

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page 1 of 39	

**CERTIFICATION FOR QUALIFIED TRUST SERVICE PROVIDER**  
**ACCORDING TO UE 2014\_910 “eIDAS” AND ETSI EN 319 401 FOR THE FOLLOWING SERVICES:**

SERVICE: Not qualified and Qualified certificate for web authentication (Art. 45 of the eIDAS Regulation UE 2014\_910 “eIDAS” and ETSI EN 319 401, ETSI EN 319 411-1 e 411-2)

**1 AUDIT GENERAL DATA**


<b>Type of audit</b>		<b>Certification audit</b>				[ ]
		<b>Extension of Scope</b>				[ ]
		<b>Supplementary Audit</b>				[ ]
		<b>Annual surveillance (Period of time)</b>				[X]
		<b>Renewal</b>				[ ]
<b>Start date</b>	3-12-2018	<b>End date</b>	4-12-2018	<b>Duration (days)</b>	2	
<b>Period of time</b>	7-12-2017	<b>End date</b>	2-12-2018			
<b>Organization</b>		<b>INFOCERT S.p.A.</b> Società soggetta a direzione e coordinamento di TINEXTA S.p.A. VAT (Value Added Tax) IT 07945211006 NTR (National Trade Register) IT - 1064345				
<b>Identification of the conformity assessment body (CAB):</b>		<b>CSQA Certificazioni Srl</b> , Via S. Gaetano, 74, 36016 Thiene VI, registered under the Italian Business Register VAT number 02603680246, Economic and Administrative Repertoire n. 258305 Accredited by L'ENTE ITALIANO DI ACCREDITAMENTO shortly ACCREDIA, national accreditation body under registration accreditation registration for the certification of trust services according to “DIN EN ISO/IEC”				
<b>Registered office (Address)</b>		Piazza Sallustio, 9 - 00187 ROMA				

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>2</b> of <b>39</b>	

<b>Operational headquarters (Address)</b>	p.za Luigi da Porto,3, 35131 Padova PD Italy
<b>Other eventual operational headquarters (address)</b>	Via Malavolti,5 41122 MODENA (MO) DC di Disaster Recovery C/O SIXTEMA
<b>Reference Person</b>	Giuliana Marzola
<b>Audited trust services and reference regulations</b>	<p><b>Qualified trust services provided:</b></p> <ul style="list-style-type: none"> <li>• <b>Qualified certificate for web authentication (Art. 45 of the eIDAS Regulation UE 2014_910 “EIDAS” and ETSI EN 319 401, ETSI EN 319 411-1 (LCP and OVCP; NCP and EVCP); 411-2 (QCP-w)</b> <ul style="list-style-type: none"> <li>○ CA/Browser Forum Baseline Requirement ver 1.6.1</li> <li>○ CA/Browser Forum Guidelines for The Issuance and Management Of Extended Validation Certificates ver 1.6.8</li> </ul> </li> </ul> <p>For details see <b>POLICIES SCHEMA</b> and <b>ROOT CAs CHAIN</b> at § 7</p>
<b>CAB Accreditation reference</b>	<p>CSQA Certificazioni Srl is accredited by Italian National Accreditation Body (Accredia – <a href="http://www.accredia.it">www.accredia.it</a>) for the following:</p> <p><i>“TSP (Trust Service Provider) and the services they offer compared with (EU Regulation) 910/2014 and / or specific provisions adopted by the national authorities for the services covered by the Accreditation Scheme.” (Scheme: PRD; Standard: UNI CEI EN/ISO/IEC 17065:2012; Certificate: N.014B;</i></p> <p><i><a href="https://bit.ly/2Qyb5Xo">https://bit.ly/2Qyb5Xo</a>; <a href="https://bit.ly/2LV2fll">https://bit.ly/2LV2fll</a>.” The eIDAS Accreditation scheme is available here:</i></p>
<b>Attached documents</b>	<ul style="list-style-type: none"> <li>[1] Check list SSL</li> <li>[2] Report VIE Eidas CA of 13/06/2018</li> <li>[3] ICERT INDI MOWS 3.0</li> <li>[4] Terms and Condition Vers. November 2018</li> <li>[5] PKI Disclosure Statement Ver 2.0 of 20/06/2018</li> </ul>

### 1.1 AUDIT GROUP

**Roles:** RGVI = Audit Group Manager; RGVQ = Audit Group Manager in qualification; AVI = Auditor responsible for Inspection; AVIQ = Auditor responsible for Inspection in Qualification; OSS = observer; ET = Technical expert

Name	Role	Signature
Natale Prampolini	RGV Team Leader	

### 1.2 INTERVIEWED REPRESENTATIVES OF THE ORGANIZATION

Name	Role
Giuliana Marzola	Certification Service Manager (TSP)
Luigi Rizzo	New Product Development Specialist
Elena Baki	Information Security Auditor
Valentina Zoppo	Privacy Manager
Umberto Caretta	Quality Assurance & Compliance Manager
Giuseppe Magro	CA Logbook Management Specialist under Devops Application Development Team
Giuseppe Parlato	Network Specialist under Security & Infrastructure Team
Elisa Rubin	Risk and Information Security Specialist
Nicolò Poniz	Head of Security & Infrastructure Team

### 1.3 DESCRIPTION OF OBJECTIVE EVIDENCES AS REGARDS THE MANAGEMENT OF NON-COMPLIANCES OF THE PREVIOUS AUDITS

**Auditor's comment:** The completion of the resolution plan has been verified during this audit, on December 2018

Observation no.	Date	Type of Observation	Regulation requirement	Auditor's observation	Remediation
(1, 2, 3, etc.)	(Audit date)	(e.g. NC_P; NC_E, NC_I, SM, etc.)		(comprehensive statement of the observation including objective evidences)	
1	6/12/2017	<b>NC_I</b>	[ETSI 319 401] Clause 5	ITA: Non risultano evidenti nell'Analisi dei Rischi, l'identificazione e relativa valutazione di revoca dagli "store" (p.es Mozilla,etc) dell'outsourcer Camerfirma (Route che "trusta" la SubCA infocert) EN: In the Risk Analysis, the identification and relative evaluation of the risk concerning the outsourcer Camerfirma's (Route that "trusta" the infocert SubCA) revocation from the "stores" (p.es Mozilla, etc) are not evident.	ITA: Il Documento MG165 doc metodologia rischio SGI_v3.4 del 4.6.18 è stato aggiornato e il rischio specifico aggiunto nello specifico MG165 - CA - Risk Analysis CA_SSL 2018 alla riga 41. EN: The document MG165 doc risk methodology SGI_v3.4 of 4.6.18 has been updated and the specific risk added in the specific MG165 - CA - Risk Analysis CA_SSL 2018 in line 41.
2	6/12/2017	<b>NC_I</b>	[ETSI 319 411-1] Clause 6.2.2 a	ITA: Non sono sufficientemente dettagliati nella PR525- IT_DELIVERY WEB SERVER V. 2.0 10.10. 2017 i controlli	ITA: La procedura PR525 è stata aggiornata con il documento PR525_IT_DELIVERY CERTIFICATI WEB

