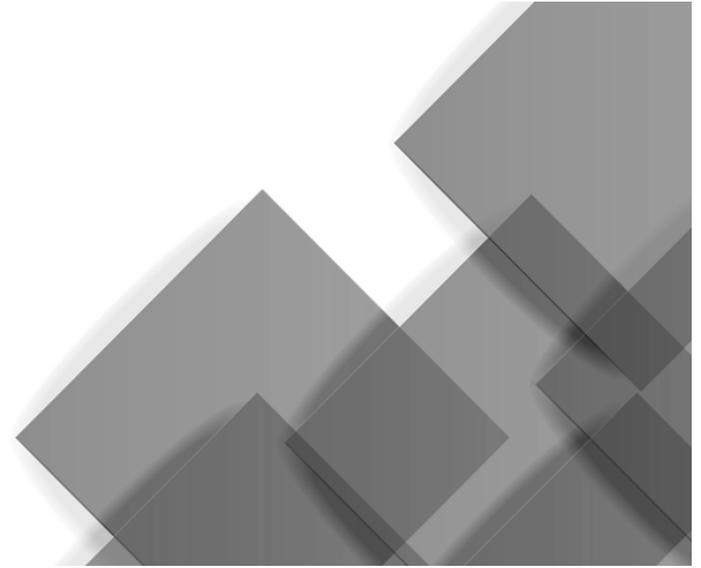




THE ACCREDITED  
CONFORMITY ASSESSMENT BODIES'  
COUNCIL

For TSP certification



## Practical ETSI Conformity Assessment

CA Assessment and Certification using ETSI European Norms

Clemens Wanko

# CONTENTS

## ETSI CA Assessment

- Assessment results
- Behind the scenes

# CONTENTS

## ETSI CA Assessment

- **Assessment results**
- Behind the scenes

# ASSESSMENT RESULTS

## Audit Attestation

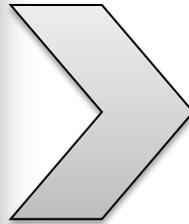
- Auditor and Accreditation
- Auditee and audited PKI (Root and CAs)
- Dates and validity



# ASSESSMENT RESULTS VALIDATION

## Audit Attestation

- Auditor and Accreditation



Website: [www.finas.fi](http://www.finas.fi)  
E-mail: [akkreditointi@finas.fi](mailto:akkreditointi@finas.fi)

### GERMANY

#### DAkS

Deutsche Akkreditierungsstelle GmbH  
Spittelmarkt 10  
10117 Berlin  
Phone: +49 (0) 30 67 059 10  
Fax: +49 (0) 30 67 0591 90

Website: [www.eak.ee](http://www.eak.ee)  
E-mail: [info@eak.ee](mailto:info@eak.ee)

### FRANCE

#### COFRAC

Comité français d'accréditation  
52 rue Jacques Hillairet  
75012 PARIS  
Phone: (33) 01.44.68.82.20  
Fax: (33) 01.44.68.82.21  
Website: [www.cofrac.fr](http://www.cofrac.fr)  
E-mail: [information@cofrac.fr](mailto:information@cofrac.fr)

### GREECE

#### ESYD

bH

Hellenic Accreditation System

Website: [www.finas.fi](http://www.finas.fi)  
E-mail: [akkreditointi@finas.fi](mailto:akkreditointi@finas.fi)

### GREECE

#### ESYD

Hellenic Accreditation System  
7 Thisseos street  
17676 Kallithra  
Phone: +30 210 9211111  
Fax: +30 210 9211112

Website: [www.esyd.gr](http://www.esyd.gr)  
E-mail: [ceo@esyd.gr](mailto:ceo@esyd.gr)

