

**9<sup>th</sup>**  
**UCAAT** *User Conference on  
Advanced Automated Testing*

# ETSI Electronic Signatures Testing activities

Laurent Velez ([laurent.velez@etsi.org](mailto:laurent.velez@etsi.org))



14/09/2022





- ETSI ESI Activities
- Electronic Signature Plugtests
- Signature Conformance Checker
- Trusted List Checker

## Electronic Signatures and Infrastructures





- TC ESI (Electronic Signatures and Infrastructures ) is the ETSI committee dealing with digital signatures.
- TC ESI also covers policy, security and technical requirements for trust service providers (TSP)
- TC ESI addresses Trusted Lists that enhance the confidence of parties relying on certificates or other services related to digital signatures by indicating whether a given TSP was operating under the approval of any recognized scheme.
- TC ESI works closely with European Commission, in support of the eIDAS Regulation  
The eIDAS regulation was created to establish trust in electronic transactions between individuals, organizations and government entities across European Member States. This begins by creating rules for electronic identification and trust services to simplify and standardize digital IDs and signatures across Europe.

# What is a digital signature ?

- An electronic (digital) signature is essentially the equivalent of a hand-written signature, with data in the electronic form being attached to other electronic subject data as means of authentication.
- A digital signature is used to authenticate digital information – such as form templates, e-mail messages, and documents – by using computer cryptography.
- Digital signatures help to establish the following assurances:
  - Authenticity: The digital signature helps to assure that the signer is who he or she claims to be.
  - Integrity: The digital signature helps to assure that the content has not been changed or tampered with since it was digitally signed.
  - Non-repudiation: The digital signature helps prove the origin of the signed content to all parties. "Repudiation" refers to the act of a signer denying any association with the signed content.

# Main ETSI Digital signature formats

- PAdES (PDF Advanced Electronic Signature ETSI TS 102 778 and EN 319 142-1&2)
- XAdES (XML Advanced Electronic Signature ETSI 101 903, TS 103 171 and EN 319 132-1&2)
- CAdES (CMS Advanced Electronic Signature ETSI TS 101 733 and EN 319 122-1&2)
- ASiC (Associated Signature Container ETSI TS 102 918 and EN 319 162-1&2)
- JAdES (JSON Advanced Electronic Signature ETSI TS 119 182-1)

- ETSI ESI also defines technical profiles and policy requirements for trust service providers for a range of services including :
  - services supporting signature (e.g. certification authorities, Timestamping authorities)
  - remote signature creation or validation functions
  - registered e-delivery (ERDS)
  - Registered Emails (REM)
  - information preservation
  - ESI also recommends cryptographic suites for digital signatures



# Electronic Signatures Plugtests

9<sup>th</sup>  
**UCAAT**



*Testing of Trustworthy Systems*

**#UCAAT**



# Interoperability for validating standards

- ETSI as Standard maker is bringing a special attention in Testing, included in the development process of the standards.
- Conformance is perfect to ensure that a product correctly implements the requirements defined in a standard.
- BUT For new standards or new release, the Interoperability testing is great to validate the standard itself and to identify error, ambiguity or conflicting requirements.
- At ETSI, our main goal, is that everybody has the same understanding of the standards that we publish.

# ETSI Plugtests

- Standards can be validated by several means but one of the most practical and cost effective is by interop events (Plugtests)



# ETSI Plugtests

- Responsibility of ETSI CTI
- Support of all the ETSI committees
- More than 200 events since 1999
- Funded by European Commission in his mission to promote standardization , bringing interoperability
- 8 events a year in average
- Physical, remote and hybrid
- Technical feedback provided to the related ETSI TC

# ETSI ESI Plugtests

- Interoperability Testing event
- Scheduled for 4 weeks
- Remote test event using a dedicated portal
- Open 24/24, testing is not in real time, companies participate when they wish.
- Companies upload signatures that are validated by other participants.
- Plugtests portal, updated and tuned for each event.
  - <http://signature-plugtests.etsi.org>,
- Fruitful technical exchanges on Slack workspace or my mailing lists
- Usually, the participation is between 100 and 200 persons from all over the world.

