and try again.

b) If your card is full you must clean your smart card (i.e. deleting keys and certificates you don't need) and try again.

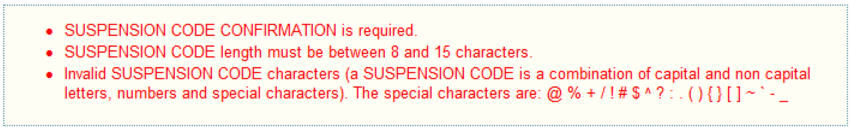
c) Insert the smart card with the correct serial number.

[8] This is a very rare situation. Typically this could happen in the acceptance environment when you store multiple different certificates in the same card. The ESCB-PKI smart-card can store up to 11 certificates, taking into account that initially 3 certificates are stored and that, in normal circumstances, 1 extra certificate will be added every 3 years (the old encryption certificate is not deleted when renewing certificates), it will take 20 years to reach the number of 11 certificates in the same smart-card.

6. OTHER COMMON ERRORS

21. Invalid suspension code

EPK application error:



- SUSPENSION CODE CONFIRMATION is required.
- SUSPENSION CODE length must be between 8 and 15 characters.
- Invalid SUSPENSION CODE characters (a SUSPENSION CODE is a combination of capital and non capital letters, numbers and special characters). The special characters are: @ % + / ! # $ ^ ? : . ( ) { } [ ] ~ ` - _

Reason:

a) You have selected a code not compliant with the security rules.
b) The value entered in the code confirmation entry does not match the suspension code.

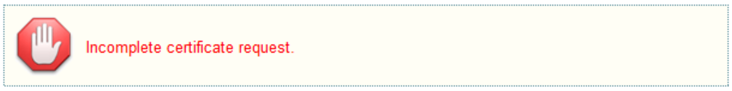
Action:

a) Select and type a code compliant with the security rules:
   - PIN length must be between 8 and 15 characters
   - PIN is a combination of capital and non-capital letters, numbers and special characters (special characters are: @ % + / ! # $ ^ ? : . ( ) { } [ ] ~ ` - _)

b) Ensure that you type the same value in the suspension code confirmation entry.

22. Error downloading Terms and Conditions

EPK application error:



Incomplete certificate request.

Reason:

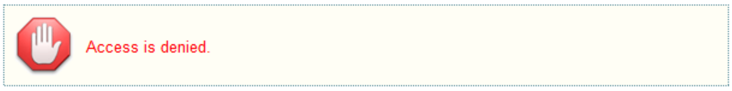
You will receive this message when some data is missed in the request.
Typically, the information that could be missed is the serial number of your smart card in case of advanced certificate requests.

Action:

Complete the missed information.

23. Access denied

EPK application error:



Access is denied.

Reason:

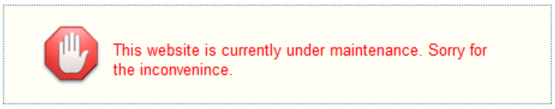
You have requested an action and you are not authorized to perform it. In normal circumstances you shouldn’t receive this error.

Action:

Try again, if the error continues contact your Help Desk to communicate the error to the ESCB-PKI coordinating service desk.

24. System under maintenance

EPK application error:



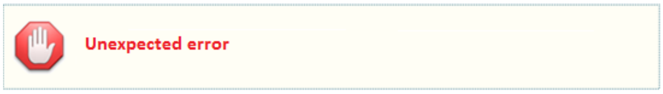
This website is currently under maintenance. Sorry for the inconvenince.

Reason:
The system has been stopped due to maintenance.

Action:
Try later. If the problem continues contact your Help Desk to communicate the unavailability to the ESCB-PKI coordinating service desk.

25. Unexpected error

EPK application error:



Unexpected error

Reason:
The application detected a non-controlled situation. In normal circumstances you shouldn't receive this error.

Action:
Try again, if the error continues contact your local Help Desk to communicate the error to the ESCB-PKI coordinating service desk.