### IRELAND

#### IC

Irish Accreditation Board

# ASSESSMENT RESULTS VALIDATION

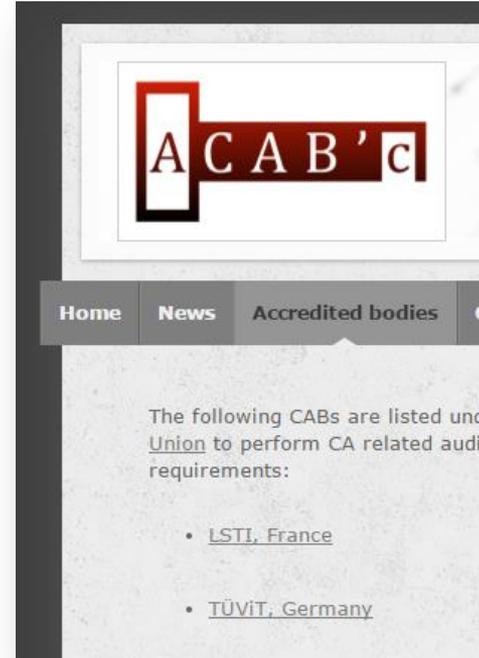
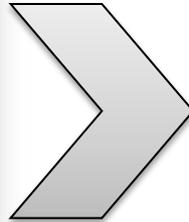
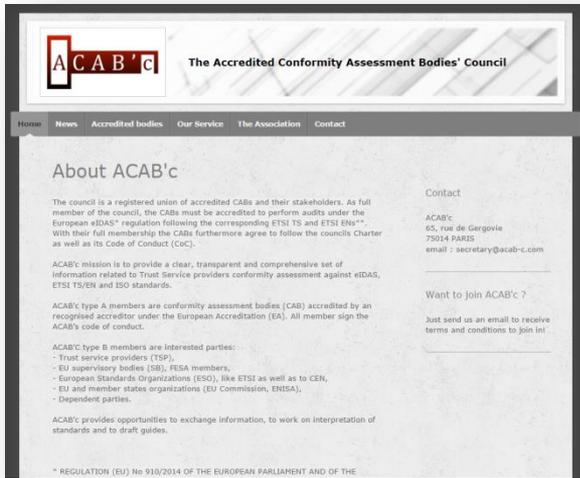
**And that's it!**

# ASSESSMENT RESULTS VALIDATION

## Audit Attestation

### ▪ Auditor and Accreditation Crosscheck

<http://www.acab-c.com>



# CONTENTS

## ETSI CA Assessment

- Assessment results
- Behind the scenes

# CONTENTS

## ETSI CA Assessment

- Assessment results
- **Behind the scenes**
  - Audit Frequency and Coverage
  - Audit Process
  - Audit Documentation

# CONTENTS

## ETSI CA Assessment

- Assessment results
- **Behind the scenes**
  - Audit Frequency and Coverage
  - Audit Process
  - Audit Documentation

# ETSI AUDIT FREQUENCY AND COVERAGE

## ETSI EN 319 403

### 7.4.6 Audit Frequency

- *There shall be a period of no greater than **two years** for a full (re-)assessment audit unless otherwise required by the [...] commercial scheme applying the present document.*

### 7.9 Surveillance

- *[...] It is recommended that at least **one surveillance audit per year** is performed in between full (re-)assessment audits.*

### 7.10 Changes affecting certification

- Changes, like
  - a) major changes in the CA (TSP) documentation;
  - b) changes in CA (TSP) policies, objectives or procedures affecting the trust service; or
  - c) security relevant changes