Observation no.	Date	Type of Observation	Regulation requirement	Auditor's observation	Remediation
				<p>sulla documentazione presentata dal richiedente caso di Società straniera.</p> <p>EN: Checks on the documentation submitted by the applicant for a foreign Italian company, are not enough detailed in the PR525-IT _DELIVERY WEB SERVER V. 2.0 10.10. 2017.</p>	<p>SERVER_ANALISI PER PAESE 1.0 del 29.5.18</p> <p>EN: Procedure 525 has been updated with the document PR525_EN_DELIVERY CERTIFICATI WEB SERVER_ANALISI PER PAESE 1.0 dated 29.5.18</p>
3	6/12/2017	NC_I	[ETSI 319 411-1] Clause 6.1	<p>ITA: Le CGS (Condizioni generali Servizio), il modulo Richiesta Certificato SSL e CPS (certificate Practice Statement) attualmente non sono in inglese, sono in traduzione</p> <p>EN: The CGS (Terms and Conditions), the SSL Certification Request Form and CPS (Certificate Practice Statement) are not in English, the translation is ongoing.</p>	<p>ITA Le traduzioni sono state effettuate e sono disponibili sul sito web all'indirizzo <a href="https://www.firma.infocert.it/documentation/">https://www.firma.infocert.it/documentation/</a></p> <p>EN: The translations have been made and are available at <a href="https://www.firma.infocert.it/documentation/">https://www.firma.infocert.it/documentation/</a></p>

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page 6 of 39	

## 2 OTHER INFORMATION CONCERNING THE TRUST SERVICES PROVIDED

Certification Authority Service			
N° Employees working for this service	12 FTE (TSP for CA –SSL incl)		
Registration Authority	4 internal for SSL		
N° issued certificates	<p><b>ROOT GlobalChambersign (Camerfirma): Sub CA InfoCert Organization Validation CA 3:</b></p> <ul style="list-style-type: none"> <li>N° WEB SSL QWAC Certificate: 0</li> <li>N° Client Authentication Certificate: 45 certificates in the period</li> <li>N° WEB SSL OV Certificate: 152 certificates in the period</li> </ul> <p><b>ROOT: InfoCert Root CA 3 - Sub CA: InfoCert Extended Validation SHA256 - CA 3:</b></p> <ul style="list-style-type: none"> <li>N° Certificate: NOT ISSUING CERTIFICATE TO DATE.</li> </ul> <p><b>ROOT: InfoCert Root CA 3 - Sub CA: InfoCert Organization Validation SHA256 - CA 3:</b></p> <ul style="list-style-type: none"> <li>N° Certificate: NOT ISSUING CERTIFICATE TO DATE.</li> </ul>		
Outsourced activities	Company (company name, address)	Type of activity performed	Certifications in possession
	Infocamere	Housing Data center - Padova	ISO 27001
	Sixtema	DR Site- Modena	ISO 27001
	Sirecom	Service desk – monitoring of events	--
	Intuity	Vulnerability assessment e penetration test	Qualified as organization / laboratories providing tests of vulnerability assessment & penetration test, as per National Supervisory Body
	Giotto	Contact Center	
	Mediatica	Contact Center	

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>7</b> of <b>39</b>	

	AC Camerfirma SA (Spain)	ROOT GlobalChambersign	QTSP for the services CA/QC, TSA/QTST, WebTrust for Cas, WebTrust for Cas – SSL Baseline with Network Security, WebTrust for Cas – EV SSL
Specific information about this audit.	This audit checked all the operations <b>for the full period of time</b> since the last audit. For this purpose, sample certificates have been extracted for each month and checked for compliance to cover the full period of time since last audit. Moreover, the incident & problem management System has been checked and investigated, to get confidence on the CA operations.		

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>8</b> of <b>39</b>	

### 3 DOCUMENTS ANALYSIS

The organization has drawn up the documentation supporting Certification Authority Service according to the indications established in the standards ETSI EN 319 401 and ETSI EN 319 411-1 and 411-2 as well as in the management systems supporting the services provided. The publicly disclosed documentation provides sufficient information and the certificate policy and certificate practice statement are publicly available on Website (qualified trust service provider). CPs and CPSes have been reviewed and updated twice in 2018.

#### 3.1 LIST OF DOCUMENTS CHECKED

The detail of documentation and evidences found has been reported in the reference Check list attached.

#### 3.2 SAMPLE OF CERTIFICATE VERIFIED DURING THE AUDIT

In the period InfoCert has issued 152 Web Server Certificates (OV SSL). The first certificate was issued the 5th of January. All the 21 certificates issued from the 1st of May until the 19<sup>th</sup> of July were reissued to be compliant with the Google's certificate transparency requirements.

