

Εγκατάσταση  
πιστοποιητικών  
ATHEX στον σταθμό  
του χρήστη της  
υπηρεσίας  
HE.R.ME.S II

Έκδοση 0.1 - 01/07/2024



## Περιεχόμενα

Ιστορικό αλλαγών .....	2
1. Γενικά .....	3
2. Βήματα .....	3

## Ιστορικό αλλαγών

Έκδοση	Ημερομηνία	Αλλαγές
0.1	01/07/2024	Αρχική έκδοση

## 1. Γενικά

Τα πιστοποιητικά που απαιτούνται προκειμένου να μπορέσει ο χρήστης να κάνει υποβολές με το σύστημα ΕΡΜΗΣ, είτε στο τεστ περιβάλλον είτε στο παραγωγικό, είναι τα ακόλουθα:

## 2. Βήματα

- 2.1. Στο **'Trusted Root Certifications Authorities'** να εγκατασταθεί το παρακάτω πιστοποιητικό:

### ATHEX RSA Root CA R2



- 2.2. Στο **'Intermediate Certification Authorities'** να εγκατασταθούν τα παρακάτω πιστοποιητικά:

### ATHEX Qualified eSign Certificates CA G3 R20

### ATHEX Qualified WEB Certificates CA G3 R20



2.3. Μπορείτε να κατεβάσετε τα πιστοποιητικά από [εδώ](#) και με ένα click και να τα εγκαταστήσετε.

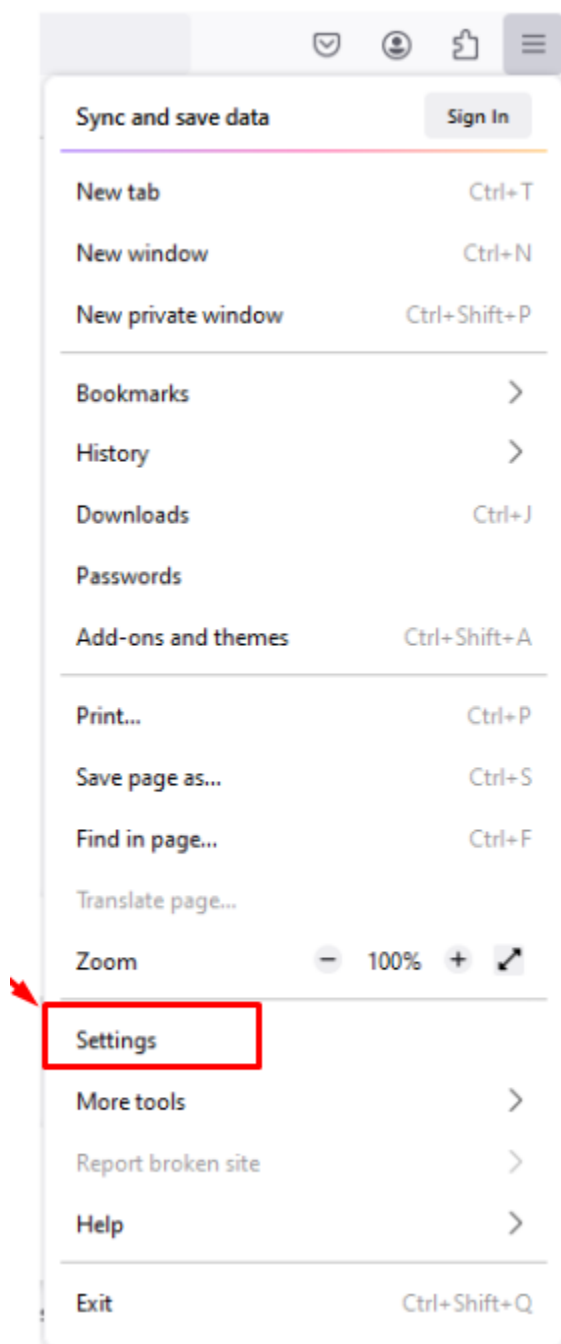
**ATHEX RSA Root CA R2** [Download DER/CRT](#)

**ATHEX Qualified eSign Certificates CA G3 R20** [Download DER/CRT](#)

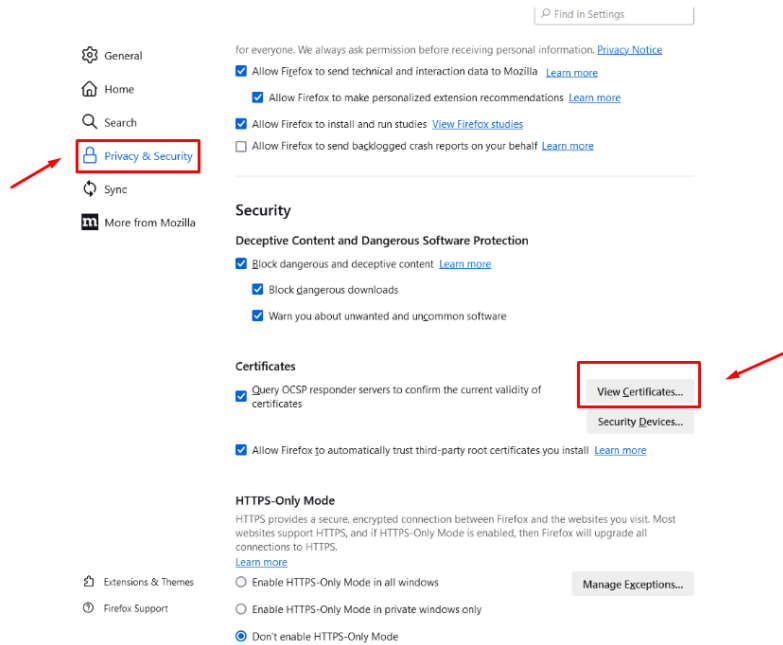
**ATHEX Qualified WEB Certificates CA G3 R20** [Download DER/CRT](#)

