

# Cittadinanza Digitale e Tecnocivismo

## 1. Titolo esercizio

Guida sul come riconoscere la validità di un certificato SSL

## 2. Per chi

Utenti con una base informatica, la procedura è semplice, la comprensione dell'output un pò meno.

## 3. Durata

10/15 minuti

## 4. Livelli arcobaleno + tag/keyword

L0 - Network

## 5. Difficoltà (relatività utente)

Facile

## 6. Esempi già pronti

Visualizzatore certificati: \*.esselungaacasa.it

Generali    Dettagli

Rilasciato a

Nome comune (CN)	*.esselungaacasa.it
Organizzazione (O)	Esselunga S.p.a.
Unità organizzativa (OU)	<Non parte del certificato>

Emesso da

Nome comune (CN)	Bitdefender Personal CA.Net-Defender
Organizzazione (O)	Bitdefender
Unità organizzativa (OU)	IDS

Periodo di validità

Emesso in data	mercoledì 29 giugno 2022 alle ore 18:11:06
Scade in data	lunedì 31 luglio 2023 alle ore 18:11:05

Impronte digitali

Impronta digitale SHA-256	F2 53 F3 FA 8D 8B 92 3F 14 F0 2A A1 AF D0 94 3C 65 9D 02 F7 48 5A 20 43 5E 30 60 EB 60 33 7C D5
Impronta digitale SHA-1	A1 B6 4D 3E 99 28 5D 3A 4C 92 A3 E6 9F 16 7C B5 F3 24 A2 63

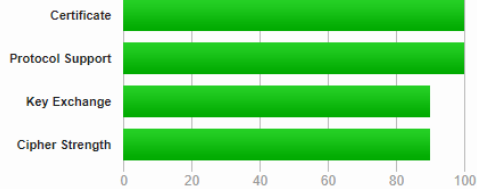
## SSL Report: www.esselunga.it (185.96.117.10)

Assessed on: Sun, 02 Jul 2023 07:58:57 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)



[Home](#) [Projects](#) [Qualys Free Trial](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > SSL Server Test

### SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

☐ Do not show the results on the boards

#### Recently Seen

<a href="#">ido.ahnu.edu.cn</a>	
<a href="#">www.freeopenvon.org</a>	
<a href="#">www.esselunga.it</a>	A+
<a href="#">esselungaacasa.it</a>	Err
<a href="#">saviorhost.com</a>	A+
<a href="#">corecrimexat.coreretirements...</a>	A+
<a href="#">dex.water-exchange.com</a>	A
<a href="#">windrosemena.com</a>	A
<a href="#">www.amazon.it</a>	A
<a href="#">wallet.water-exchange.com</a>	A

#### Recent Best

<a href="#">www.esselunga.it</a>	A+
<a href="#">saviorhost.com</a>	A+
<a href="#">corecrimexat.coreretirements...</a>	A+
<a href="#">dex.water-exchange.com</a>	A
<a href="#">windrosemena.com</a>	A
<a href="#">wallet.water-exchange.com</a>	A
<a href="#">lokaaladvertiser.nl</a>	A
<a href="#">marktforschung.raiffeisen.at</a>	A
<a href="#">www.kst-serviceportal.de</a>	A
<a href="#">fedido.org</a>	B

#### Recent Worst

<a href="#">webmail.rmq.gov.my</a>	F
<a href="#">gel-st.jio.com</a>	T
<a href="#">wordle.sk</a>	T
<a href="#">priorityoneservers.com</a>	T
<a href="#">qcnaraingarh.edu.in</a>	T
<a href="#">del.or</a>	T
<a href="#">news.uscg.afpms.mil</a>	T
<a href="#">atc-cloud.xyz</a>	T
<a href="#">lvkasz.us</a>	T
<a href="#">toba138.shop</a>	F

## Certificate #1: RSA 2048 bits (SHA256withRSA)



### Server Key and Certificate #1



Subject	*.esselunga.it Fingerprint SHA256: 259df62962e74b8fe5878c9ac4ea1eef71d841c661b8c02c30c714233bc52374 Pin SHA256: KY6hxwZyghGE9YEBDDCN+c8w5JKIZIfg0S26ebm/FrA=
Common names	*.esselunga.it
Alternative names	*.esselunga.it esselunga.it
Serial Number	7239bd1ed0a95bdd47f24e04
Valid from	Thu, 29 Dec 2022 16:36:02 UTC
Valid until	Tue, 30 Jan 2024 16:36:01 UTC (expires in 6 months and 28 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GlobalSign RSA OV SSL CA 2018 AIA: <a href="http://secure.globalsign.com/caoert/gsrsoovsslca2018.crt">http://secure.globalsign.com/caoert/gsrsoovsslca2018.crt</a>
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: <a href="http://crl.globalsign.com/gsrsoovsslca2018.crl">http://crl.globalsign.com/gsrsoovsslca2018.crl</a> OCSP: <a href="http://ocsp.globalsign.com/gsrsoovsslca2018">http://ocsp.globalsign.com/gsrsoovsslca2018</a>
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

## 7. Strumenti (necessaire), s.o., pacchetti/app

Browser web aggiornato.

## 8. Costi

Gratis

## 9. Istruzioni dettagliate

- 9.1. Aprire pagina sito web da analizzare
- 9.2. Cliccare sul lucchetto a sinistra dell'URL
- 9.3. Cliccare su "la connessione è sicura"
- 9.4. Cliccare su "il certificato è valido"
- 9.5. Si aprirà un pop up con il CN (Common Name) del sito, il quale rappresenta il nome del certificato, già da qui si può vedere se il certificato è ancora valido
- 9.6. Copiare il CN
- 9.7. Recarsi al link <https://www.ssllabs.com/ssltest/index.html>
- 9.8. Incollare il CN
- 9.9. Aspettare
- 9.10. Visualizzare il rating assegnato al certificato ed altri parametri

## **10. Lesson learned, obiettivi**

Quando si naviga su internet, soprattutto nel momento in cui ci rechiamo su pagine che trattano dati sensibili, è buona norma controllare se il certificato utilizzato dalla piattaforma è ancora valido, per avere un'idea della correttezza della piattaforma scelta è possibile utilizzare strumenti, come quello di Qualys, che permettono di visionare il rating assegnato.

## **11. Autore**

Stefano Golcondi

## **12. Note**

Lo Scan su <https://www.ssllabs.com/ssltest/index.html> ha bisogno di molto tempo per processare l'output.

## **13. Licenza**

Libera