The auditor assessed the lifecycle of the following certificates:

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Signature Algorithm	Not Before	Not After	SKI
1	1	CN = www.sanmarinoteatro.sm OU = ARTI PERFORMATIVE - ISTITUTI CULTURALI O = Pubblica Amministrazione della Repubblica di San Marino C = SM	CN = InfoCert Organization Validation CA 3 SERIALNUMBER = 07945211006 OU = WSA Trust Service Provider O = InfoCert S.p.A. C = IT	091c889f4caa7b225aef68d985a4738519d134be	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	2018-07-20 07:24:29 UTC	2019-07-20 00:00:00 UTC	888dffe6fb2aeab35b29f978be5ea3cae7d30bc1
1	2	CN = accesso.cdp.it O = Cassa Depositi e Prestiti SPA L = Roma S = Lazio C = IT	CN = InfoCert Organization Validation CA 3 SERIALNUMBER = 07945211006 OU = WSA Trust Service Provider O = InfoCert S.p.A. C = IT	427d74cd96a52a8eb0a18ea9d2e431a2614c530	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	2018-07-27 08:19:43 UTC	2020-07-27 00:00:00 UTC	8c308aee3e2fd54cbcdc1110e6f4f5bae3d6a50f

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it			SCHEME: eIDAS	Procedure: <b>174015/14</b>
			FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
			Page <b>10</b> of <b>39</b>	

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Signature Algorithm	Not Before	Not After	SKI
1	3	CN = pcc.asl2.liguria.it OU = Sistemi Informativi Aziendali O = ASL2 Savonese L = SAVONA C = IT	CN = InfoCert Organization Validation CA 3 SERIALNUMBE R = 07945211006 OU = WSA Trust Service	56ecb6436e7512e415ec5221a0605d4eef8bbd5	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	2018-07-30 06:56:28 UTC	2020-07-30 00:00:00 UTC	c94782fcac18016011e6a2d7763384cf6502c00d
1	4	CN = www.comune.valsamoggia.bo.it OU = Servizio Informatico Associato O = Comune di Valsamoggia L = Valsamoggia S = Bologna	CN = InfoCert Organization Validation CA 3 SERIALNUMBE R = 07945211006 OU = WSA Trust Service	194c21f986f198f6435a8bbe6e99430d7bf3e9e3	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	2018-08-13 08:21:12 UTC	2019-08-13 00:00:00 UTC	a642b503db14cc1e89dfce05cfa8f71648af5d7f
1	5	CN = www.ilportaleofferte.it OU = Sistema Informativo Integrato Parallelo O = Acquirente Unico S.p.A. L = Roma C = IT	CN = InfoCert Organization Validation CA 3 SERIALNUMBE R = 07945211006 OU = WSA Trust Service	38b1d07543e7139255fc3bdce8c62fc007f48640	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	2018-09-06 10:12:06 UTC	2019-09-06 00:00:00 UTC	a4d80ba73c6c793affaada83085fd4f03b97163f

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Signature Algorithm	Not Before	Not After	SKI
1	6	CN = www.regdial.it OU = Telemedicina O = COOPERATIVA EDP La traccia L = Matera S = Matera C = IT	CN = InfoCert Organization Validation CA 3 SERIALNUMBE R = 07945211006 OU = WSA Trust Service	0eb7b297cf38f8aaf5 3a9e0e1925ba76009 bcfcc	rsaEncr yption	(204 8 bit)	sha256WithRSAEncryption	2018-10-31 16:14:21 UTC	2019-10-31 00:00:00 UTC	01bf7ccc1ccedbe62e20378176 44ba8782c404a4
1	7	CN = soluzionibenessere.groupa ma.it OU = Security O = Groupama Assicurazioni SpA L = Roma S = Italia C = IT	CN = InfoCert Organization Validation CA 3 SERIALNUMBE R = 07945211006 OU = WSA Trust Service	3368e0ee4830c95feb 4b2831dda1994d645 72fdf	rsaEncr yption	(204 8 bit)	sha256WithRSAEncr yption	2018-11-19 10:05:06 UTC	2020-11-19 00:00:00 UTC	33768c8726cd819d76241de2f 7e2f7c8bf8cfd41

### 3.3 NON-COMPLIANT CERTIFICATES

The following cases are reported to problems related to the certificate generation service or to misissued certificates, concerning the SubCA "InfoCert Organization Validation CA 3".

**Problem concerning the OCSP responder of the SubCA InfoCert Organization Validation CA 3. The period under investigation is from the 12<sup>th</sup> of December 2017 through the 22<sup>th</sup> of December 2017**

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>12</b> of <b>39</b>	

In details errors are:

*Responder URLs that violate the BR prohibition on returning a signed a "Good" response for a random serial number. Responder*

*URLs GET response are 404*

The 12th of December 2017 Mozilla highlighted that the OCSP responder for the subCA InfoCert Organization Validation CA3 returned a 404 error for a request in GET mode and a valid "good" answer about a status request for a certificate that had not been issued, motivating that, as indicated in section 4.9.10 of the BRs, the OCSP responders must support the GET method and the OCSP responders MUST NOT respond with a "good" status for the certificates not issued. In response to what Mozilla communicated through the dedicated forum on mozilla.org, Camerfirma communicated that it was informed about this issue on the 12th of December 2017 06:55 (UTC) and that on the 12th of December 2017 07:00 (UTC) contacted the InfoCert technical team that manages the subCA requesting the correction of the errors. The 19th of December 2017 16:42 (UTC) the InfoCert technical team confirmed that both problems had been solved. Meanwhile Camerfirma had told Mozilla that it was not considered to stop issuing certificates from this subCA because this issue didn't affect the quality of the structure of the certificates.

#### **Problem regarding the issuing of misissued certificates**

- See details in <https://crt.sh/?id=326112834&opt=cablint>
1. The CA was notified about the misissuance by email from Camerfirma, the 9<sup>th</sup> of February 2018
  2. The certificate was revoked the 9<sup>th</sup> of February 2018
  3. The CA software was modified for avoiding issuing any other similar certificate. However, currently every newly generated web server certificate is checked by using certlint before being provided to the end customer.
  4. This is the only certificate generated with such error: "ERROR: DNSName must not start with ."
  5. crt.sh ID: 326112834; SHA-256(Certificate): 5D8545DF25B7DDB7EA6E9EAEC083920FD47F2EB4CB504379AB5994011D518D7E
  6. When the certificate was generated, the CA software did not yet check the presence in the SubjectAlternativeName extension of any DNS name starting with .
  7. See item 3)

- See details in <https://crt.sh/?id=381869446&opt=cablint,x509lint>
1. The CA became aware of the problem in consequence of Camerfirma e-mail of the 10<sup>th</sup> of April.