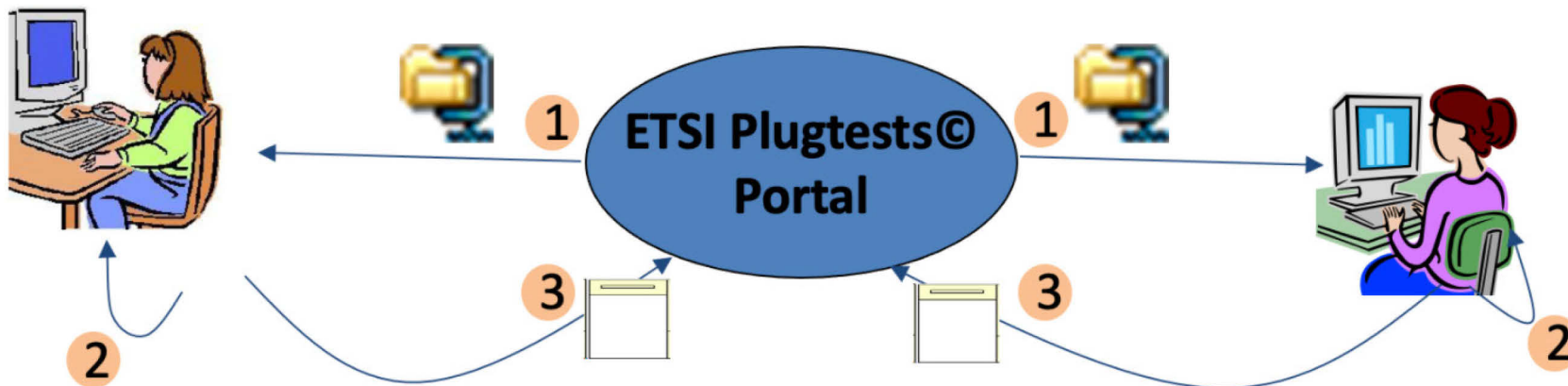


# ETSI ESI Plugtests

- Responsibility of ETSI CTI
- Company results are strictly confidential. Each participating company shall sign a NDA, even observers.
- Free of charge , open to All, ETSI or Non ETSI members.
- Useful for companies to debug their implementations or clarify their understanding of the standards.
- Feedback will be provided to ETSI TC ESI for further standardization work in order to improve the specifications if required.

# Signatures Plugtests

- The scope of the event is to check the interoperability of product implementing the Technical Specification on an ETSI Advanced Signature.
- This remote event aims at conducting interoperability and conformance testing





# 4 Types of tests

- **Generation and cross-verification tests**
  - Each participant is invited to generate a certain set of valid Signatures with certain characteristics (generation). The rest of the participants are invited afterward to verify these signatures (cross-verification).
  - The Plugtests portal automatically generates an updated set of interoperability matrixes that all the participants may access.
- **Augmentation and verification of augmented signatures**
  - Each participant is invited to augment (augmenting phase) a certain set of baseline signatures previously generated by other participants,
- **Only verification tests**
  - ETSI has generated a number of invalid Signatures by different reasons.
  - Each participant tries to verify these signatures, checking in this way that the corresponding tool actually detects that the signature is not valid.
- **Conformance tests**
  - participants upload signatures to the Conformance checker.



# ETSI Signature Conformance Checker

9<sup>th</sup>  
**UCAAT**



- The ETSI Centre for Testing and Interoperability (CTI) provides a free online tool that performs numerous checkings in order to verify the conformity of the ETSI Advanced Electronic Signatures.
- This is NOT a signature validation tool. It checks the structure of the AdES signature versus the ETSI Specifications. It DOES NOT verify the validity of the signature. It cryptographically verifies the digital signature value, but it does not validate the certificate chain.
- This “self-testing” and “on demand” is greatly appreciated by signing tools companies to debug their implementations.
- The tool is a collaboration between ETSI and UPC (Universitat Politècnica de Catalunya · Barcelona)

[PAdES Checker](#)

[XAdES Checker](#)

[CAAdES Checker](#)

[ASiC Checker](#)

[JAdES Checker](#)

[ETSI Standards](#)

[Tools  
Documentation](#)

[Checker  
Statistics](#)

[Issues /  
Questions](#)

## ETSI Signature Conformance Checker

ETSI Centre for Testing and Interoperability (CTI) provides a **free online tool** that performs numerous checkings in order to verify the conformity of the ETSI Advanced Electronic Signatures.

