Digical Operating Manual
International Subsidiary Bank Division

Distribution:	PUBLIC								
Document code:	ISP	-	SCD	-	04	-	2022	-	06
	Company		*Service*		*Code*		*Year*		*Version*

VERSIONS OF THE REMOTE DIGITAL SIGNATURE OPERATING MANUAL

Version	Date of issue	Description of change
01	01/12/2018	First version
02	02/07/2019	Annual review
03	31/10/2019	Review
04	30/11/2019	Document update following replacement of the 45 AgID resolution
05	31/05/2020	Document update following the creation of Business Continuity CA
06	30/06/2022	Update after AgID Inspection

CONTENTS

Versions of the Remote Digital signature operating manual 2
Contents 3
1. General Information 6
1.1 Overview 6
1.2 Definitions and interpretation 6
1.2.1 References to legal provisions 7
1.3 References to standards 7
1.4 Abbreviations 8
2. Introduction 10
2.1 Identification details of the Certification Authority 10
2.2 Remote Digital Signature Operating Manual Identification 10
2.3 Person responsible for this Remote Digital Signature Operating Manual 11
3. General provisions 12
3.1 Obligations of the Registration Authority, the Certification Authority and the Holder 12
3.1.1 Obligations of the Certification Authority and the Registration Authority 12
3.1.2 Obligations of the Holder 12
3.1.3 Obligations of the Legal Entity (if applicable) 13
3.1.4 Obligations of the entity required to verify the signature 13
3.2 Limitation of liability and indemnification 13
3.2.1 Limitation of liability 13
3.2.2 Indemnification 14
3.3 Availability Hours 14
4. Operational Aspects 15
4.1 Content of qualified certificates for electronic signature 15
4.2 Personnel organisation rules 15
4.3 Key generation procedure 15
4.3.1 Certification key generation procedure 16
4.3.2 Time stamp key generation procedure 16
4.4 User identification and registration procedure 16
4.4.1 User identification and registration 16
4.4.2 Individuals Activation of the Remote Digital Signature service and signing of the relevant contract 17

4.4.3 Legal-Entity User Activation of the Remote Digital Signature service and signing of the relevant contract 18
4.4.4 Issuance of qualified certificates for electronic signature....19
4.5 Qualified electronic signature revocation certificate procedure....19
4.5.1 Request for revocation submitted by the Holder....19
4.5.2 Request for revocation submitted by the Legal Entity....20
4.5.3 Revocation submitted by the Certification Authority or by the Registration Authority 20
4.5.4 Completion of the qualified certificate for electronic signature revocation procedure 20
4.6 Qualified certificate for electronic signature suspension procedure....21
4.7 Procedure for PIN and OTP (TOKEN) device loss....21
4.8 Keys replacement procedure....21
4.8.1 Replacement of Holders' signature keys....21
4.8.2 Replacement of certification keys....21
4.9 Management of the qualified certificated for electronic signature directory....21
4.9.1 Qualified certificates for electronic signature directory....21
4.9.2 Publication of qualified certificates for electronic signature and CRL....22
4.9.3 Reproduction of the qualified certificates for electronic signature directory on different websites....22
4.10 Personal data protection procedures....22
4.11 Procedure for organising the control log....23
4.12 Backup copy management procedure....23
4.12.1 Backup procedure....23
4.13 Procedure for managing accidents and catastrophic events....23
4.13.1 Computer failures....24
4.13.2 Software impairments....24
4.13.3 Failure of the Certification Authority's signature device....24
4.13.4 Certification key impairments....24
4.13.5 Main site compromise....24
5. Cessation of qualified certificate for electronic signature service....25
5.1 Details of the cessation of qualified certificate for electronic signature service....25
6. Management of time references....26
6.1 Timestamp service....26
6.2 Accuracy of the time reference....26

7. Digital Signature Verification Process 27
7.1 Verification application 27
7.2 Documents format 27
7.3 Warnings on CRL consultation 27
8. Operating Procedure for Generating Digital Signatures 28

1. GENERAL INFORMATION

1.1 Overview

This "Remote Digital Signature Operating Manual" (as defined below) is aimed at regulating the qualified certificates for electronic signature services provided - in accordance with the Legislative Decree 82/2005 (Digital Administration Code), as subsequently amended, and the national and European applicable laws and regulations - by Intesa Sanpaolo S.p.A. to the User (as defined below) of International Subsidiary Bank (as defined below) in connection with the multichannel services (i.e. access by the User to the services provided by the International Subsidiary Banks through remote channels and branch).
This Remote Digital Signature Operating Manual refers also to the technical rules for the implementation of the legal framework on digital signature contained in the DPCM 22/02/2013. Should any change of law occur, this RDS Operating Manual shall be modified accordingly.