**...will result in an audit either of the change or even of the full scope before implementation!**

# ETSI AUDIT FREQUENCY AND COVERAGE RESULT

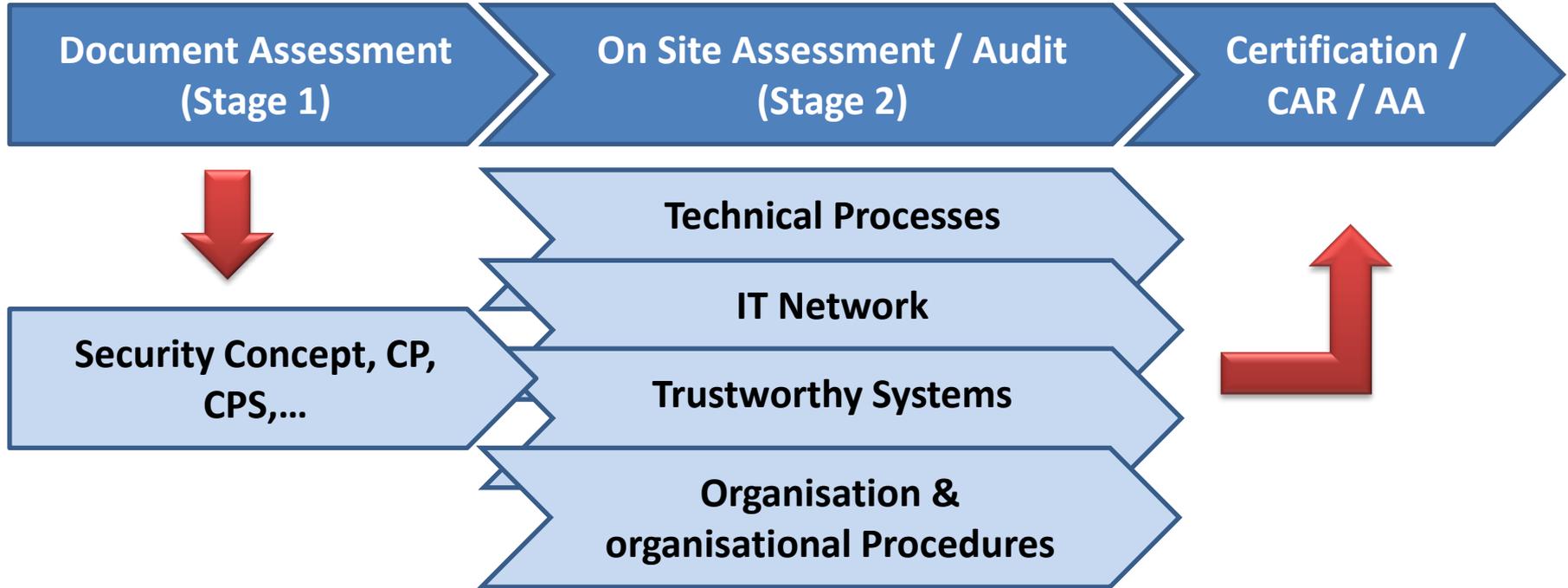
**The CA (TSP) current operations  
is covered by an audit at any time!**

# CONTENTS

## ETSI CA Assessment

- **Assessment results**
- **Behind the scenes**
  - Audit Frequency and Coverage
  - Audit Process
  - Audit Documentation

# AUDIT PROCESS



# PRINCIPLE ELEMENTS OF CONFORMITY ASSESSMENT - ETSI TS / EN

## 1. Document assessment (security concept / operations) - Stage 1

- all necessary technical, functional and organisational security measures and
- their appropriateness for fulfilment of eIDAS requirements

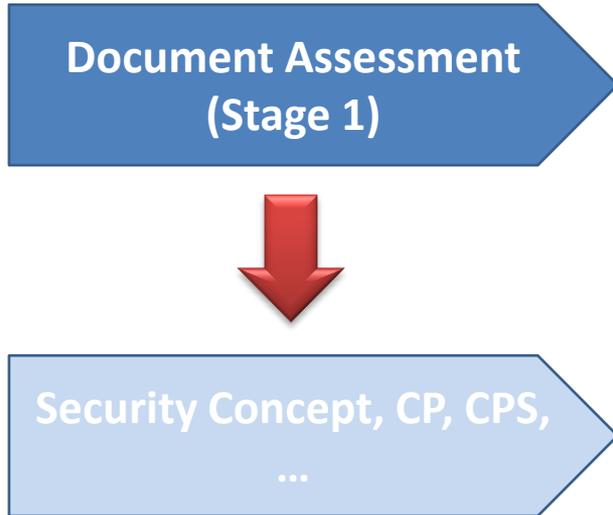
## 2. On-Site assessment - Stage 2

- verify implementation of security measures
- including technical and penetration testing

## 3. Results documentation

- scope: identification of the TSP, service and policy
- content and summary of conformity assessment activities
- audit results
- additional content as required by third parties like browsers, supervisory body,...