The tool performs conformance tests on :

1. **PAdES (PDF Advanced Electronic Signature ETSI TS 102 778 and EN 319 142-1&2)**
2. **XAdES (XML Advanced Electronic Signature ETSI 101 903, TS 103 171 and EN 319 132-1&2)**
3. **CAAdES (CMS Advanced Electronic Signature ETSI TS 101 733 and EN 319 122-1&2)**
4. **ASiC (Associated Signature Container ETSI TS 102 918 and EN 319 162-1&2)**
5. **JAdES (JSON Advanced Electronic Signature ETSI TS 119 182-1) **NEW !!!****



- The tool performs conformance tests on :
  - PAdES (PDF Advanced Electronic Signature ETSI TS 102 778 and EN 319 142-1&2)
  - XAdES (XML Advanced Electronic Signature ETSI 101 903, TS 103 171 and EN 319 132-1&2)
  - CAdES (CMS Advanced Electronic Signature ETSI TS 101 733 and EN 319 122-1&2)
  - ASiC (Associated Signature Container ETSI TS 102 918 and EN 319 162-1&2)
  - JAdES (JSON Advanced Electronic Signature ETSI TS 119 182-1) **NEW !!!**
  
- When uploading a signature, the user gets a full conformance report listing:
  - XML Raw Output
  - Errors and Warnings
  - Full Report
  - Content Details
  - Trace on Message Imprints



## PADES Conformance Checker

PADES Checker

XAdES Checker

CADES Checker

ASiC Checker

JAdES Checker

ETSI Standards ▶

Tools  
Documentation

Checker  
Statistics ▶

Issues /  
Questions

**IMPORTANT: The tools check the structure of the signature versus the ETSI Specifications. It DOES NOT verify the validity of the signature. It cryptographically verifies the digital signature value, but it does not validate the certificate chain.**

This tool enables to test conformity of PAdES signature against the requirements defined in the PAdES standards **ETSI EN 319 142-1 V1.1.1** and **EN 319 142-2 V1.1.1**

- You must upload a **.pdf** file. The signature will not be stored on the server

### Select PAdES signature to upload

Parcourir... Aucun fichier sélectionné.

Upload

Select the PAdES Technical Specification on you wish to perform the test :

- ETSI EN 319 142-1 v1.1.1 Building Blocks and Baseline
- ETSI EN 319 142-2 v1.1.1 Additional PAdES signatures profiles

**The PAdES was uploaded successfully to the server.**

[Click here to see the PAdES Conformance Report index.html](#)

# ETSI Signature Conformance Checker



## XML Input File Overview

[Back to Presentation Page](#)

## Signatures tested

[PAdES-signature-1](#)

## All Reports

[XML Raw Output](#)

[Errors and Warnings](#)

[Full Report](#)

[Content Details](#)

[Trace on Message Imprints](#)

## Report on errors, warnings and exceptions

This page shows the errors, warnings and exceptions generated by the XAdES Baseline Profile Conformance Checker Tool.