1.2 Definitions and interpretation

The following terms used in this Remote Digital Signature Operating Manual shall have the below meanings:

- **"Applicant**": the person requesting the issuance of a qualified certificate for electronic signature; for Individuals the Applicant is the same as the Holder; for Legal Entity, Applicant is always a legal representative of Legal entity (there could be more than one Legal Representative for Legal Entity);
- "**Branch**": a location where business between the client and the Bank is conducted, this include all the premises, offices and locations of the International Subsidiary Bank
- "**Certification Authority**": the trust service provider, which is authorised to issue qualified certificates for electronic signature through a certification procedure that is compliant with international standards and European and national laws and regulations. For the purposes of this RDS Operating Manual, the Certification Authority is Intesa Sanpaolo S.p.A.
- **"Legal Entity":** non-consumer, i.e. a public or private company or a natural person operating within his/her line of business or as a self-employed professional, which signs the Digital Banking Service Usage Agreement with an International Subsidiary Banks and authorizes an Applicant/Holder to use the qualified certificate for electronic signature issued on its behalf;
- **"User**": the Individual or Legal Entity end-user, signatory of Agreement on Provision of Certification services concluded with International Subsidiary Banks;
- **"Digital Acquisition"**: a channel to perform a digital acquisition process through a video identification executed by the bank operator and an ID document provided by the client;
- **"International Subsidiary Banks"**: any International Subsidiary Bank belonging to Intesa Sanpaolo group;
- **"Holder**": the User to whom a qualified certificate for electronic signature has been issued; the Holder is authorised to use such certificate to digitally sign electronic documents, while ensuring the authenticity of the origin of such electronic documents and the integrity of its content, pursuant to the limitations specified in the Agreement on Provision of Certification services of International Subsidiary Banks;
- **"Intesa Sanpaolo"**: Intesa Sanpaolo S.p.A., the provider of qualified certificates for electronic signature;
- **"One Time Password (OTP)":** password valid for one transaction only and generated and make at disposal of the Holder just immediately before the digital signature operation. The OTP is sent via sms to the client if the channels are digital acquisition or branch. The OTP is generated by TOKEN on remote digital banking services**;**
- **"Registration Authority**": the entity appointed mainly to (i) identify the Applicants and conclude the contract with Applicants, guaranteeing the accuracy of their identity, (ii) provide the Applicants with all information on the qualified certificates for electronic signature and restrictions on their use, (iii) conclude the contract with Applicants in the name and on behalf of Intesa Sanpaolo and (iv) submit to Intesa Sanpaolo the revocation and suspensions requests for such certificates. For the purposes of this RDS Operating Manual, the Registration Authority is any of the International Subsidiary Banks of Intesa Sanpaolo S.p.A. that executed with Intesa Sanpaolo S.p.A. an agreement on qualified certificates for electronic signature;

- **"Remote Digital Signature (RDS) Operating Manual"**: this document as subsequently amended and supplemented.
- **"Bank"**: any International Subsidiary Bank belonging to Intesa Sanpaolo group
- **"TOKEN"**: Secure authentication systems ensure strong customer authentication (SCA); it is used to generate OTP (One Time Password) after PIN verification
- **"Private Key":** means the reserved element of a pair of Asymmetric Keys saved in a protected manner by the Certification Services Provider on an appropriate signature device.
- **"Public Key":** means the element of a pair of Asymmetric Keys with which authentication of the electronic signature is conducted.

1.2.1 References to legal provisions

[Dlgs 82/2005]	Legislative Decree no. 82 of 7 March 2005, published in the Official Gazette no. 112 of 16 May 2005, - Ordinary Supplement no. 93 "Digital Administration Code" updated by Legislative Decree no. 217 of 13 December 2017 published in Official Gazette no. 9 January of 2018.
[DPCM]	Prime Minister's Decree of 22 February 2013 - Technical rules on the creation, application and verification of advanced, qualified and digital electronic signatures pursuant to art. 20 (3), 24 (4), 28 (3), 32 (3) letter b), 35 (2), 36 (2), and 71.
[CNIPA/CR/48]	CNIPA/CR/ 48 Circular no. 48 of 6 September 2005 (published in Official Gazette no. 213 of 13 September 2005), Procedure for submitting an application to be entered in the public list of certification-service providers pursuant to art. 28 (1) of Presidential Decree no. 445 of 28 December 2000.
EU Regulation 910/2014 – eIDAS	Regulation (EU) N. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
EU Regulation (EU) N°679/2016 – GDPR	Regulation (EU) N°679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
AgID Deliberation n.121/2019	Guidelines containing the Technical Rules and Recommendations concerning the generation of qualified electronic certificates, qualified electronic signatures and seals and qualified electronic time validations

1.3 References to standards

[LDAP2] Zeilenga, "Lightweight Directory Access Protocol version 2", Internet RFC 3494, March 2003.
[PKCS7] B. Kaliski, "PKCS#7: Cryptographic Message Syntax Version 1.5", Internet RFC 2315, March 1998.
[PKCS10] B. Kaliski, "PKCS#10: Certification Request Syntax - Version 1.7", Internet RFC 2986, November 2000.
[SHA1] ISO/IEC 10118-3:2018, "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions", 2018.

[SHA-256] ISO/IEC 10118-3:2018, "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions".
[X500] ISO/IEC 9594-1:2008, ISO/IEC 9594-2:2008 “Information technology — Open Systems Interconnection — The Directory: Overview of concepts, models and services”.
[X509] ISO/IEC 9594-8:2008 “Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks”.
[RFC3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu.
[RFC 3778] The application PDF Taft, Pravetz, Zilles, Masinter, May 2004.

1.4 Abbreviations

The following terms used in this Remote Digital Signature Operating Manual shall be abbreviated as follows:

AgID The Agency for Digital Italy,

CRL Certificate Revocation List

CPS Certificate Practice Statement

DBMS Database Management System

DN Distinguished Name

DNS Domain Name System

DPR Presidential Decree

HSM Hardware Security Module

HTTP HyperText Transfer Protocol

ITSEC Information Technology Security Evaluation Criteria

LDAP Lightweight Directory Access Protocol

NEI National Electrotechnical Institute "Galileo Ferraris" (in Italian “Istituto Elettrotecnico Nazionale”)

OTP One Time Password

PDF Portable Document Format

PIN Personal Identification Number

PKCS Public Key Cryptography Standard

RDS Remote Digital Signature

RFC Request For Comments

RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Function 1
SHA-2	Secure Hash Function 2
SSL	Secure Sockets Layer
URL	Uniform Resource Locator

2. INTRODUCTION

The digital signature is based on asymmetric keys, one public and one private, which ensure the authenticity of the origin of the electronic documents digitally signed and the integrity of their content to one or more recipients that can, in turn, verify the relevant validity.

The new provisions introduced by art. 8 of [DPCM] allow a Certification Authority to store the private keys of the Holders (i.e. the keys used to create a digital signature) on special security devices (i.e. HSM), while ensuring that the use of the keys shall be exclusively granted to the Holder, as specified in art. 11 (2) [DPCM].

As a consequence, the use of the digital signature is no longer subject to the Holders' possession of digital signature kits (e.g. smartcard, special reader and relevant software), and the certification and registration authorities can provide digital signature services to the User through direct channels (i.e. web, mobile).

The Holder may initiate a digital signature process through the use of an OTP (either received on a Certified mobile number or, on Remote Banking Service, generated by TOKEN inserting a PIN), while sole control of the Holder is guaranteed. The beginning of the process, if performed at the Branch, may also happen through a card reader (i.e. the Holder may be able to perform the first step by scanning his debit card with a card reader at the Branch).

In this Remote Digital Signature Operating Manual the following processes shall be explained:

- signature key generation and management procedures within Remote Digital Signature service offered by Intesa Sanpaolo;
  - the Remote Digital Signature activation procedure and the Strong Authentication mechanism within the digital bank on the basis of the authentication procedure defined by the International Subsidiary Banks
- the role of both the Certification Authority and Registration Authority, compliant with the applicable laws and regulations;

The RDS Operating Manual refers to all the Intesa Sanpaolo International Banks in scope of the International Subsidiary Bank Division.

The following paragraphs refer to the requirements stemming from art. 40 (3) a, b and c of [DPCM].

2.1 Identification details of the Certification Authority

The certification service is provided by the entity identified below:

Name:	**Intesa Sanpaolo S.p.A.**
Registered office:	**Piazza San Carlo, 156 10121 Turin**
Legal Representative:	**Carlo Messina, Managing Director and CEO**
Registration no. at the Turin Company Register:	**Economic Administrative Register (REA) no. 00799960158**
VAT No.:	**10810700152**
Telephone no. (switchboard):	(+39) 011 555 1
ISO Object Identifier (OID):	**1.3.6.1.4.1.20052**
General website (information):	**www.intesasanpaolo.com**
Digital certification service website:	**ca.intesasanpaolo.com**

2.2 Remote Digital Signature Operating Manual Identification

This Remote Digital Signature Operating Manual is identified by document code ISP-SCD-04-2022-06 (also shown on the title page)and it refers to certificates with the following OID: 1.3.6.1.4.1.20052.1.3.1 and 1.3.6.1.4.1.20052.1.4.3.

This Remote Digital Signature Operating Manual is published on the website of the Certification Authority and is therefore available online.

The current version of this Remote Digital Signature Operating Manual is available in electronic format:

- on the Certification Authority's website (https://ca.intesasanpaolo.com/);
- on the AgID website;
- on the Internet Banking web site of the International Subsidiary Banks Division

In case of discrepancies, the version published on the AgID website shall all the time prevail.

2.3 Person responsible for this Remote Digital Signature Operating Manual

Action	Nominative	Function
Editing	Office: Infrastructure, Network, Info-physical and Data Protection Solutions	Cybersecurity and Business Continuity Management
Approval	Giorgio Cusmà Lorenzo	Responsible: Cybersecurity and Business Continuity Strategy and Group Governance

3. GENERAL PROVISIONS

3.1 Obligations of the Registration Authority, the Certification Authority and the Holder

3.1.1 Obligations of the Certification Authority and the Registration Authority

The Certification Authority shall act in compliance with the provisions set out in [DLgs 82/2005], art. 32, adopting all organisational and technical measures to prevent any damage to third parties.

The Certification Authority issuing, in accordance with art. 27 of [DLgs 82/2005], qualified certificates for electronic signature shall also be required:

- to properly identify the Applicant (and the Holder if different); such activity shall be performed by the Registration Authority in accordance with national law;
- to clearly and completely inform the Applicants (and the Holder if different) about the features of the qualified certificates for electronic signature and the restrictions on the use thereof; such activity shall be performed by the Registration Authority before concluding the Agreement on Provision of Certification services contract;
- to proceed, on the basis of the instructions promptly provided by the Registration Authority, with the timely revocation of qualified certificates for electronic signature and with the relevant publication;
- to adopt security measures for processing personal data of the User, in compliance with the applicable laws and regulations; this obligation shall be performed by both the Registration Authority and the Certification Authority;
- to issue the qualified certificates for electronic signature as prescribed by [DPCM], in compliance with [GDPR Regulation], as subsequently amended and supplemented;
- to comply with the technical rules set out in [DPCM] and in art. 71 of DLgs 82/2005;
- to ensure that the secure device for the signatures generation has the characteristics and safety requirements prescribed under art. 35 of [DLgs 82/2005] and art. 11 of [DPCM];
- to store records, also in electronic form, of all information concerning qualified certificates for electronic signature for at least 20 (twenty) years, in order to be able to provide evidence of the certification within any eventual judicial action;
- to store records, also in electronic form, of all documents signed by the Holder during the qualified certificates for electronic signature issuance procedure for at least 20 (twenty); this activity shall be performed by the Registration Authority;
- not to export the private keys of the Holders from the HSM, where such keys have been generated and are utilised;
- Certification Authority and Registration Authority shall also keep this Remote Digital Signature Operating Manual constantly updated and, Registration Authority promptly will inform User of changes applied.