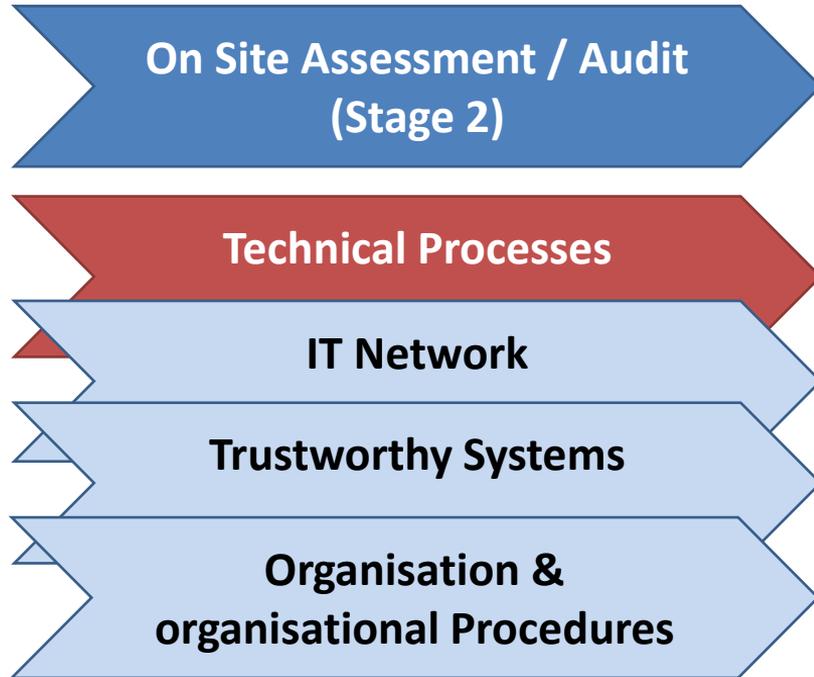
# CA ASSESSMENT AND AUDIT PROCESS



## Document assessment - Stage 1

- remote check CA set of policy and operational documents
- find an appropriate measure described for every single ETSI requirement
- auditor judges measure for appropriateness and completeness

# CA ASSESSMENT AND AUDIT PROCESS

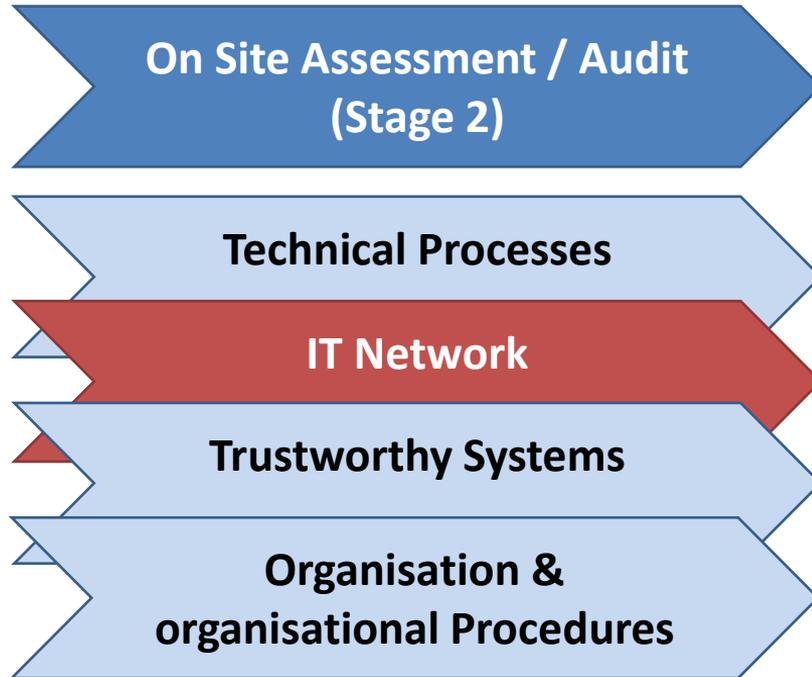


## On-Site assessment - Stage 2

Technical Processes: Spot check of technical security functions

- Cryptographic algorithms
- Trusted channels
- etc.