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>13</b> of <b>39</b>	

2. The certificate was revoked the 10<sup>th</sup> of April at 08:42:32 UTC
3. The CA software was modified for avoiding issuing any other similar certificate. Moreover every newly generated web server certificate will be checked by using certlint before being provided to the requesting customer.
4. This is the only certificate generated with such errors: “ERROR: Constraint failure in X520OrganizationalUnitName: ASN.1 constraint check failed: UTF8String: constraint failed (X520OrganizationalUnitName.c:174)” and “ERROR: organizationalUnitName too long”
5. crt.sh ID: 381869446; SHA-256(Certificate): 649E679DE605C25A7415CED080B54BC1A18BA33734B574DA96AC73613ACEB530
6. The CA returned an error when this certificate was requested to be generated, but the CA operator had the possibility to force certificate generation even if the CA reports a problem in generating such certificate. Because of the end customer urgency the operator wrongly decided to force the certificate generation.
7. The possibility to force any certificate generation in case of errors reported by the CA was dropped by modifying the CA software.

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>14</b> of <b>39</b>	

#### 4 RISK ANALYSIS AND TREATMENT PLAN

Infocert has defined a Risk Analysis process concerning the trust services defined in the application scope of this audit. The Methodology (Informational risk methodology 4.6.18) explains how the model examines the risk scenarios and evaluates threats and vulnerabilities for their potential impact on the services. The risk scenarios, the assets and the controls/countermeasures are specific for the CA environment, included in the ISO 27001 scope. Infocert implements annually, or in case of any major change, a risk assessment activity, with relative treatment plan and residual risk acceptance by risk owners.

The Risk Management procedure is MG165 Metodologia Gestione Rischio Infocert REV v3.4 del 4.6.18. The current implementation of this methodology is based on the GRC RM tool (Governance Risk & Compliance Management), which contains the records of the risk analysis and whose functional structure is described in InfoCert - Risk Management SharePoint Platform - Functional Analysis. The available latest risk assessments reports are as follows: Global risk assessment, carried out in June 2018: a MG165 Risk Analysis 2018 - Specific assessment of the CA risk and a MG165 - CA - Risk Analysis CA\_SSL 2018 version.

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>15</b> of <b>39</b>	

## 5 AUDIT RESULTS

### 5.1 ANALYSIS REPORT

The analysis of the service has been carried out by using the reference clause defined in **ETSI EN 319 411-1 and ETSI EN 319 411-2** as reported in the attachment [1].

For each requirement, the following is reported:

- The audit method used
- The comment and the evidence
- Indication of conformity and improvement suggestions

### 5.2 COMPREHENSIVE ASSESSMENT

Hereunder, the evidences of the audit carried out on all the operating controls established into Regulation (Eu) 2014\_910 “eIDAS” and ETSI EN 319\_401, 411-1 e 411-2 standards are reported with reference to the Certification Authority audit. The TSP has defined, and keeps updated, a chart concerning the management of indexes for each process and for each significant product/ service. The KPI are monitored in compliance with the company policies. The audit is carried out every year during the Top Management review.

### 5.3 GENERAL REQUIREMENTS FOR QUALIFIED TSPs WITH INDICATION OF RELEVANT ARTICLES OF EIDAS REGULATION.

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
i.	<b>Data processing and protection (Art.5)</b>		7.13 Compliance	<b>Comment:</b> The organization is aware of the actual data protection laws in Italy D.Lgs 196/2003 & of the EU GDPR 679/16. <b>Evidence as follows:</b> <ul style="list-style-type: none"> <li>Piano della Sicurezza INDI-PPS ver. 3.1 23.05.2018</li> <li>Communication Tinexta Group (rf prot 20180011739)</li> </ul> The InfoCert privacy policies for their services are publicly available at the URL <a href="https://help.infocert.it/privacy-policy/">https://help.infocert.it/privacy-policy/</a> the privacy policy for InfoCert Services
		Art.5.2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.		<b>Comment:</b> N.A
ii.	<b>Liability and burden of the proof (Art.13)</b>	1. (Art.13.1) TSP liable for damage caused intentionally or negligently to any natural or legal person due to a	7.1.1 Organization Reliability	<b>Comment:</b> The TSP has financial resources, as per public Balance Sheet, and has established: insurance contract to cover liabilities and Voluntary Guarantee Deposit for Termination Evidence as follows: Insurance contract -Infocert SPA “Tutti i rischi dell’informatica” n388750912 start. 31.12.17 exp. 31.12.2018 + APPENDICE -oggetto Tutti i rischi dell’informatica n388750912 with detailed QTSP eIDAS services of 14.5.18:

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>17</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
		failure to comply with the obligations under this Regulation		specified as follow: a) Creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic services of certified delivery and certificates related to these services b) Creation, verification and validation of websites authentication certificates c) Preservation of signatures, seals or electronic certificates related to these services of 10 million of Euro (from 6 million in previous contract) per year and 10 million of Euro for damage  <b>Evidence:</b> Terms and Condition, PKI disclosure Statement and CPS
		a. Burden of proving intention/negligence of non-qualified TSP is on claiming party.		
		b. Intention or negligence of a QTSP shall be presumed, unless proven otherwise by QTSP.		

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>18</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
		2. (Art.13.2) When TSP informed customer in advance on limitations on the use of their services, & when such limitations are recognisable to third parties, TSP not liable when limitations have been exceeded.		
		3. (Art.13.3) In accordance with national rules on liability.		
iii.	<b>Accessibility for person with disabilities (Art.15)</b>		7.13 Compliance	<b>Comment:</b> N.A.

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>19</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
iv.	<b>Due diligence (Art.19.1)</b>	1. TSP shall take appropriate technical and organizational measures to manage the risks posed to the security of the trust services they provide.	5 Risk Assessment	<b>Comment and Evidence:</b> The document MG165 risk methodology SGI_v3.4 of 4.6.18 has been updated and the specific risk added in the specific MG165 - CA - Risk Analysis CA_SSL 2018 in line 41.
		2. Having regard to the latest technological developments, those measures shall ensure that the level of security is		
		commensurate to the degree of risk.		