Report on Errors, Warnings and Exceptions		
Result	TI/VI	Tested Element and Test
Test Result Details		
5. Error	Tool	Location- {CodeTest}:SubFilter- {CheckIfValueIsOneOfDefined} Found value: 'adbe.pkcs7.detached'. Allowed values: ETSI.CAdES.detached
21. Error	Tool	Location- {CodeTest}:Contents/CAdESSignature- {VerifyCMSOrCAdESWithinPAdES} The CRYPTOGRAPHIC VERIFICATION of the SIGNATURE whose certificate has been issued by "C=BE,O=GlobalSign nv-sa,CN=GlobalSign CA 2 for AATL" to "C=BE,ST=Oost-Vlaanderen,L=Hasselt,OU=Soft,CN=Patrick D'Anghe,E=p.danghe@globalign.be", and whose serial number is 15469493658293542857252595327, HAS FAILED. Additional details follow: verifier not valid at signingTime
44. Error	Tool	Location- {CodeTest}:Contents/CAdESSignature/content/signedData/signerInfos/signerInfo[1]/signedAttrs- {CheckAllowedAttributes} Children order and number DO NOT MATCH specification Specification: (contentType    messageDigest    essSigningCertificate    essSigningCertificateV2    signerAttributesV2    contentTimeStamp)* Elements found: contentType signingTimeUTCTime messageDigest Error indication (^ appears at the end of the last correct child): contentType^ signingTimeUTCTime messageDigest
46. Error	Tool	Location- {CodeTest}:Contents/CAdESSignature/content/signedData/signerInfos/signerInfo[1]/signedAttrs- {CheckOnlyOneAttrOfTheListPresent} Only one of the attributes in the following list have to be present: essSigningCertificate essSigningCertificateV2 . Instead NONE of them has been found
62. Warning	Tool	Location- {CodeTest}:Contents/CAdESSignature/content/signedData/signerInfos/signerInfo[1]/signedAttrs/attribute[4]/attrValues/UnknownName[1]- {UnknownComponent} An unknown attribute, defined by OID 1.2.840.113583.1.1.8 has been reached. Its contents and their processing are unknown to the AdESCC. No further checks will be done to this component