# CA ASSESSMENT AND AUDIT PROCESS



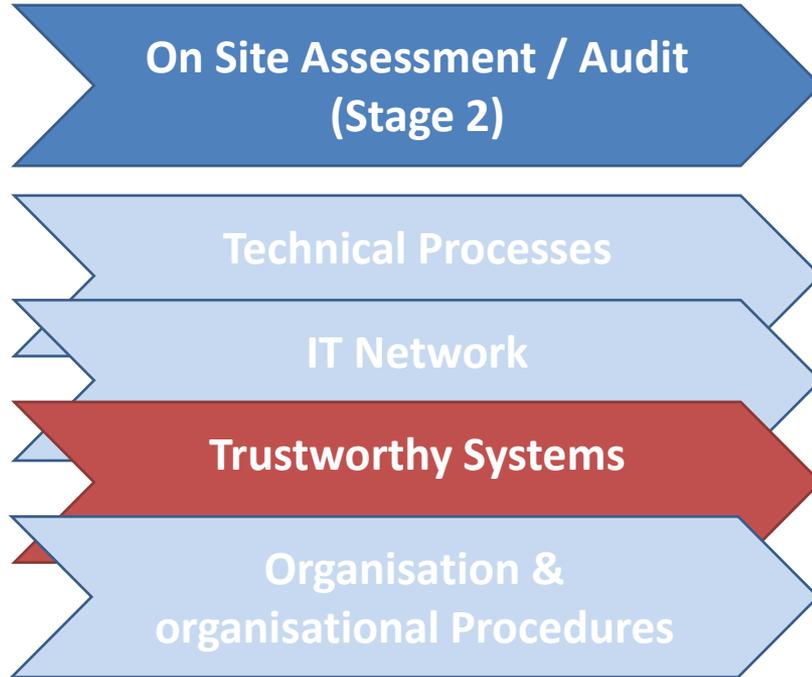
## On-Site assessment - Stage 2

IT Network: Check of relevant CA network

- Management
- Penetration testing
- Vulnerability analysis

Oriented on CA/B-Forum Network security requirements.

# CA ASSESSMENT AND AUDIT PROCESS

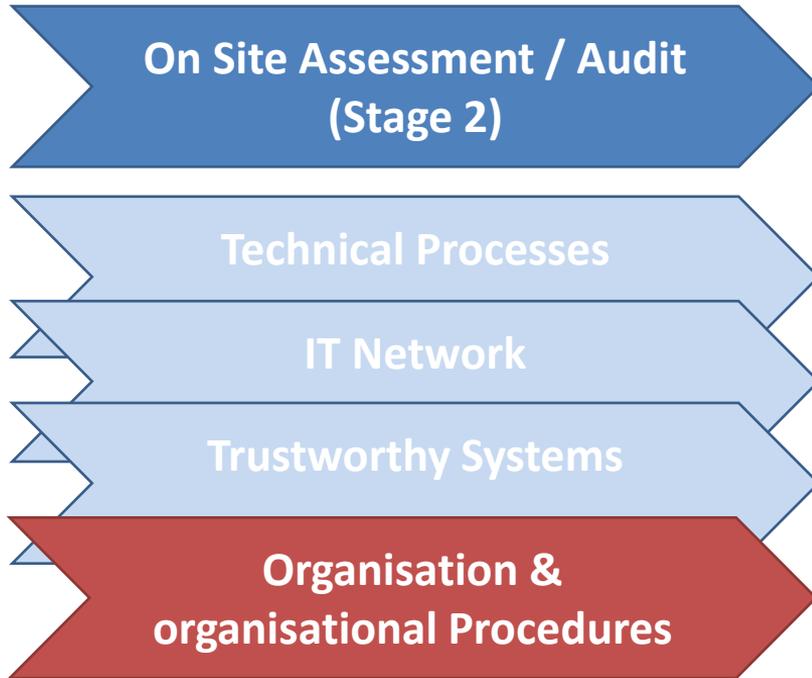


## On-Site assessment - Stage 2

Trustworthy Systems:

- Check of HSM identification, certification and mode of operation
- etc.

# CA ASSESSMENT AND AUDIT PROCESS



## On-Site assessment - Stage 2

Organization: Evidence check for

- IT Security Management
- CA operations (incident and risk mgmt. including follow-up, etc.)
- Personnel security
- etc.

# CERTIFICATION



CA  
CAR / AA  
(+Cert)

Qualified TSP included in  
Trust Service Status List  
(TSL)



Third parties:  
- Supervisory Body  
- Browsers  
- ...