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>20</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
		3. Measures shall be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents		
v.	<b>Security &amp; personal data breach notification (Art.19.2)</b>	1. TSP shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for	7.9 Incident management	<p><b>Comment:</b> There are all the policies, procedures and Role and Responsibilities provided to be compliant to 24 hours time response to Incident Management</p> <p><b>Evidence:</b></p> <ul style="list-style-type: none"> <li>• Clause 10.6.16 of the CPS and application of the Business Continuity and Disaster Recovery Plan.</li> <li>• MG745 Business continuity plan ver 2.0 31/01/2018</li> <li>• MG745 Piano di continuità CA e TSA ver 3.0 del 01/03/2018</li> </ul>

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>21</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
		information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.		<p>To follow better the new requirements introduced by regulations such as the GDPR, and bodies that issue specific provisions such as the Privacy Authority, ENISA and AgID which classify the events in a diversified manner, the internal organization for incident management envisages two distinct flows with involvement of different groups -for Events related to the availability of services that follow the dictates of ITIL, -for the events of Security &amp; Compliance that instead follow the provisions and classifications issued by the various regulatory bodies</p> <p>To comply with the Art. 19 eIDAS is implemented the procedure required by the AgID Communication OF 19.4.2017: in case of an incident concerning the TSP, a report is drawn up as Template AgID according to the severity and classification levels required by ENISA, then transferred to the Supervision office of AgID encrypted with their public key.</p> <p>To also incorporate relieves from the previous audit eIDAS 2017 and ISO 20000 and 27001 2018: Incident Project (as per the 2018 Management Review) currently under FINALIZATION to review the complete management of the incident through new management and the new tool JIRA</p>
		2. TSP shall also notify the [likely adversely affected] natural or legal [customer] of the breach of security or loss of integrity without undue delay.	7.9 Incident management	
		3. May be required by the supervisory body to inform the	7.9 Incident management	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
		public, when it is in the public interest.		<p>TOOLS: EVENT EST tool (Events on technological services) NEW IMPLEMENTED INSTRUMENT, (in use since MARCH 2018) distinguished by TOOLS for the management of Events and Incidents of Security &amp; Compliance, which is still the tool Sugar + New tool for events registration: TOOL JIRA Sec &amp; Com Events: (in the phase of collection the requirements for the part fulfillment to create specific Tasks, to manage also the Classification, required by the various interested parties like AgID, GDPR Authority, etc)</p> <p>DOCS: Policy MG605_A16_Incidents - Incident management and MG605_A16_Incidents - Classification Safety incidents + updated the PROCEDURE PR 455 INCIDENT MGNT in V8 of 16.4.2018 + created DOC Organization for the management of incidents OF 29/05/2018 which defines the guidelines used for Incident management</p>
vi.	<b>Art.24.2 of the eIDAS Regulation:</b>			
	(a) Inform SB of any change in QTS provisioning and of intention to cease;	6.1 Trust Service Practice Statement		<p><b>Comment and Evidence:</b></p> <p>Certificate Policy - Certificate Practice Statement for web authentication certificate VERS. 3.0 of 30.11.18.</p> <p>The TSP has in place a CPS review process, in which describe how communicate the changes. Before publishing new CPS changes on the webpage, InfoCert will inform Agid</p>

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>23</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
	(b) Requirements on staff;		7.2 Human Resources	<p><b>Comment and Evidence:</b>  InfoCert has implemented and certified a Quality Management System according to ISO 9001 and an Information Security Management System according to ISO / IEC 27001. Human Resources are managed according following procedures/evidences:</p> <ul style="list-style-type: none"> <li>• Clause 5.3 of the CPS.</li> <li>• MG433 GESTIRE LA FORMAZIONE</li> <li>• MG435_Gestire Risorse Umane</li> <li>• MG295 GESTIRE PIANIFICAZIONE AP 295 GESTIRE APPROVVIGGIONAMENTI</li> </ul> <p>2018 specific training</p> <ul style="list-style-type: none"> <li>• training PSD2 Vetting for Validation Specialist -22.11.18</li> <li>• training Seminario SignaCert – 21-02-2018</li> </ul> <p><b>ROLES &amp; REPONSABILITIES GENERAL e x SSL:</b></p> <p><b>ASSIGNMENT CA Responsible:</b> to Giuliana Marzola from 11.5.15, revised on 1.12.17 to better define relative tasks.</p> <p><b>RAOVS (Validation Specialist):</b> Validation Specialists maintain a skill level that enables them to perform such duties satisfactorily: in the CA context the RAOVS who collects and verifies identity information about the subscriber (certificate applicant) and the related organization is different from the one that validates the domain and approves the request.</p> <p>RAOVs are formally appointed: 5 persons –already RAO for CA + special appointment for SSL: V. ES. appointment letter for Marco Grotto – time stamp 14.11.17</p>

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>24</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
	(c) Sufficient financial resources and/or liability insurance, in accordance with national law;		7.1 Internal Organization	<p><b>Comment:</b> The TSP has financial resources, as per public Balance Sheet, and has established: insurance contract to cover liabilities and Voluntary Guarantee Deposit for Termination</p> <p><b>Evidence as follows:</b> Voluntary Guarantee Deposit for TERMINATION Clause 5.8, and 9.6 and 9.7 of the CPS.</p> <p>Insurance contract -Infocert SPA “Tutti i rischi dell’informatica” n388750912 start. 31.12.17 exp. 31.12.2018 + APPENDICE -oggetto Tutti i rischi dell’informatica n388750912 with detailed QTSP eIDAS services of 14.5.18: specified as follow: a) Creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic services of certified delivery and certificates related to these services b) Creation, verification and validation of websites authentication certificates c) Preservation of signatures, seals or electronic certificates related to these services of 10 million of Euro (from 6 million in previous contract) per year and 10 million of Euro (from 3 million in previous contract) for each single insurance claim to cover liabilities</p>