# ETSI Signature Conformance Checker

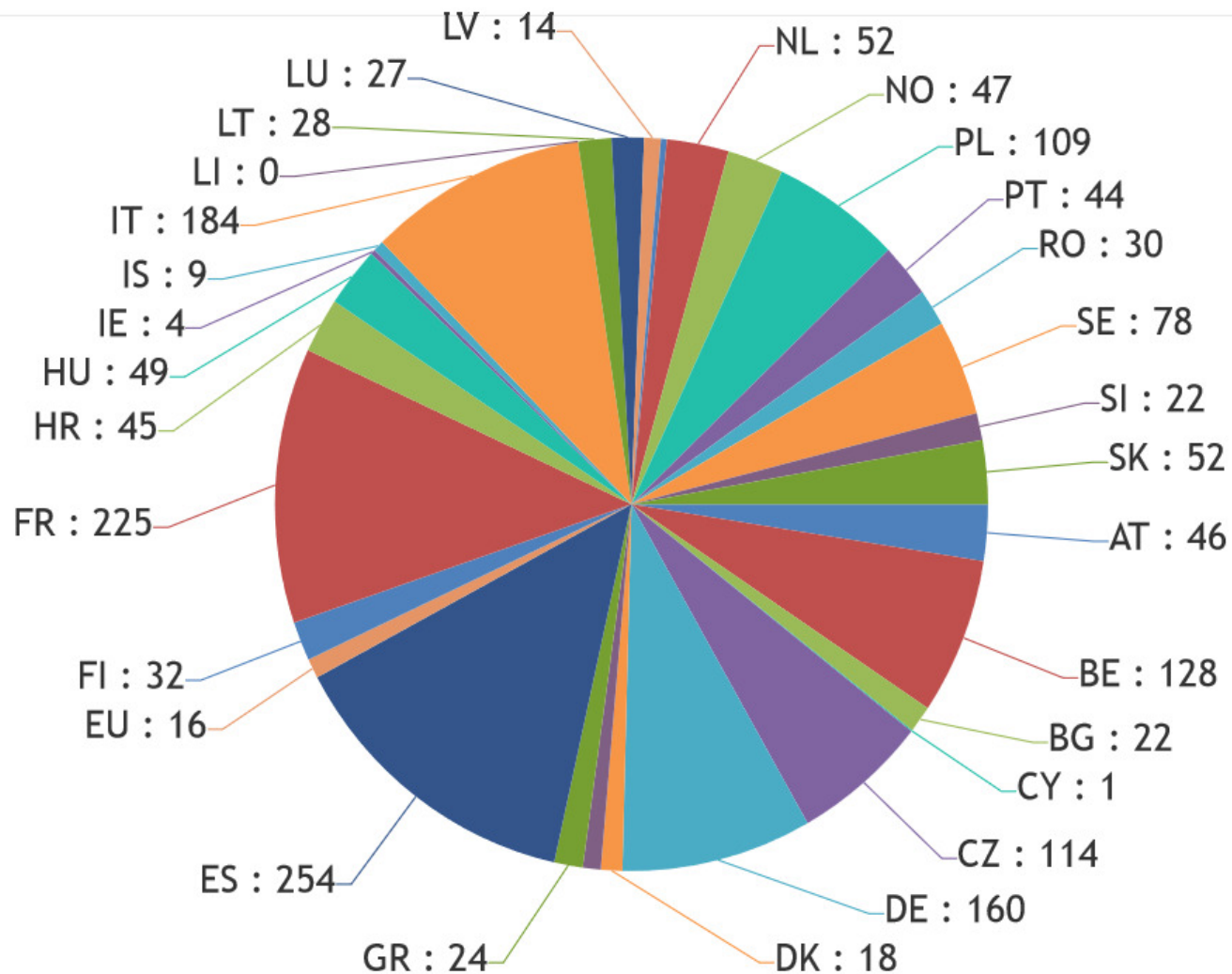


- Regular members : 2559 accounts from 90 countries
- Since Jan 2016, 53 000 Signatures conformance testing performed online
- in average 800 online tests a month
- Listed by the European Commission in the CEF Digital program as the “Reference” tool for testing Digital Signatures

<https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+Overview>

# Users per EU Member State

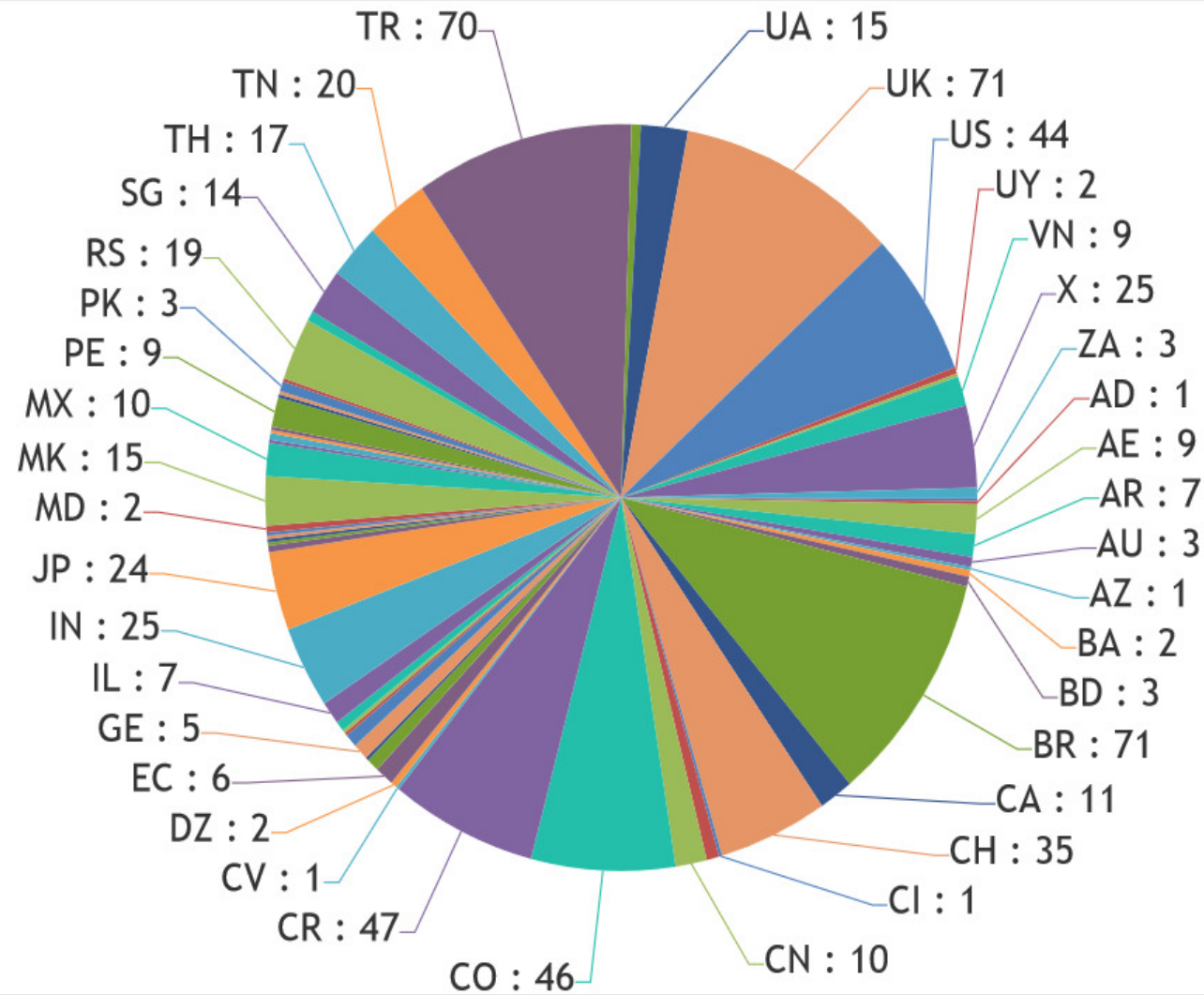
1854 users from EU





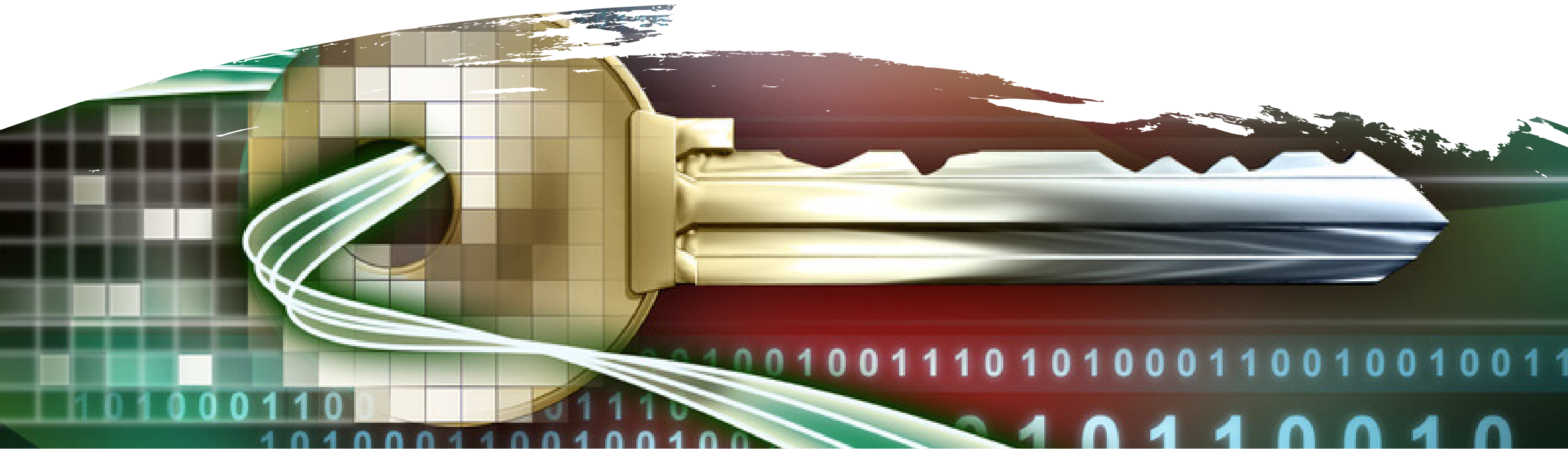
# non-EUMS users

705 from non-EU



# Trusted List conformance checker

9<sup>th</sup>  
**UCAAT**





## Trusted List Browser

The Member States of the European Union and European Economic Area publish trusted lists of qualified trust service providers in accordance with the eIDAS Regulation. The European Commission publishes a list of these trusted lists, the List of Trusted Lists (LOTL). The European Commission allows anyone to browse the national trusted lists and the LOTL.