2.4. Εγκατάσταση με **FIREFOX**

Θα πρέπει να εγκατασταθούν και τα **3 πιστοποιητικά**.



- Πατάμε το **Privacy & securities** και επιλέγουμε το **view certificates**.



Find in Settings

General for everyone. We always ask permission before receiving personal information. [Privacy Notice](#)

Allow Firefox to send technical and interaction data to Mozilla [Learn more](#)

Allow Firefox to make personalized extension recommendations [Learn more](#)

Allow Firefox to install and run studies [View Firefox studies](#)

Allow Firefox to send background crash reports on your behalf [Learn more](#)

**Security**

**Deceptive Content and Dangerous Software Protection**

Block dangerous and deceptive content [Learn more](#)

Block dangerous downloads

Warn you about unwanted and uncommon software

**Certificates**

Query OCSP responder servers to confirm the current validity of certificates

Allow Firefox to automatically trust third-party root certificates you install [Learn more](#)

Query OCSP responder servers to confirm the current validity of certificates **View Certificates...** [Security Devices...](#)

**HTTPS-Only Mode**

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS. [Learn more](#)

Enable HTTPS-Only Mode in all windows [Manage Exceptions...](#)

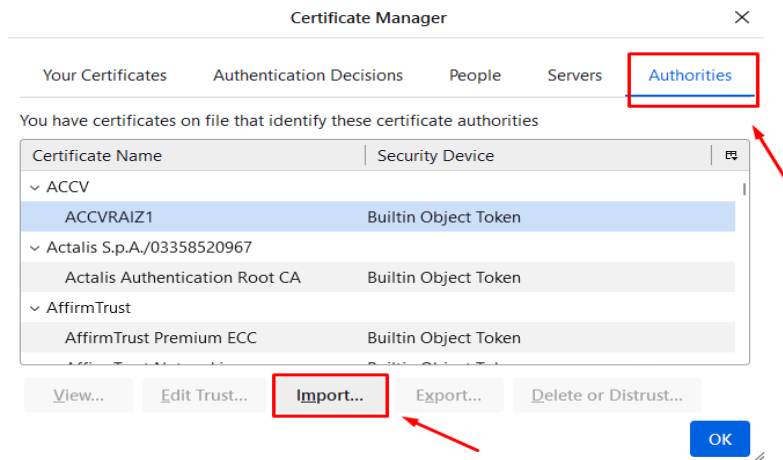
Enable HTTPS-Only Mode in private windows only

Don't enable HTTPS-Only Mode

Extensions & Themes

Firefox Support

- Στο **Authorities** κάνουμε **import**.



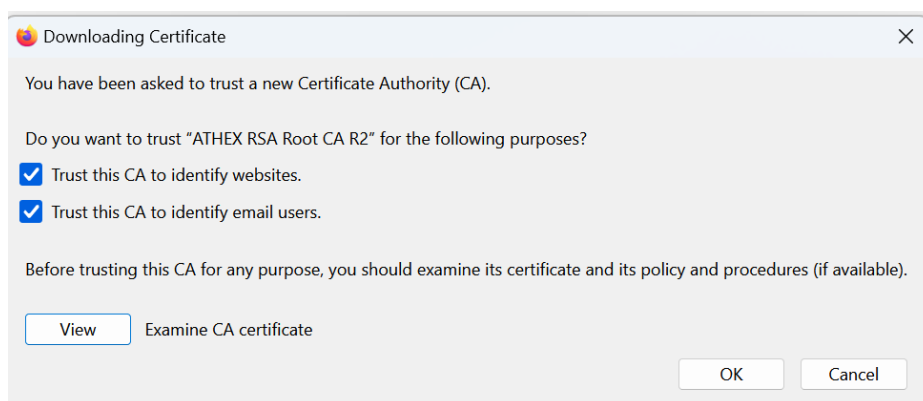
Certificate Manager

Your Certificates Authentication Decisions People Servers **Authorities**

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
ACCV <ul style="list-style-type: none"> <li>ACCRAIZ1 Builtin Object Token</li> </ul>	
Actalis S.p.A./03358520967 <ul style="list-style-type: none"> <li>Actalis Authentication Root CA Builtin Object Token</li> </ul>	
AffirmTrust <ul style="list-style-type: none"> <li>AffirmTrust Premium ECC Builtin Object Token</li> </ul>	

- Εάν εμφανιστεί το παρακάτω, τότε επιλέξτε όπως φαίνεται στην εικόνα.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "ATHEX RSA Root CA R2" for the following purposes?

Trust this CA to identify websites.

Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate