

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 1 a 36	

CERTIFICATION FOR QUALIFIED TRUST SERVICE PROVIDER

ACCORDING TO UE 2014_910 “eIDAS” AND ETSI EN 319 401 FOR THE FOLLOWING SERVICES:

SERVICE: Organization Validation certificate for web authentication (Art. 45 of the eIDAS Regulation UE 2014_910 “eIDAS” and ETSI EN 319 401 and ETSI EN 319 411-1)

1 AUDIT GENERAL DATA

Type of audit		Certification audit				[]
		Extension of Scope				[]
		Supplementary Audit				[]
		Annual surveillance (Period of time)				[X]
		Renewal				[]
Start date	5-12-2018	End date	6-12-2018	Duration (days)	2	
Period of time		7-12-2017 - 5-12-2018 (1year)				
Organization		Intesa Sanpaolo S.p.A. VAT (Value Added Tax) IT 11991500015 NTR (National Trade Register) IT —00799960158				
Identification of the conformity assessment body (CAB):		CSQA Certificazioni Srl, 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”				
Registered office (Address)		Piazza San Carlo, 156 -10121 TORINO				
Operational headquarters (Address)		Intesa Sanpaolo S.p.A.IN REMOTE CONFERENCE at Infocert office: p.za Luigi da Porto,3, 35131 Padova PD Italy				
Other eventual operational headquarters (address)		Via Malavolti,5 41122 MODENA (MO) DC di Disaster Recovery C/O SIXTEMA				
Reference Person		Intesa Sanpaolo S.p.A.: Maurizio Sisto - Infocert : Luigi Rizzo; Elena Baki				


CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 2 a 36	

Audited trust services and reference regulations	Qualified trust services provided: <ul style="list-style-type: none"> • Certificate for web authentication ETSI EN 319 401, ETSI EN 319 411-1 (LCP and OVCP) <ul style="list-style-type: none"> ○ CA/Browser Forum Baseline Requirement ver 1.6.1 <p>For details see POLICIES SCHEMA and ROOT CAs CHAIN at § 7</p>
CAB Accreditation reference	<p>CSQA Certificazioni Srl is accredited by Italian National Accreditation Body (Accredia – www.accredia.it) 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>https://bit.ly/2Qyb5Xo; https://bit.ly/2LV2fll).”</i> The eIDAS Accreditation scheme is available here:</p>
Attached documents	<p>[1] Check list SSL</p> <p>[2] Report VIE Eidas CA of 13/06/2018</p> <p>[3] ISP-CBCM-002-2018-01.2</p>

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 3 a 36	

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
Luigi Rizzo	New Product Development Specialist
Elena Baki	Information Security Auditor
Silvia Beltrami	Design support for certificates SSL & Digital Signature – Consulting Company PA ABS Moncalieri (Torino)
Cecilia Abbati	Risk Analysis Responsible for Cybersecurity, Business Continuity Strategy – ISP – Bisceglie (Milano)
Maurizio Sisto	Design Responsible for certificates SSL & Digital Signature – Società ISP – Moncalieri (Torino)
Gloria Roero	Technical & Legal Advice for QTSP Consulting Company EY S.p.A. Moncalieri (Torino)
Serena Ciolino	Technical & Legal Advice for QTSP Consulting Company EY S.p.A. Moncalieri (Torino) (Torino)

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	07/12/2017	NC_I	[ETSI 319 401] Clause 5	ITA: Non risultano evidenze dell'Analisi dei Rischi, specifica per il servizio WEB SSL OV Certificate oggetto di audit (Evid: Data Security & Information Security e Business Continuity Areas interviews)	ITA: Emissione del documento Analisi del Rischio per Certificati SSL OV, v.01 del 8-11-18
				EN: There are not evidence of the specific Risk Analysis for WEB SSL OV Certificate service (Evid: Data Security & Information Security e Business Continuity Areas interviews)	ENG: Issue of the document Risk Analysis for OV SSL Certificates, v.01 of 8-11-18
2	07/12/2017	NC_I	[[ETSI 319 401] Clause 7.2	ITA: Nella contrattualistica di riferimento, non risultano sufficientemente dettagliate, le attività e responsabilità operative per i certificati SSL (Organisation Validation) di competenza di Intesa San Paolo, rispetto a quelle affidate in outsourcing ad Infocert SPA. Assicurare un quadro più omogeneo della documentazione di riferimento del Contratto. (offerta secondo standard di Intesa: prot.2226 del 28.2.17/4.5.17: offerta per fornitura di una infrastruttura di CA servizi esterni +- ODA 7200104017 del 26.6.17 + INTESA SAN PAOLO CUSTOMER CARE MASTER- SLA InfoCert relativi alle CA Agid_Identrust e SSL del 3.11.17 , MANUALE OPERATIVO, ETC)	ITA: Emissione del documento Ruoli e Responsabilità per la CA Intesa SanPaolo per Certificati SSL OV, v.01 del 1-12-18
				EN: The activities and operational responsibilities for the SSL certificates (Organization Validation) pertaining to Intesa San Paolo are	

CSQA Certificazioni Srl

Via s. Gaetano, 74 - 36016 Thiene (Vi)

Tel. 0445 313011 - Fax 0445 313070

csqa@csqa.it

www.csqa.it



SCHEME: eIDAS

Procedure: **174015/4**

FORM: RVETSP_ST2

REV. 3 – March, 24th 2016

Pag. 5 a 36

Observation no.	Date	Type of Observation	Regulation requirement	Auditor's observation	Remediation
				not sufficiently detailed in the reference contracts, compared to those outsourced to Infocert SPA. Ensure a more homogeneous picture of the reference documentation of the Contract. (quote according to Intesa standard: prot.2226 of 28.2.17 / 4.5.17: quote for a CA infrastructure supply external services + - ODA 7200104017 of 26.6.17 + INTESA SAN PAOLO CUSTOMER CARE MASTER- SLA InfoCert relativi alle CA Agid_Identrust e SSL del 3.11.17, OPERATING MANUAL, ETC	the CA Intesa SanPaolo for OV SSL Certificates, v.01 of 1-12-18
3	06/12/2017	NC_I	[[ETSI 319 401] Clause 7.12	ITA: Non risultano chiare nel TERMINATION PLAN: Cessazione fornitura dei servizi di certificazione digitale (v. 01.06.2017), le tempistiche/priorità previste per l'espletamento delle attività indicate	ITA: Nuovo Termination Plan v 2 del 16-10-2018
				EN: The following issues are not clear in the TERMINATION PLAN: (Cessazione fornitura dei servizi di certificazione digitale (v. 01.06.2017), the timing / priorities defined for the implementation of the indicated activities	ENG: New Termination Plan v 2 date 16-10-2018

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 6 a 36	

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			
N° issued certificates	ROOT: Camerfirma Sub CA: Intesa Sanpaolo Organization Validation CA: <ul style="list-style-type: none"> N° Client Authentication Certificate: 0 N° WEB SSL OV Certificate: In the period between the 7th of Dicembre 2017 and the 3rd of December 2018 Intesa San Paolo has issued 269 Web Server Certificates (OV SSL). 		
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	
	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

CSQA Certificazioni Srl

Via s. Gaetano, 74 - 36016 Thiene (Vi)

Tel. 0445 313011 - Fax 0445 313070

csqa@csqa.it

www.csqa.it



SCHEME: eIDAS

Procedure: **174015/4**

FORM: RVETSP_ST2

REV. 3 – March, 24th 2016

Pag. **7** a **36**

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 8 a 36	

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 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 between the 7th of Dicembre 2017 and the 3rd of December 2018 Intesa San Paolo has issued 269 Web Server Certificates (OV SSL).

During the audit the auditor was able to analyze a set of certificates. Of these certificates, 11 have been seen in each specific attribute whose characteristics can be read below.

The auditor assessed the lifecycle of the following certificates:

z	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI
1	1	CN = www.intesasanpaoloforvalue.com OU = Intesa Sanpaolo S.p.A. O = Intesa Sanpaolo S.p.A. L = Lodi S = Lodi C = IT	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	5a 65 ee 27 81 14 30 9b af fd 58 da 5d 97 84 17 49 89 2b 75	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	25/01/2018 13:26:49 UTC	25/01/2020 00:00:00 UTC	1e 52 15 80 26 fd 2f e7 69 69 5b be 2c e3 d7 ce 1b 61 56 7c
1	2	CN = ibcm.eurizoncapital.it OU = Intesa Sanpaolo S.p.A. O = Intesa Sanpaolo S.p.A. L = TO S = TO C = IT	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	32 4e 6e 90 f6 97 48 5f b6 af 71 5c 53 ba c9 c3 81 d1 ab 91	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	09/02/2018 13:34:35 UTC	09/02/2020 00:00:00 UTC	64 e7 04 bf 72 d8 cf 86 27 9a 0b 0b 48 f1 9a 30 7b d4 ba 5c
1	3	CN = www.intesasanpaoloreoco.com O = Intesa Sanpaolo S.p.A. S = TO C = IT subjectAltName www.intesasanpaoloreoco.com www.intesasanpaoloreoco.it	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	19 e3 61 15 2b c3 62 b8 17 f4 67 d7 6e 6f d3 67 40 ad 5b 2c	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	19/03/2018 07:02:55 UTC	19/03/2020 00:00:00 UTC	62 a8 20 a4 b0 a8 f0 7d 4f f3 85 2e 84 1d 92 95 9b ef 2a 9a
1	4	CN = www.fondazioneintesasanpaoloonlus.org O = Intesa Sanpaolo S.p.A.	CN = Intesa Sanpaolo Organization Validation CA	21 c9 d3 a4 bb 0b 23 73 0f 83 fe 5a 6e 03 66 73 e8 d1 b2 7d	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	20/04/2018 08:52:59 UTC	20/04/2020 00:00:00 UTC	2c a5 f9 ee cd 45 da d1 db 0e 99 97 2f 83 4b 0f d7 20