Search a trust service by type

Search by type of trust service (e.g. time-stamping, certificate for e-signature) and country



Search a trust service by name































Search based on the name of a trust service



Search a trust service with a signed file

Find the trust service that issued the signing certificate(s) contained in a file

## Trusted Lists

 <b>Austria</b> Issue date 2022-04-07	...	 <b>Belgium</b> Issue date 2022-06-01	...	 <b>Bulgaria</b> Issue date 2022-06-30	...
 <b>Croatia</b> Issue date 2022-06-15	...	 <b>Cyprus</b> Issue date 2022-03-30	...	 <b>Czech Republic</b> Issue date 2022-06-24	...
 <b>Denmark</b> Issue date 2022-01-11	...	 <b>Estonia</b> Issue date 2022-03-21	...	 <b>Finland</b> Issue date 2022-05-25	...
 <b>France</b> Issue date 2022-06-07	...	 <b>Germany</b> Issue date 2022-06-29	...	 <b>Greece</b> Issue date 2022-06-08	...
 <b>Hungary</b> Issue date 2022-05-02	...	 <b>Iceland</b> Issue date 2022-04-25	...	 <b>Ireland</b> Issue date 2022-04-26	...
 <b>Italy</b> Issue date 2022-06-20	...	 <b>Latvia</b> Issue date 2022-05-24	...	 <b>Liechtenstein</b> Issue date 2022-04-25	...
 <b>Lithuania</b> Issue date 2022-07-01	...	 <b>Luxembourg</b> Issue date 2022-04-21	...	 <b>Malta</b> Issue date 2022-03-15	...
 <b>Netherlands</b> Issue date 2022-06-02	...	 <b>Norway</b> Issue date 2022-06-28	...	 <b>Poland</b> Issue date 2022-05-06	...
 <b>Portugal</b> Issue date 2022-06-14	...	 <b>Romania</b> Issue date 2022-02-25	...	 <b>Slovakia</b> Issue date 2022-07-01	...
 <b>Slovenia</b> Issue date 2022-06-28	...	 <b>Spain</b> Issue date 2022-06-29	...	 <b>Sweden</b> Issue date 2022-05-30	...

**SchemeInformation**

<b>TSL Id</b>	ID0001		
<b>TSL Tag</b>	<a href="http://uri.etsi.org/19612/TSLTag">http://uri.etsi.org/19612/TSLTag</a>		
<b>TSL Version Identifier</b>	5		
<b>TSL Sequence Number</b>	103		
<b>TSL Type</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric">http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric</a>		
<b>SchemeOperatorName</b>	Name	en	French Network Information Security Agency
	Name	fr	Agence nationale de la sécurité des systèmes d'information (ANSSI)
<b>PostalAddress</b>	Street Address	fr	51 boulevard de La Tour-Maubourg
	Locality	fr	Paris Cedex 07
	Postal Code	fr	75700
	Country Name	fr	FR
<b>PostalAddress</b>	Street Address	en	51 boulevard de La Tour-Maubourg
	Locality	en	Paris Cedex 07
	Postal Code	en	75700
	Country Name	en	FR
<b>ElectronicAddress</b>	URI	en	<a href="mailto:supervision-eidas@ssi.gouv.fr">mailto:supervision-eidas@ssi.gouv.fr</a>
	URI	en	<a href="https://ssi.gouv.fr/en">https://ssi.gouv.fr/en</a>
	URI	fr	<a href="mailto:supervision-eidas@ssi.gouv.fr">mailto:supervision-eidas@ssi.gouv.fr</a>
	URI	fr	<a href="https://ssi.gouv.fr">https://ssi.gouv.fr</a>
<b>SchemeName</b>	Name	en	FR:Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
	Name	fr	FR:Liste de confiance comprenant des informations relatives aux prestataires de services de confiance qualifiés qui sont contrôlés par l'État membre émetteur, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent, conformément aux dispositions pertinentes établies par le règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.
<b>SchemeInformationURI</b>	URI	en	<a href="https://ssi.gouv.fr/eidas/tl/en">https://ssi.gouv.fr/eidas/tl/en</a>
	URI	fr	<a href="https://ssi.gouv.fr/eidas/tl/fr">https://ssi.gouv.fr/eidas/tl/fr</a>
<b>Status Determination Approach</b>	<a href="http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate">http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate</a>		
<b>SchemeTypeCommunityRules</b>	URI	en	<a href="http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon</a>
	URI	fr	<a href="http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR">http://uri.etsi.org/TrstSvc/TrustedList/schemerules/FR</a>
<b>Scheme Territory</b>	FR		
<b>PolicyOrLegalNotice</b>	TSL Legal Notice	en	The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
	TSL Legal Notice	fr	Le cadre juridique applicable de la présente liste de confiance est le règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.
<b>Historical Information Period</b>	65535		



- Since 2011, ETSI CTI and the European Commission have proposed a web portal to allow EU Member States to check the conformance of their Trusted Lists regarding the Commission Decision CD 2009/767/EC as amended by CD 2010/425/EU and by CD 2013/662/EU.
- In June 2016, the online tool has been updated to match the new requirements for compliance with the legal context applicable from 1/7/2016, i.e. with CID (EU) 2015/1505 relying on ETSI TS 119 612 v2.1.1.
- The EU Member States representatives have the possibility to upload their XML Trusted Lists and check the results.
  - Conformance Checker report
  - PrettyPrint Pdf version of the uploaded TSL (including accessibility requirements for the PDF)
  - PrettyPrint Html version of the uploaded TSL
  - SHA2 companion file of the binary representation of the national XML Trusted List

## ETSI Trusted List Conformance Checker TLCC

Login

ETSI Standards

Login

### Scope

Since 2011, ETSI CTI (ETSI Centre for Testing and Interoperability) and the European Commission have proposed a web portal to allow EU Members States to check the conformance of their TSL signatures regarding the Commission Decision CD 2009/767/EC as amended by CD 2010/425/EU and by CD 2013/662/EU.

In June 2016, the online tool has been updated to match the new requirements for compliance with the legal context applicable from 1/7/2016, i.e. with CID (EU) 2015/1505 relying on ETSI TS 119 612 v2.1.1.

### Testing

The EU Member States representatives have the possibility to upload their XML Trusted Lists and check the results.

After having uploaded his TSL, each user gets the following results:

1. Conformance Checker report
2. PrettyPrint Pdf version of the uploaded TSL (including accessibility requirements for the PDF)
3. PrettyPrint Html version of the uploaded TSL
4. SHA2 companion file of the binary representation of the national XML Trusted List

None of the file that you upload are stored on the portal. They are deleted automatically when running the conformance testing

### Registration

The access to the portal is restricted to EUMS representatives. All the access requests must be granted by ETSI and EC.

For requesting access to the tool, please register by sending an email to [Plugtests@etsi.org](mailto:Plugtests@etsi.org) indicating **TL Conformance Checker** in the title .

Please provide your name, company and the EUMS that you represent.



This project is funded by European Commission



- The European Commission has produced an open source tool “TL-Manager” to help the Member States to produce and maintaining their national Trusted List
- There is also a version for non-EU Trusted List
- All-in-one tool: TL-Manager is a tool for editing a TL, browsing and monitoring any TL
- ETSI is working with the Commission to fully integrate the ETSI Trusted List conformance checker tools into the TL-Manager software. It allows triggering immediate verification when building the trusted List

<https://ec.europa.eu/digital-building-blocks/wikis/display/TLSO/Trusted+List+Manager>

# Any further questions?

[Laurent.Velez@etsi.org](mailto:Laurent.Velez@etsi.org)