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>25</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
	(d) Consumer information on terms and conditions, incl. limitations on use;		6.2 Terms and Conditions	<p><b>Comment:</b> Terms and conditions are drawn up, and are published and available 24x7 on the website, under the service documentation section, with a specific referral to eIDAS regulation.</p> <p><b>Evidence:</b></p> <p>PKI disclosure statement and terms and conditions are available at <a href="https://www.firma.infocert.it/documentation/">https://www.firma.infocert.it/documentation/</a></p> <p>The organization or the APPLICANT who has powers or has been delegated by the organization, requests SSL certificate, digitally signing a request form (PDF: DATA of the Organization and CERTIFICATE...) which also contains ref. to TERMS &amp; CONDITIONS (TSP standard verified in the previous audit x CA-with in-depth analysis for the SSL service) and confirmation of acknowledgment of terms and conditions and privacy policies.</p>
	(e) use trustworthy systems and products;		7.3 3 Asset management 7.4 4 Access control 7.5 Cryptographic controls 7.6 Physical and environmental security	<p><b>Comment:</b> The organization is compliant to this requirement as per the ISO 27001:2013 certificate and per the on-site audit. CSQA 27001:2013 Certificate n: 21501</p> <p><b>Evidence:</b></p> <ul style="list-style-type: none"> <li>• Clause 5, 6.5 of the CPS.</li> <li>• MG165 Security Policy Vers. 2.1 29/01/2016</li> <li>• Log of logical and physical accesses stored in the InfoCert system for a long preservation “LegalDOC”</li> </ul>

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>26</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
	(f) use trustworthy systems to store (personal) data;		7.7 Operation security 7.8 Network security	<p><b>Comment:</b> The organization physical security is compliant</p> <p>The Root CA system is physically in the "bunker" zone of the InfoCert DataCenter and logically in the CA separated environment. The networks schema shows that physical segregation is in force and the LAN and VLAN are separated via firewall to obtain the required security</p> <p>All the communications are under https and/or VPN.</p> <p>The internet connection is provided by a TLC provider with a double connection, and there is a second TLC provider that provides one more connection.</p> <p><b>Evidence</b></p> <ul style="list-style-type: none"> <li>• CPS Clause 5.1 and Physical and Environmental Security Policy</li> <li>• IT/Segregazione delle reti e policy di firewall versione 1 del 02/09/2016</li> <li>• MIS - Management of Information Systems IT / Configurazione e implementazione policy di sicurezza sulla rete Infocert versione 2 del 18/10/2017</li> <li>• CMDB_PKI_CA3_asset_Cens</li> <li>• Schema-rete-CA_cens</li> <li>• Firewall log: Firewall logging and some extractions were viewed although some data were obscured (IPs and server names are sensitive data)</li> <li>• VA/PT Report: Tests performed with software Rapid7 InsightVM and with some manual activity by</li> </ul>
	(g) take appropriate measures against forgery and theft of data;			

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>27</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
				Intuity <b>Ecer-EcerCA</b> test date 07/05/2018 all the vulnerabilities that were found, have been fixed ( epic change SEC-59 ) <b>Signacert</b> test date 26/11/2018 no vulnerabilities were found
	(h) Record and keep accessible activities related data, issued and received, even after cessation;		7.10 Collection of evidence	<b>Comment:</b> The organization is compliant. The data are store in InfoCert system of digital preservation <b>Evidence:</b> <ul style="list-style-type: none"> <li>Clause 5.4, 5.5 of the CPS (applicable to Qualify Certification Service for EU qualified website authentication certificates)</li> <li>“Prodotto INDI – Infocert Digital Certification MO/GDCCA – Archiviazione dei Giornali di Controllo delle CA” ver 2.2 05/09/18</li> </ul>
	(i) Up-to-date termination plan (to be agreed with SB) to ensure continuity of service;		7.12 TSP Termination and termination plans	<b>Comment:</b> The organization is compliant. <b>Evidence:</b> <ul style="list-style-type: none"> <li>Clause 5.8 of the CPS (applicable to Qualify Certification Service for EU qualified website authentication certificates)</li> <li>“IT_TSP Termination CA” ver 1.2 20/11/2018</li> </ul>
	(j) Ensure lawful processing of personal data		7.13 Compliance	<b>Comment:</b> The organization is aware of the actual data protection laws in Italy D.lgs 196/2003 and with the implementation of the new EU GDPR 679/16 <b>Evidence as follows:</b> Clause 9.3-9.4-9.5-9.15 of the CPS applicable to Qualify

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>28</b> of <b>39</b>	

Cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence (DEC 2018)
	in accordance with Directive 95/46/EC.			Certification Service for EU qualified website authentication certificates) and “terms and conditions”

#### 5.4 Specific requirements for the applicable type of qualified trust.

Qualified trust service	Specific requirements eIDAS	EU qualified certificate policy reference: - ETSI EN 319 411-1 e 411-2	Comment / Evidence
<b>Qualified certificate for Web Authentication</b>	1. Art.24.1.a) to d)	1. ETSI EN 319 411-1, clause 6.2.2 Initial identity validation ETSI EN 319 411-1, clause 6.2.3 Identification and authentication for Re-key requests	1. Different checks are in place in order to assure the certificates applicants and related organizations identity validation and verification. Such procedures are followed by InfoCert employees (no Third Parties are in charge at the moment with operations regarding SSL certificate life cycle management). The evidences required for the initial identification of the domain applicant (person and organization) are indicated in the CPS 4.2. The validator specialist collects, verifies and puts them into InfoCert digital preservation system. All operations described



<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>30</b> of <b>39</b>	

Qualified trust service	Specific requirements eIDAS	EU qualified certificate policy reference: - ETSI EN 319 411-1 e 411-2	Comment / Evidence
	5. 6. Art.45 – Annex IV	<p>requires this service to be provided free of charge.</p> 5. ETSI EN 319 411-1 clause 6.6.1 i) and ii) Certificate profile	<p>5. The certificate profiles are according to RFC 5280. Some Certificates were provided and reviewed that's the ones assessed in § 3.3</p> <p><b>Evidence:</b></p> <ul style="list-style-type: none"> <li>PR525-IT _DELIVERY WEB SERVER CERTIFICATES V. 3.0 of 10.10.2018 (Gestione DELIVERY e Assistenza InfoCert Certificati Web Server/Richiesta,controlli e rilascio del servizio)</li> <li>“Prodotto INDI – Infocert Digital Certification MO/GDCCA – Archiviazione dei Giornali di Controllo delle CA” ver 2.2 05/09/18</li> </ul>

## 5.5 SUMMARY OF OBSERVATIONS

Type
ESSENTIAL NON-COMPLIANCE (NC_E)
MINOR NON-COMPLIANCE (NC_I)
IMPROVEMENT SUGGESTIONS (SM)

Hereunder, it is reported the summary of observations raised during the current audit and reported in the document “PAC” –Corrective Actions Plan:

Observation no.	Date	Type of Observation	Regulation requirement	Auditor's observation
<i>(1, 2, 3, etc.)</i>	<i>(Audit date)</i>	<i>(e.g. NC_P; NC_E, NC_I, SM, etc.)</i>		<i>(comprehensive statement of the observation including objective evidences)</i>
1	3-12-2018	NC_I	[ETSI 319 411-1 and 411-2] Clause 6.2.4 Clause 4.9 of the CA Browser Forum BR	<p>ITA: Si è riscontrata la presenza di 4 certificati web authentication errati emessi dalla subCA “InfoCert Organization Validation CA 3”. Questi certificati presentano l’emailAddress nel SubjectDN. Questi certificati errati non sono installati ma alla data non risultano esser stati revocati. Si raccomanda di procedere alla revoca dei certificati misissued di cui sopra.</p> <p>EN: It was found the presence of 4 incorrect web authentication certificates issued by the subCA "InfoCert Organization Validation CA 3. The certificates had the emailAddress in the Subject. The certificates are not used and not installed anywhere but not revoked. It is recommended to proceed with the revocation of the misissued certificates referred to above.</p>

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>32</b> of <b>39</b>	

Observation no.	Date	Type of Observation	Regulation requirement	Auditor's observation
2	4-12-2018	NC_I	[ETSI 319 411-1] Clause 4.2.5; 5.2 and 5.3	<p>ITA: Nel Manuale Operativo non ci sono policy e procedure riguardanti i certificati client che invece, alla data, risultano esser stati emessi dalla subCA "InfoCert Organization Validation CA 3". Si raccomanda di prevedere delle procedure di richiesta e rilascio, nonché le relative policy per i certificati di tipo client authentication.</p> <p>EN: In the CPS there are no policies and procedures regarding client authentication certificates that have been issued by the subCA "InfoCert Organization Validation CA 3". It is recommended to detail the procedures for requesting and issuing these certificates and the policies that are applying to them.</p>
3	3-12-2018	SM	[ETSI 319 411-1 and 411-2] Clause 6.3	<p>ITA: Si consiglia di descrivere attraverso il supporto di uno schema grafico, tutto il flusso di richiesta e rilascio di un certificato web authentication in maniera da aiutare gli auditor nella comprensione del processo di generazione</p> <p>EN: It is advisable to describe all the request flow and submission of a web authentication certificate, also through the support of a graphic scheme in order to help the auditors in understanding the generation process already existing in a log that is more intelligible and easier to consult.</p>

## 5.6 TOTAL AMOUNT OF OBSERVATIONS

Type	No.
ESSENTIAL NON-COMPLIANCE (NC_E)	--
MINOR NON-COMPLIANCE (NC_I)	2
IMPROVEMENT SUGGESTION (SM)	1

## 6 RESERVES AND/OR ORGANIZATION NOTES

No reserve.

## 7 CONCLUSIVE INDICATIONS

The Organization **INFOCERT Spa**, that carries out the function of Trust Services Provider (TSP) is **considered compliant to the requirements of the (EU) REGULATION no. 910/2014 (eIDAS)** as regards the electronic identification and trust services for the electronic transactions in the internal market.

The Issuing certificate service, object of the audit, is considered in line with (EU) Regulation no. 910/2014 (eIDAS).

**Moreover, the Trust Services Provider is conforming as regards to Qualified certificates, Organizational Validation and Extended Validation certificates for web authentication** in compliance with the following regulations: (EU) REGULATION no. 910/2014 (eIDAS), ETSI EN 319 401; **ETSI EN 319 411-1 and ETSI EN 319 411-2; CA Browser Forum BR and CA Browser Forum EV Guidelines.**

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>34</b> of <b>39</b>	

**Below are indicate the details about the conformity assessment body, the trust service provider and each audited Root-CA**

<b>Identification of the audited Root-CA:</b>	<b>InfoCert Organization Validation CA 3</b> <a href="http://cert.infocert.it/ca3/ovcf/CA.crt">http://cert.infocert.it/ca3/ovcf/CA.crt</a>	
	Distinguished Name CN = InfoCert Organization Validation CA3 OU = WSA Trust Service Provider O = InfoCert S.p.A. C = IT	
	SHA-256 fingerprint 247a6d807ff164031e0eb22ca85de329a3a4e6603dbc6203f0c6e282a9c9ea84	
	Certificate Serial number	0249528bfbff7ddf
	Applied Policy	InfoCert policy for OV certificates (1.3.76.36.1.1.19.2) ETSI EN policy 319 411-1 OVCP (0.4.0.2042.1.7) CabForum policy OV Certificates for Web Authentication (2.23.140.1.2.2) <hr/> InfoCert policy for qualified [QWAC] OV certificates (1.3.76.36.1.1.45.2) ETSI EN policy 319 411-2 QCP-w (0.4.0.194112.4) CabForum policy OV Certificates for Web Authentication (2.23.140.1.2.2) Remarks: Qualified certificates aimed specially to PSD2 QWACs, <b>not yet issued</b>

Identification of the audited Root-CA:	<b>InfoCert Extended Validation SHA256 - CA</b>
	Distinguished Name CN = InfoCert Extended Validation SHA256 - CA 3 OU = WSA Trust Service Provider O = InfoCert S.p.A. C = IT
	SHA-256 fingerprint fe5e29a8bc39e99b1a1e77d29590ac1948a337a387c63e83f0c4b18bfc8be1b2
Certificate Serial number	6b445ba522e87824cff71ce8444f9bb887f5e4b1
Applied Policy	InfoCert policy for qualified [QWAC] EV certificates (1.3.76.36.1.1.45.3) ETSI EN policy 319 411-2 QCP-w ( <b>0.4.0.194112.4</b> ) CabForum policy EV Certificates for Web Authentication (2.23.140.1.1) <b><u>Remarks: not yet issued</u></b> <hr/> InfoCert policy for qualified [QWAC] certificates (1.3.76.36.1.1.45.4) ETSI EN policy 319 411-2 QCP-w ( <b>0.4.0.194112.4</b> ) Remarks: Qualified certificates aimed specially to PSD2 QWACs, <b>not yet issued</b>

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>36</b> of <b>39</b>	

Identification of the audited Root-CA:	<b>InfoCert Organization Validation SHA256 - CA 3</b> <a href="http://cert.infocert.it/ca3/ovca/CA.crt">http://cert.infocert.it/ca3/ovca/CA.crt</a>
	Distinguished Name CN = InfoCert Organization Validation SHA256 - CA 3 OU = WSA Trust Service Provider O = InfoCert S.p.A. C = IT
	SHA-256 fingerprint 90f70db89e1f300aa162ad351e44d5d19a64be441d59fd8c57fc7af71bd5352a
Certificate Serial number	7d04f008647c18b07ee55a1f5a45874c7b45855b
Applied Policy	InfoCert policy for qualified [QWAC] OV certificates (1.3.76.36.1.1.45.2) ETSI EN policy 319 411-2 QCP-w ( <b>0.4.0.194112.4</b> ) CabForum policy OV Certificates for Web Authentication (2.23.140.1.2.2) <b><u>Remarks: not yet issued</u></b> <hr/> InfoCert policy for qualified [QWAC] certificates (1.3.76.36.1.1.45.4) ETSI EN policy 319 411-2 QCP-w ( <b>0.4.0.194112.4</b> ) Remarks: Qualified certificates aimed specially to PSD2 QWACs, <b>not yet issued</b>

### 7.1 SUGGESTIONS PURSUANT TO AUDIT

The suggestions of the audit Group will be subject to assessment by CSQA Certification Committee, which has the authorization for conforming them, or eventually, for modifying them.

<b>Certification issuing</b>	<input type="checkbox"/>	<b>Maintenance of certification</b>	<input checked="" type="checkbox"/>	<b>Renewal</b>	<input type="checkbox"/>
<b>Modification of application scope</b>	<input type="checkbox"/>	<b>Suspension</b>	<input type="checkbox"/>		
<b>Indicate the next audit and eventual operational notes or explanations:</b>			<input type="checkbox"/>	Supplementary certification audit	
			<input type="checkbox"/>	Surveillance	
			<input type="checkbox"/>	Supplementary surveillance	
			<input type="checkbox"/>	Extension of certification	
			<input checked="" type="checkbox"/>	Renewal	

### 7.2 SUBDIVISION OF AUDIT TIMES (\*)

Description	No. of days*
Time dedicated to auditing the documents of the system	0,5
Time dedicated to the analysis of risks assessment	0,2
Time dedicated to the audit of operating processes	1,3
Time dedicated to the preparation of the report	0,5

(\*) In case of first Certification, the audit times shall be intended inclusive of Stage 1 and Stage 2.

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>38</b> of <b>39</b>	

## 8 DECLARATIONS CONCERNING THE PRESENCE OF CRIMINAL PROCEEDINGS OR OTHER LEGALLY SIGNIFICANT SITUATIONS

The company declares:


- X **not to have** criminal proceedings or other significant legal situations (e.g.: injunctions, revocation of authorizations) to communicate to CSQA.
- ☐ to **have** criminal proceedings or other significant legal situations (e.g.: injunctions, revocation of authorizations) to communicate to CSQA (please, attach documents)
- 
- X that, in the days when the audit was carried out, emergency situations and events whose nature is such to lead to the incompliance with the applicable normative obligations on matters related to environment and/or health and safety at the work place **have not occurred**.
- ☐ that, in the days when the audit was carried out, emergency situations and events whose nature is such to lead to the incompliance with the applicable normative obligations on matters related to environment and/or health and safety at the work place have occurred (please, attach reports/ documentation/ communication).

## 9 DECLARATIONS AND ANSWER TO OBSERVATIONS.

- This report:
  - includes all the results of the audit as well as the list of observations that shall be dealt with for meeting the requirements necessary for certification
  - is disclosed by the Audit Group in the name and on behalf of CSQA Certificazioni Srl.
- As established in the applicable accreditation regulations, the audit activity, **and its consequent result and observations reported**, is based on a **sampling** of the information available.
- The suggestions of the Audit Group as regards the result of the audit itself shall be subject to **independent assessment** by the Certification Executive Committee, that is authorized to confirm them or, if necessary, to modify them.
- In case Stage 2 Audit cannot be immediately performed, the Company **shall send within 30 days from the date of this report** the “Corrective Actions Plan- CAP model” **to CSQA and to the Assessment Group Manager**. The CA plan shall be completed in the specifically dedicated spaces with the Corrective Actions suggested for solving the observations emerged during this audit. **The above mentioned Plan has not to be returned if it includes only observations made as “Improvement suggestions”.**
- CSQA will assess the Corrective Actions suggested by the Company for approval within the following 15 days and reserve itself the right, if necessary, to require the integrations necessary. The Corrective Actions suggested are intended as approved by CSQA in case no communication is sent to the Company within the established due time.

<b>CSQA Certificazioni Srl</b> Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: <b>174015/14</b>
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page <b>39</b> of <b>39</b>	

It is noted that the members of the Audit Group sign a Confidentiality declaration aimed at protecting the confidentiality of the information acquired during the audit activities and, therefore, also concerning this audit.

Date 4-12-2018	 <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> Signature of the Audit Group Manager(*)
(*) The signature of the report by the appointed Audit Group Manager certifies the truthfulness of the information included in it and, especially, the effective presence during the audit of the Organization members and of CSQA Assessment Group members mentioned in the very same report.	

4-12-2018	
Date <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/>	Signature of the Organization (*) <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/>
(*) The signature of the Organization certifies that: <ul style="list-style-type: none"> <li>The Organization is in possession of this report</li> <li>The Organization confirms that the data concerning the identification of your Organization and the definition of the application scope are correct.</li> <li>The organization has been informed that CSQA regulations applicable to this report are available and can be consulted in the website <a href="http://www.csqa.it">http://www.csqa.it</a>. On the contrary, if the organization does not have the possibility of connection to the website, it commits to inform CSQA who shall send it.</li> <li>The organization <b>does not have</b> criminal proceedings or other significant legal situations (e.g.: injunctions, revocation of authorizations) to communicate to CSQA.</li> <li>in the days when the audit was carried out, emergency situations and events whose nature is such to lead to the incompliance with the applicable normative obligations on matters related to environment and/or health and safety at the work place <b>have not occurred</b>.</li> <li>CSQA Certificazioni Srl commits itself to protect the confidentiality of the information acquired during this audit.</li> </ul>	