3.1.2 Obligations of the Holder

The Holder is required to ensure the safekeeping of all information enabling the use of the private key and to adopt all technical and organisational measures to prevent any damage to third parties; the Holder is also required to personally use the data enabling the creation of the digital signature (art. 8 (5) of [DPCM]).

The Holder shall comply with [DPCM]; in particular, the Holder shall be required:

- to request the qualified certificates for electronic signature according to the procedures set out in this RDS Operating Manual;
- to safeguard the codes (code generated by TOKEN and sms OTP) necessary to use the qualified certificates for electronic signature

- to request for revocation of the qualified certificates for electronic signature according to the procedures set out in this RDS Operating Manual;
- to promptly notify the Registration Authority of any changes in the information provided to the Registration Authority during the registration procedure (personal data, addresses, etc.);
- to not use the private key for purposes other than those indicated in the limitations of use defined in the qualified certificates for electronic signature in the Digital Banking Service Usage Agreement and Agreement on Provision of Certification services;
- to provide the correctness, truthfulness and completeness of the information to the person making the identification, for the certificate request;
- to use the certificate only for the methods set out in this Operating Manual and by current national and international laws.

3.1.3 Obligations of the Legal Entity (if applicable)

In case the Holder is using a qualified certificate for electronic signature on behalf of Legal Entity, the same Legal Entity will be part of the obligations and will have to provide proper authorization for the Holder to use the qualified certificate for electronic signature on its behalf.

The Legal Entity shall comply with [DPCM]; in particular, the Legal Entity shall be required:

- to authorize the request of the Holder to have the qualified certificate for electronic signature according to the procedures set out in this RDS Operating Manual;
- to request for revocation of the qualified certificate for electronic signature according to the procedures set out in this RDS Operating Manual;
- to promptly notify the Registration Authority of any changes in the information provided to the Registration Authority during the registration procedure (Holder's personal data, Holder's death, Holder's loss of business ability, Legal Entity's data, etc.);
- to use the certificate only for the methods set out in this Operating Manual and by current national and international laws.

3.1.4 Obligations of the entity required to verify the signature

The entities in charge of verify the electronic signature generated by certification keys by Intesa Sanpaolo, shall be required:

- to verify the certificate's validity period (in accordance with the current regulation);
- to check through the list of revoked qualified certificates for electronic signature if the certificate was revoked in the signature moment;
- to ensure that the electronic signature refers to a qualified certificate issued by a Certification Authority previously approved by AgID in the signature moment;
- to ensure that the generated "subscription" keys typology (as prescribed by [DPCM], Art.5, comma 4, letter a) and the certificate's extension keyUsage 11 (OID: 2.3.29.15) have only the non Repudiation value (bit 1 sets on 1);
- to verify the restrictions on use specified in the qualified certificate.

3.2 Limitation of liability and indemnification

3.2.1 Limitation of liability

Intesa Sanpaolo shall not be liable for any disruptions resulting from any failure of the Holder to comply with the applicable laws and regulations, as well as with technical/operating specifications contained in the Digital Banking

Service Usage Agreement of Banks entered into by and between the Holder and the relevant Bank or in any document referred to thereto.

Intesa Sanpaolo shall not be liable for any damages resulting from any use exceeding the limits specified in the qualified certificates for electronic signature and/or in the Digital Banking Service Usage Agreement of Bank and/or Agreement on Provision of Certification services.