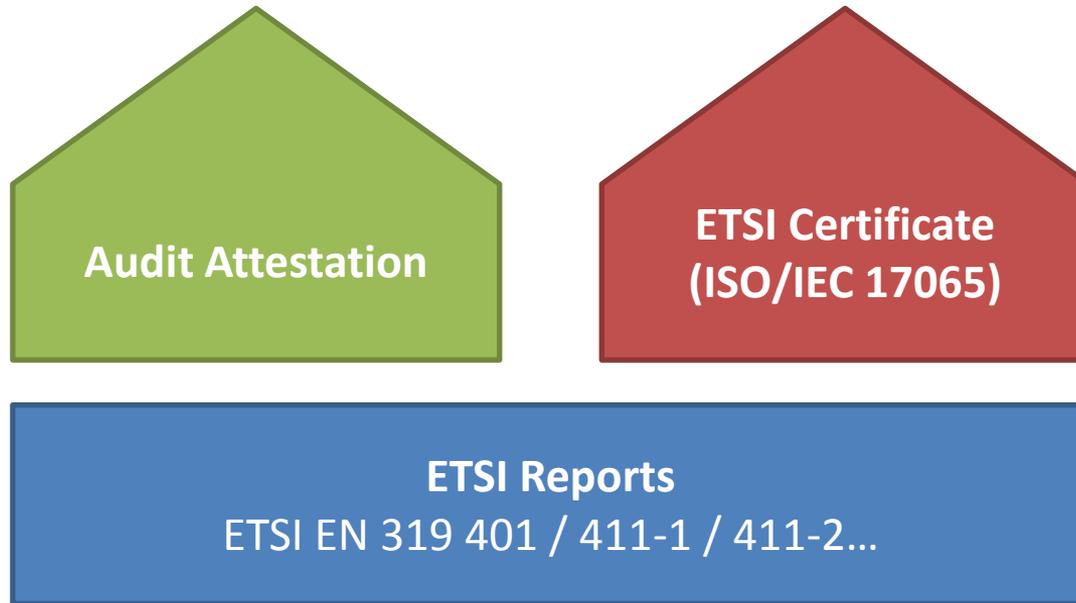
# CONTENTS

## ETSI CA Assessment

- **Assessment results**
- **Behind the scenes**
  - Audit Frequency and Coverage
  - Audit Process
  - Audit Documentation

# AUDIT DOCUMENTATION

## General Structure



# ASSESSMENT RESULTS

## Audit Attestation



### Audit Attestation for CA <<CA name>>

To whom it may concern,

This is to confirm, that <<Auditor company name>> has successfully audited the <<names of the CAs>> operated by

<<name and address of the company operating the CA>>  
<<unique company ID>>

on behalf of

<<name and address of the CA's company>>  
<<unique company ID>>

[...]

# ASSESSMENT RESULTS

## Audit Attestation



[...]  
The audit took place from <<audit period>> according to the appropriate ETSI Technical Specifications.  
<<Name of Conformity Assessment Body >> is accredited to perform such audits by <<name of national accreditation body>> under registration ID <<ID>>. The audit was performed as full audit and will be documented and referred to in the according certificates, which will be issued in <<date of certificate issuance>>:  
<<unique IDs of certificate, ETSI specifications, policies>>

...  
[...]

# ASSESSMENT RESULTS



## Audit Attestation

[...]

The CAs had been issued under the following Root CAs which had been covered and successfully audited according to **<<ETSI specification and policy>>**:

Root 1, Friendly Name: "abcd for Data Protection ZZZZZZZZ 2015 Certification Service", audited for policy LCP,

CN: ZZZZZZZZ 2015

Thumb Print (SHA-1): 46 5b ...

Certificate Serial #: 00

[...]

# ASSESSMENT RESULTS

## Audit Attestation



[...]  
The assessment covered the period <<start date and end date of audit period>>.  
The **next assessment has to be successfully finalized before <<date>>** in order to maintain the certificate validity as stated in the corresponding certificates issued by **<<Conformity Assessment Body>>**.

The assessment performed covered all relevant CAs, including their roots as described in the aforementioned certificates that will be issued to **<<name of CA operator>>** The full PKI hierarchy has been documented during the audited - see Appendix I to this audit attestation.

**<<name of CA operator>>** may publish this audit attestation in a publicly-accessible location, as required.

In case of any question, please contact **<<contact of the conformity assessment body: name, email, phone>>**

# ASSESSMENT RESULTS

## ETSI Certificate under EA Accreditation



Website: [www.fnas.fr](http://www.fnas.fr)  
E-mail: [akreditoint@fnas.fr](mailto:akreditoint@fnas.fr)

**GERMANY**  
DAKKS  
Deutsche  
Spielmar  
10117 Ber  
Phone: +4  
Fax: +49 (0  
Website: +  
E-mail: co

Website: [www.esk.ee](http://www.esk.ee)  
E-mail: [info@esk.ee](mailto:info@esk.ee)

**GREECE**  
ESYD

**FRANCE**  
COFRAC  
Comité français d'accréditation  
52 rue Jacques Hilaret  
75012 PARIS  
Phone: (33) 01 44 68 82 20  
Fax: (33) 01 44 68 82 21  
Website: [www.cofrac.fr](http://www.cofrac.fr)  
E-mail: [information@cofrac.fr](mailto:information@cofrac.fr)

**HUNGARY**  
NAH  
National

**GREECE**  
ESYD  
Hellenic Accreditation System

Die Zertifizierungsstelle der TÜV Info  
bescheinigt hiermit dem Unternehmen

**Izenpe S.A.**  
**Beato Tomás de Zum**  
**71 - 1ª Planta**  
**01008 Vitoria-Gasteiz**

für den Zertifizierungsdienst

**CA de Certificados SS**

die Erfüllung aller Anforderungen der

**ETSI TS 102 042 V2.4**  
**policy EVCP.**

Die Anlage zum Zertifikat ist Bestan  
aus 7 Seiten.  
Dieses Zertifikat gilt nur in Verbindun  
Prüfbericht bis zum 31.07.2018.

**2015** **Trusted Site**  
**Voluntary Validat**  
© TÜVIT - Member of TÜV NORD GRC

Essex, 26.07.2015

Dr. Christoph Gultor  
Leiter Zertifizierungsstelle

**TÜV Informationstechnik GmbH**  
Unternehmensgruppe TÜV NORD

45141 Essen  
www.tuvt.it

**LSTI**

ATTESTATION DE QUALIFICATION

**CERTEUROPE**

Siège : 26, rue du Faubourg Poissonnière 75010 PARIS

The Provider is in conformity with applicable requirements to be qualified under the French Decree 2010-112 published on 2 February 2010 related to articles 9,10 and 12 of the French directive 2005-1516 published on 8 December 2005 on electronic exchanges between users and administrative Authorities and between administrative Authorities.

Electronic certification services provided by the Provider in accordance with the requirements of the Référentiel Général de Sécurité (RGS) approved by the French Prime Minister (arrêté du Premier ministre du 6 mai 2010) are detailed in appendix.

The Provider is in conformity with Decree of 26 July 2004 on the certification of electronic service providers and recognition organizations that conduct their evaluation. Signing certificates at the level RGS\*\* issued by the provider are presumed qualified in accordance with Decree No. 2001-272 of 30 March 2001 adopted in application of article 1316-4 from the French Civil Code and on the electronic signature and in accordance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Provider issues certificates that meet the requirements of ETSI/TS 101456 V1.4.3, Policy Requirements for certification authorities issuing qualified certificates in accordance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures and the French regulation n° 2000-230 of 13 March 2000, Decree n°2001-272 of 30 March 2001 and Order of 26 July 2004.

The provider issues certificates that meet the requirements of ETSI/TS 102042 V2.1, Electronic Signatures and Infrastructures ; Policy Requirements for certification Authorities issuing public key certificates.

Armelie Trotin  
Présidente LSTI

**cofrac**  
Certification  
FRANCE  
11 000  
1999  
23 Juin  
Le présent certificat peut être vérifié auprès de LSTI

**LSTI - 24, AVENUE DE MOKA - 35400 SAINT-MALO**  
RCB 483 897 883 SAINT-MALO ; NAB AU CAPITAL DE 97 000 €  
WWW.LSTI-CERTIFICATION.FR

ETSI Certificate  
(ISO/IEC 17065)



Thanks for your attention!



**Clemens Wanko**  
ACAB'c Vice-Chairman

@TUViT  
IT Infrastructure  
+49 201 8999-586  
c.wanko@tuvit.de