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 10 a 36	

z	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI
		L = Turin S = Italy/TO C = IT	SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT				ryption			bf 0f
1	5	CN = www.info-vendite.it OU = IT O = Intesa Sanpaolo S.p.A. L = Torino S = Italia C = IT	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	5c 77 ee e0 a0 75 2e a1 d1 68 46 26 78 18 70 de a6 65 f7 14	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	16/05/2018 14:05:14 UTC	16/05/2020 00:00:00 UTC	34 69 42 b3 87 cc c0 3f fe 6e 07 1e 57 8b c9 e7 22 18 60 2c
1	6	CN = www.sirefiduciaria.it O = Intesa Sanpaolo S.p.A. C = IT S = Italia L = Torino	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	1b 9d 32 0e 0a 68 93 0f 6b 0b d4 ee 79 e9 ac 9d 50 fb 68 88	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	28/06/2018 14:42:11 UTC	28/06/2020 00:00:00 UTC	5f 96 d8 7f 14 36 55 98 39 de 51 1d 01 bd ac fe b5 eb fe aa
1	7	CN = www.info-vendite.com O = Intesa Sanpaolo S.p.A. C = IT L = Torino S = Italia OU = Intesa Sanpaolo S.p.A. subjectAltName www.info-vendite.com www.info-vendite.it info-vendite.com info-vendite.it	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	2b c9 4b 71 2b 9b 2f d4 2f bf e6 16 39 76 63 00 a5 aa ad b1	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	26/07/2018 14:09:49 UTC	26/07/2020 00:00:00 UTC	36 f2 9e ba ea f1 cb f6 d8 58 0f 96 d9 0f b6 8b c7 20 6c 36

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 11 a 36	

z	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI
1	8	E = fmtorino@eng.it CN = demoweb.infogroup.it O = Intesa Sanpaolo S.p.A. L = Torino S = Italia C = IT	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	07 df 8e 09 5c bc 88 84 8b 58 4c db 10 11 19 5a 4d aa 24 fb	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	08/08/2018 10:17:54 UTC	08/08/2020 00:00:00 UTC	5c 5a e8 ca c7 69 31 57 9e ad 53 bd f4 c4 a3 c9 aa b7 d1 dd
1	9	CN = www.digifatturapro.it OU = Intesa Sanpaolo S.p.A. O = Intesa Sanpaolo S.p.A. L = Torino S = Italia C = IT subjectAltName www.digifatturapro.it www.digifatturapro.com www.digifatturastart.it www.digifatturastart.com	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	73 9b d3 63 68 cf 6b 45 cb be fe 35 9e db 76 82 5b 2c 05 55	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	17/09/2018 13:58:41 UTC	17/09/2020 00:00:00 UTC	41 fe 37 14 74 22 27 65 b3 36 e2 32 83 d3 ea a4 2a 96 b7 78
1	10	E = noc-ig@eng.it CN = www.terzovalore.com O = Intesa Sanpaolo S.p.A. L = Torino S = Italia C = IT	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT	47 b9 0a 37 f0 bd 3e 3b 57 46 87 b7 c2 b2 b9 0e ce d4 f4 7°	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	12/10/2018 15:30:35 UTC	12/10/2020 00:00:00 UTC	59 e4 4f 31 90 87 dc a1 44 90 07 2d 89 de 28 ec 1f 35 60 74
1	11	CN = www.restituzioni.com O = Intesa Sanpaolo S.p.A. L = Torino S = Italia C = IT	CN = Intesa Sanpaolo Organization Validation CA SERIALNUMBER = 10810700152 OU = WSA Trust Service Provider	60 65 2d 57 d7 88 9c c5 f8 18 ee 05 86 09 c3 4e 25 8f 8a 73	rsaEncryption	(2048 bit)	sha256WithRSAEncryption	21/11/2018 08:49:44 UTC	21/11/2020 00:00:00 UTC	b6 46 30 79 a8 ed 13 90 19 ab ed e0 1d 9c b8 f2 22 2c c1 a1

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 12 a 36	

z	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI
			O = Intesa Sanpaolo S.p.A. C = IT							

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 "Intesa Sanpaolo Organization Validation CA".

Problem	Description
Problem concerning the OCSP responder of the SubCA Intesa Sanpaolo Organization Validation CA. The period under investigation is from the 12th of December 2017 through the 22th of December 2018	<p>In details errors are:</p> <p><i>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</i></p> <p>The 12th of December 2017 Mozilla highlighted that the OCSP responder for the subCA Intesa Sanpaolo Organization Validation CA 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 technical team that manages the subCA requesting the correction of the errors. The 19th of December 2017 16:42 (UTC) the 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.</p>

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 13 a 36	

Problem	Description
Problem regarding the issuing of misissued certificates	<p>misissued certificates: see details in https://crt.sh/?cablint=583&iCAID=57139&minNotBefore=2017-7-7</p> <ol style="list-style-type: none"> 1) The CA was notified about the misissuance by email from Camerfirma, the 18th of October 2017. 2) The first certificate with this error was issued the 15th of September. The notification only covered 62 public certificates. In fact, the subCA has detected on its own another 74 certificates of which there was no notification because they were non-public domains: the total number of misissued certificates was 136. 3) InfoCert had immediately identified the certificates that were generated with a serial number having 20 octets with the first bit set to 1 (and so really with a wrong serial number of 21 octets). The day after this analysis the technical team had applied the needed changes to CA software to solve the issue. The certificates were revoked in November and December 2017 with the exception of 7 certificates (*) that were revoked in August 2018. All certificates were replaced by December 2017 on their websites. 4) There were 136 certificates involved by this problem of the error of the serial number: “ERROR: Serial numbers must be 20 octets or less”. 5) Here below there are the details of the first certificate of the list: crt.sh ID: 242233184; SHA-256(Certificate): D89874110D4F78B0A81A16E524C8A7C241608DE6113CBE26FD99F9BD20051253. In the attached file there are the details of all the misissued certificates (with SubjectDN and SHA256 fingerprint). 6) When the certificates were generated, the CA software did not yet check the correct serial number 7) See item 3) <p>(*) Details about 7 certificates revoked in August 2018</p>

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 14 a 36	

Problem	Description
	<p>A4EC1471059552B7907BB0A4A343AA993026B218 941539242987010476218520211002670872430465430040 C=IT,S=Italy/TO,L=Turin,O=Intesa Sanpaolo S.p.A.,CN=imap.intesasanpaolo.com [was issued in 2017-10-2, revoked in 2018-08-7]</p> <p>99DB6DC3E9668C0A80524952AC30D4C6EC642445 878369013038996342792347839581229606954166658117 C=TR,S=Turkey,L=Istanbul,O=Intesa Sanpaolo S.p.A.,OU=IT,CN=ehaciz.intesasanpaolo.com [was issued in 2017-10-16, revoked in 2018-08-7]</p> <p>BCA86B71FDA78D921DF5C4B41D9DA068AB94BC55 1077046149911901803561343664858156727464103296085 C=IT,S=TO,L=Torino,O=Intesa Sanpaolo S.p.A.,OU=Intesa Sanpaolo S.p.A.,CN=GiftsWeb.intesasanpaolo.com [was issued in 2017-10-18, revoked in 2018-08-7]</p> <p>BCB6908E00F52164EDAF9CF2F7E69D95FA96DBF2 1077361593031557470262603930610150558717896481778 CN=dbstartup.intesasanpaolo.com,O=Intesa Sanpaolo S.p.A.,C=IT,S=TO,L=Torino [was issued in 2017-10-18, revoked in 2018-08-7]</p> <p>CF0243FA05AB2487685D2D3937A329B76A6155AD 1181811612652215764570265834245073667638654227885 C=IT,S=Italy/TO,L=Turin,O=Intesa Sanpaolo S.p.A.,CN=pop.intesasanpaolo.com [was issued in 2017-10-2, revoked in 2018-08-7]</p> <p>D88A5C4696E8B2BC333B8E79BB95F1AB23291B5F 1236227547686010407054852137131246526947333315423 C=IT,S=Italy,O=Intesa Sanpaolo S.p.A.,CN=cwiam0-wsapweb.intesasanpaolo.com [was issued in 2017-10-16, revoked in 2018-08-7]</p> <p>A48C3EDDFC5DDDCFC0ADB55D8A912F34FFEFFDE 939402067242487665294768868625766357908557070302 C=IT,S=IT,O=Intesa Sanpaolo S.p.A.,CN=extn0.intesasanpaolo.com [was issued in 2017-09-12, revoked in 2018-08-8]</p>

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 15 a 36	

Problem	Description
Problem regarding the issuing of misissued certificates: see details in https://crt.sh/?id=214233658&opt=cablint	1) The CA was notified about the misissuance by email from Camerfirma, 20th of October 2017 The certificate was revoked the 20th of November 2017 2) The CA software was modified in order to avoid the inclusion of the email address in the SubjectAlternativeName extension and the generation of serial numbers with more than 20 octets. 3) This certificate had two errors, the serial number > 20 octets and 'ERROR: BR certificates must not contain rfc822Name type alternative name' (CA/B Forum's BR). 4) It was issued in 2017-09-15. It was revoked in 2017-11-20. The last detected certificate with an email into the SAN extension is: https://crt.sh/?id=242854548&opt=cablint . It was issued in 2017-10-23 and revoked in 2017-12-13 5) crt.shID:214233658; SHA-256(Certificate): 4D0D5D141F15AA2691F187D000671ED40561024C052F82B6F0114BBC44389864 6) When the certificate was generated, the PKI Software did not yet carry out checks regarding the inclusion of the emailAddress in the subject alternative name extension and the serial number octets lenght 7) See item 3)
Problem regarding the issuing of misissued certificate: see details in https://crt.sh/?id=326810668&opt=cablint	The CA was notified about the misissuance by email from Camerfirma, the 27 th of February 2018 The certificate was revoked the 3 rd of April 2018 The CA software was modified in order to check not only that one of the two fields locality and the stateorprovince is included in the SubjectDN but also that if any of them is present there shall be also a value This is the only certificate generated with such error: "ERROR: L appears to only include metadata" crt.sh ID: 326810668; SHA-256(Certificate): EA4FF184EEF15E340F1EADB4ABD4ECF8D6563C883A2E42BAA3B77C7C998836F7 When the certificate was generated, the CA software did not yet check that any fields locality and the stateorprovince included in the SubjectDN contained a correct value

Problem	Description
	<p>See item 3)</p> <p>SerialNumber: 42:1b:5a:05:29:81:f5:ae:9d:4f:28:2a:71:6c:23:1f:06:c3:4f:0b commonName = app.totalerg.infogroup.it organizationName = Intesa Sanpaolo S.p.A. localityName = stateOrProvinceName = FI countryName = IT</p> <p>A new certificate to replace the incorrect one was generated the 9th of March, 2018.</p>
<p>WARNING: Name has deprecated attribute emailAddress</p> <p>In October 2018 the subCA has took over two other certificates with the e-mail in the subjectDN:</p>	<p>The 2nd of October 2018 InfoCert informed Intesa San Paolo about the presence of an misissued certificate and asked for its immediate revocation and re-issuance without the emailAddress in the subjectDN (moreover in the email field there is a value different from the email). The attributes of the SubjectDN are detailed below</p> <p>SerialNumber: 4c:28:ea:4d:a1:a4:d3:6e:11:49:55:70:9c:5c:b1:d0:6b:34:0f:bd Validity: Not Before: Sep 27 12:57:56 2018 GMT Not After : Sep 27 00:00:00 2020 GMT commonName = webvpnstrong.intesasnpaolo.com emailAddress = u0e2819 organizationName = Intesa Sanpaolo S.p.A. stateOrProvinceName = Italia countryName = IT</p> <p>The certificate was revoked the 3rd of October 2018.</p> <p>The 17th of October InfoCert identified a certificate with the same problem (warning) of the emailAddress in the subjectDN and requested to Intesa Sanpaolo the immediate revocation</p>

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 17 a 36	

Problem	Description
	<p>and re-issuance without the emailAddress in the subjectDN. The attributes of the SubjectDN are detailed below:</p> <p>Serial Number: 47:b9:0a:37:f0:bd:3e:3b:57:46:87:b7:c2:b2:b9:0e:ce:d4:f4:7a Validity: Not Before: Oct 12 15:30:35 2018 GMT Not After : Oct 12 00:00:00 2020 GMT emailAddress = noc-ig@eng.it commonName = www.terzovalore.com organizationName = Intesa Sanpaolo S.p.A. localityName = Torino stateOrProvinceName = Italia countryName = IT</p> <p>The certificate was revoked the 18th of October, 2018.</p>

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/4
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Pag. 18 a 36	

4. RISK ANALYSIS AND TREATMENT PLAN

IntesaSanPaolo has defined a Risk Analysis process concerning the trust services defined in the application scope of this audit. A new document Risk Analysis for OV SSL Certificates, v.01 of 8-11-18 has been issued , ref. previous NC_I #1 solved.

The Methodology 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. Intesa SanPaolo implements annually, or in case of any major change, a risk assessment activity, with relative treatment plan and residual risk acceptance by risk owners.

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/14
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page 19 of 36	

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** 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 standards are reported with reference to the Certification Authority audit. The TSP has defined, and keeps updated, a management system for service in the audit scope–

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
i.	Data processing and protection (Art.5)	1. Art.5.1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.	7.13 Compliance	Comment: The organization is aware of the actual data protection laws in Italy D.Lgs 196/2003 & of the EU GDPR 679/16. Evidence as follows: Letter: Appointment to the processing of personal data: p.es Marco Grotto (VALIDATION SPECIALIST) Comment: N.A
		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.		
ii.	Liability and burden of the proof (Art.13)	1. (Art.13.1) TSP liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the	7.1.1 Organization Reliability	Comment - Evidence: Intesa San Paolo issues certificates within an internal perimeter. In fact, these are web server domains requested by internal staff. This is evident from the internal operating guide: "ICT Management and IT Security - Enterprise Security - Data Security" version of 28/09/2018

cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence
		<p>obligations under this Regulation</p> <p>a. Burden of proving intention/negligence of non-qualified TSP is on claiming party.</p> <p>b. Intention or negligence of a QTSP shall be presumed, unless proven otherwise by QTSP.</p> <p>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.</p> <p>3. (Art.13.3) In accordance with national rules on liability.</p>		

cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence
iii.	Accessibility for person with disabilities (Art.15)		7.13 Compliance	Comment: N.A. FOR SSL
iv.	Due diligence (Art.19.1)	<div>1. TSP shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.</div> <div>2. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk.</div> <div>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</div>	5 Risk Assessment	Comment and Evidence: The Intesa Sanpaolo Organization Validation CA has implemented a security system for the information system related to the digital certification service. The implemented security system is divided into three levels: <ul style="list-style-type: none"> • a physical layer that aims to guarantee the security of the environments in which the CA manages the service, • a procedural level, with purely organizational aspects, • a logical level, through the preparation of technological hardware and software measures that address the problems and risks associated with the type of service and with the infrastructure used. This security system is designed to avoid risks from the malfunctioning of systems, the network and applications, as well as unauthorized interception or modification of data. Evidence: “- “Risk Analysis - Organization Validation SSL Certificates” version 01 of 08/11/2018”

cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence
v.	Security & personal data breach notification (Art.19.2)	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 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.	7.9 Incident management	<p>The Security Manager of Intesa Sanpaolo maintains an incident management plan that includes the following phases:</p> <ul style="list-style-type: none"> transitory management: at this stage the issuance of certificates and the restoration of additional services at the disaster recovery site are ensured; restoration of full operation: in this phase the restoration of all the CA's services is guaranteed, at the original site or in an alternative one. <p>The supplier responsible for managing the CA has described the incident management procedures related to the SGSI certificate in the ISO 27000. Any incident, as soon as it is detected, is subject to timely analysis, identification of corrective countermeasures and verbalization by the responsible for the service. The report is digitally signed and sent to the supplier's Document Storage System; a copy is also sent to AgID, together with the declaration of the intervention actions aimed at eliminating the causes that may have given rise to the accident, if under the control of InfoCert.</p> <p>Evidence: § 6.7.1 Incident management procedures of the "Certificate Policy – Certificate Practice Statement Intesa Sanpaolo Organization Validation CA "ISP-CBCM-002-2018-01.2" version 01.2 of 01.28/11/2018.</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 public, when it is in the public interest.	7.9 Incident management	

cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence
vi.	Art.24.2 of the eIDAS Regulation:(for qualified services)			
	(a) Inform SB of any change in QTS provisioning and of intention to cease;		6.1 Trust Service Practice Statement	Comment and Evidence: This CP-CPS is drafted, published and updated at least annually and whenever changes occur in the PKI. "Certificate Policy –Certificate Practice Statement Intesa Sanpaolo Organization Validation CA "ISP-CBCM-002-2018-01.2" version 01.2 of 01.28/11/2018.
	(b) Requirements on staff;		7.2 Human Resources	Comment and Evidence: On the occasion of specific needs such as adaptations to the infrastructure, regulatory adjustments or activation of new services, Intesa Sanpaolo provides to provide specific training courses. The supplier, on the other hand, every year, carries out the analysis of the preparatory needs for the definition of the training activities to be provided during the year. The analysis is structured as follows: <ul style="list-style-type: none"> - meeting with the Management for data collection related to the training needs necessary to achieve the company objectives; - interview with the managers for the detection of specific training needs of their areas; - return of the data collected to the Company Management for the closure and approval of the Formative Plan. By the end of February the Training Plan as defined is shared and made public.

cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence
				ROLES & REPONSABILITIES: There is a document that specifies the division of roles and responsibilities between Intesa San Paolo and InfoCert: “Roles and responsibilities - Intesa Sanpaolo Organization Validation CA” “ISP-CBCM-003-2018-01” version 01 of 01/12/2018. This document includes, among other figures, the Validation Specialist: the responsible for checking the accuracy and authenticity of the information provided by the applicant ensuring and that all documents and contractual clauses adopted are legitimate. The Validation Specialist is one or more persons belonging to an InfoCert team. Evidences of courses attended by the Validation Specialists: <ul style="list-style-type: none"> - “SignaCert Seminar of 21/02/2018” - “Course on the vetting of PSD2 certificates of 22/11/2018”
	(c) Sufficient financial resources and/or liability insurance, in accordance with national law;		7.1 Internal Organization	Comment: Intesa San Paolo has financial resources, as to cover liabilities This is an aspect that falls within the risk scenarios as well as in the insurance plan of Intesa San Paolo Evidence as follows: - “Risk Analysis - Organization Validation SSL Certificates” version 01 of 08/11/2018

cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence
	(d) Consumer information on terms and conditions, incl. limitations on use;		6.2 Terms and Conditions	Comment: The General Conditions of Service are defined within the "service contracts" entered into the companies of the Intesa Sanpaolo Group. The services of issuing, revocation of certificates and publication of the CRL has been delegated to Infocert S.p.A. through regular service contract. The supplier therefore has the role of managing the sub-CA and as such has the obligation to act in compliance with the legislation in force in the field of digital certificates (EU Regulation No. 910/2014 and Legislative Decree 82/2005 and subsequent amendments).
	(e) use trustworthy systems and products;		7.3 Asset management 7.4 Access control 7.5 Cryptographic controls 7.6 Physical and environmental security 7.7 Operation security 7.8 Network security	Comment: Intesa San Paolo complies with this requirement according to the ISO 27001: 2013 certificate. Obviously also the outsourcer (InfoCert) is certified ISO / IEC 27001: 2005 since March 2011 for EA activities: 33-35. In March 2015 it was certified for the new version of the ISO / IEC 27001: 2013 standard. In the ISMS there are, among others, procedures about the Asset Management; other evidences can be found in the "Certificate Policy – Certificate Practice Statement Intesa Sanpaolo Organization Validation CA "ISP-CBCM-002-2018-01.2" version 01.2 of 01.28/11/2018: § 7.2.1 Controls and standards of the cryptographic module § 6 Safety Measures and controls § 7.6 Operation on control systems § 7 Network security checks
	(f) use trustworthy systems to store (personal) data;			Comment: The organization physical security is compliant Evidence: "Certificate Policy –Certificate Practice Statement Intesa Sanpaolo

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/14
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page 27 of 36	

cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence
	(g) take appropriate measures against forgery and theft of data;			Organization Validation CA “ISP-CBCM-002-2018-01.2” version 01.2 of 01.28/11/2018: § 6.1 Physical Safety Checks
	(h) Record and keep accessible activities related data, issued and received, even after cessation;		7.10 Collection of evidence	Comment: The organization is compliant. The events related to the management of the CA and the life of the certificate are collected, by the supplier, in the control journal as foreseen by the Regulation (Eidas) and by the technical rules (see Technical rules on the generation, affixing and verification of signatures advanced, qualified and digital electronics certificate). Evidence: § 6.4 “Logging Procedures” of the CPS
	(i) Up-to-date termination plan (to be agreed with SB) to ensure continuity of service;		7.12 TSP Termination and termination plans	Comment: The organization is compliant. In case of termination of the Certification Authority, Intesa Sanpaolo will communicate this intention to the Supervisory Authority (AgID) with an advance of at least 60 days, indicating, where appropriate, the new Certification Authority, the depositary of the certificate register and the related documentation. With equal advance notice, Intesa Sanpaolo informs all the holders of certificates issued by Intesa Sanpaolo CA of the cessation of business. In the communication, if a replacement certification is not indicated, it will be clearly specified that all the certificates not yet expired at the time of the termination of the CA's activities will be revoked. Similarly, InfoCert, in the event of termination of the certification activity, will communicate the same intention to Intesa Sanpaolo and the Supervisory Authority (AgID) with an advance of at least 60 days, indicating, where appropriate, the new Certification Authority, the custodian of the register certificates and related documentation.

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/14
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page 28 of 36	

cod	Title	Description	Rif ETSI EN 319 401	Comment/ Evidence
				Evidence: : <ul style="list-style-type: none"> - § 6.8 “Termination of the CA” of the CPS - Termination Plan “Termination of digital certification services” “ISP - CBCM - 003 - 2018 – 02” version 02 of 16/10/2018
	(j) Ensure lawful processing of personal data in accordance with Directive 95/46/EC.		7.13 Compliance	Comment: The organization is aware of the actual data protection laws in Italy dlgs 196/2003 and had implemented the compliance new GDPR.

5.4 Specific requirements for the applicable type of qualified trust.

Assessed trust service	Specific requirements eIDAS	EU qualified certificate policy reference: ETSI EN 319 411-1	Comment / Evidence
Organization Validation certificate for Web Authentication	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	Comment: At operating level Intesa San paolo manages the life cycle of web server certificates through a platform called "RCD". Through this platform, enabled users can request the web server certificates. Evidence: internal operating guide: “ICT Management and IT Security - Enterprise Security - Data Security” version of 28/09/2018. InfoCert is the technological outsourcer for the Sub CA “Intesa Sanpaolo Organization Validation CA” and also provides for the registration of new domains, including those for which it is possible to request an SSL / web certificate through the RCD platform.

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/14
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page 29 of 36	

Qualified trust service	Specific requirements eIDAS	EU qualified certificate policy reference: ETSI EN 319 411-1	Comment / Evidence
	<p>2. Art.24.2.k)</p> <p>3. Art.24.3</p> <p>4. Art.24.4</p> <p>5. Art.45 – Annex IV</p>	<p>2. ETSI EN 319 411-1, clause 6.1 Publication and repository responsibilities</p> <p>3. ETSI EN 319 411-1, clause 6.2.4 Identification and authentication for revocation requests</p> <p>4. ETSI EN 319 411-1 [2], clause 6.3.10 Certificate Status Services. The requirements shall apply. In addition the following particular requirements apply: NOTE 1: Regulation (EU) No 910/2014 [i.1] requires this service to be provided free of charge.</p> <p>5. ETSI EN 319 411-1 clause 6.6.1 i) and ii) Certificate profile</p>	<p>§ 5.5.2 of the CPS “Publication of certificates by the CA” The CA only publishes certificates for the Certification keys.</p> <p>The revocation requests could be invoked for the reasons provided in the paragraph 5.10.1 of the CPS using the methods described at paragraphs 5.10.3 of the CPS. Intesa San Paolo provides two mechanisms for certificate status validation. In fact, in addition to the publication of the CRL in the LDAP and http registers, the supplier also provides an OCSP service for verifying the status of the certificate. The service URL is indicated on the certificate. The service is available 24 X 7.</p> <p>Evidence: § 5.10.9 “Online services for checking the status of revocation of the Certificate” of the CPS</p> <p>1. Services related to the certificate status, defined in CPS § 5.10.9, are delivered free of charge.</p> <p>2. The certificate profiles are according to RFC 5280. Test Certificates were provided and reviewed.</p>

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
(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	5-12-2018	SM	[ETSI 319 411-1 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>ENG: 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>
2	5-12-2018	NC_I	[ETSI 319 401] Clause 7.13 [ETSI 319 411-1] Clause 6.7	ITA: Tra Settembre e ottobre 2017 sono stati rilasciati 136 certificati errati che sono stati tutti revocati e sostituiti ma per alcuni di questi non sono stati comunicati con immediatezza gli incident report agli organismi competenti (es. Mozilla)

CSQA Certificazioni Srl Via s. Gaetano, 74 - 36016 Thiene (Vi) Tel. 0445 313011 - Fax 0445 313070 csqa@csqa.it www.csqa.it		SCHEME: eIDAS	Procedure: 174015/14
		FORM: RVETSP_ST2	REV. 3 – March, 24th 2016
		Page 31 of 36	

Observation no.	Date	Type of Observation	Regulation requirement	Auditor's observation
				ENG: Between September and October 2017 were issued 136 misissued certificates that were all revoked and issued, but for some of these the incident reports were not immediately communicated to the competent bodies (eg Mozilla)
3	5-12-2018	NC_I	Common CCADB Policy Clause 5. Policies, Practices and Audit Information [ETSI 319 411-1] Clause 7.1, OVR-7.1-07	<p>ITA: La CA deve fornire la versione in lingua inglese di qualsiasi policy, CPS e documenti di Audit che non sono originariamente in inglese, con numeri di versione corrispondenti al documento al documento tradotto. Si raccomanda di tradurre il CPS in inglese il prima possibile, nell'ottica che il TPS dovrebbe rendere disponibile il CPS alla sua comunità di utenti.</p> <p>EN: CAs must provide English versions of any Certificate Policy, Certification Practice Statement and Audit documents which are not originally in English, with version numbers matching the document they are a translation of.</p> <p>It is recommended to translate the CPS in English as soon as possible in the perspective that the TSP should make the CPS available to its user community</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 **INTESASanPaolo 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.**

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

Identification of the audited Root-CA:	Intesa Sanpaolo Organization Validation CA http://cert.intesasanpaolo.com/ovcf/CA.crt	
	Distinguished Name	CN = Intesa Sanpaolo Organization Validation CA OU = WSA Trust Service Provider O = Intesa Sanpaolo S.p.A. C = IT
	SHA-256 fingerprint	27cdd699de15ee88a05bb10ed9df2fc5e4ca25b5fdd42988963a38ec8940d55a
	Certificate Serial number	07d9b184e4f04310
	Applied Policy	Intesa San Paolo policy for OV certificates (1.3.6.1.4.1.20052.3.1.1) 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)

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.

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

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.

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

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 6-12-2018	<div style="text-align: center;">  <hr style="width: 80%; margin: 0 auto;"/> Signature of the Audit Group Manager(*) </div>
(*) 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.	

6-12-2018	
<div style="text-align: center;"> <hr style="width: 80%; margin: 0 auto;"/> Date </div>	<div style="text-align: center;"> <hr style="width: 80%; margin: 0 auto;"/> Signature of the Organization (*) </div>
(*) The signature of the Organization certifies that: <ul style="list-style-type: none"> The Organization is in possession of this report The Organization confirms that the data concerning the identification of your Organization and the definition of the application scope are correct. The organization has been informed that CSQA regulations applicable to this report are available and can be consulted in the website http://www.csqa.it. 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. The organization does not have criminal proceedings or other significant legal situations (e.g.: injunctions, revocation of authorizations) to communicate to CSQA. 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. CSQA Certificazioni Srl commits itself to protect the confidentiality of the information acquired during this audit. 	