The limitations on use specified in the qualified certificates for electronic signature are the following:

Intesa Sanpaolo Qualified Electronic Signature CA 2:

"Uso limitato a documenti relativi a rapporti tra Titolare e società del Gruppo Intesa Sanpaolo o altri soggetti extra Gruppo che offrono i loro servizi sui sistemi informatici delle società del Gruppo

Use limited to documents regarding Certificate-holder's relations with Intesa Sanpaolo Group companies or other persons outside the Group offering their services on Group companies' electronic systems"

CA Intesa Sanpaolo S.p.A. Firma Qualificata:

"Uso limitato a documenti relativi a rapporti tra Titolare e società del Gruppo Intesa Sanpaolo o altri soggetti extra Gruppo che offrono i loro servizi sui sistemi informatici delle società del Gruppo

Use limited to documents regarding Certificate-holder's relations with Intesa Sanpaolo Group companies or other persons outside the Group offering their services on Group companies' electronic systems"

In addition, use of qualified certificates for electronic signature shall be limited to the domain specified in the Agreement on Provision of Certification services.

Further restrictions specific to a single product or a national law will be treated in Operating Manuals dedicated to the specific product.

3.2.2 Indemnification

As detailed in art. 3.2.1 above Intesa Sanpaolo shall not be liable for any damages deriving from any inappropriate use of the qualified certificates for electronic signature.

However, pursuant to art. 15 (1) i) of [DPCM], Intesa Sanpaolo has stipulated a specific insurance to cover the relevant risks and any damages arising out of or in connection with the issuance of the qualified certificates for electronic signature.

3.3 Availability Hours

services offered by the Certification Authority (the issuance of the qualified certificates for electronic signature and the usage of electronic signature) are available via direct channels (web and mobile) and branch. The revocation of the qualified certificates for electronic signature is available via branch.

4. OPERATIONAL ASPECTS

4.1 Content of qualified certificates for electronic signature

The content of the qualified certificates for electronic signature issued by Intesa Sanpaolo complies with the provisions set out in art. 28 of [Dlgs 82/2005]
to the specification ITU-T X.509 v3 (ISO/IEC 9594-8:2005), and to the European Rules ETSI EN 319 411 ed ETSI EN 319 412 (where appicable).
Referring to the AgID Deliberation N 121/2019 it is specified that the qualified certificates are issued by Intesa Sanpaolo according to the recommendations referred to in chapter 4 of the aforementioned provision, with the exception of the following fields:

- SubjectDN: serialNumber (OID 2.5.4.5): a unique code associated with the holder is used using a naming convention different from that indicated in the recommendations referred to in chapter 4 of the N 121/2019 AgID Determination
- SubjectDN: organizationName (OID 2.5.4.10): if the owner is a simple customer of the organization, the organizationName field is still used, but enhanced with the string "not present".

As all the N 121/2019determination recommendations are not implemented, the certificates issued by Intesa Sanpaolo do not contain the coding, in the CertificatePolicies field (OID 2.5.29.32),in a PolicyIdentifier element with AgID value (OID 1.3.76.16.6).The qualified certificates for electronic signature shall not be published in publicly available registers.
The validity period of each qualified certificate for electronic signature is 3 (three) years.

The Remote Digital Signature authorizes the Holder and the Legal Entity (if applicable) to enter into a contract with the Bank. The remote digital signature can be used through all the channels (including the digital channels: digital branch, on-line banking and digital acquisition) according to the Bank's timely offer and possibilities
A qualified certificate for electronic signature is required to allow the Holder to use the Remote Digital Signature.

4.2 Personnel organisation rules

The personnel responsible for the provision and control of the certification service is organised pursuant to [DPCM 2013] meaning that, *inter alia*, responsibility roles are foreseen, as laid down in art. 38 of [DPCM].

During the performance of their duties, the personnel holding responsibility roles may avail themselves of employees and operators, also belonging to the Banks.

Regarding the RDS Operating Manual, the operators perform the certification service (here having a meaning of registration or identification of the Holder) at the Banks' branches, outside the data processing centre of Intesa Sanpaolo; the exchange of information between such operators and Intesa Sanpaolo is made through secure communication channels.
The registration activity is carried out by the Banks based on a specific contract entered into by and between the respective Bank and Intesa Sanpaolo.
The Banks' operators perform the registration activity in accordance with the procedures agreed between the Banks and Intesa Sanpaolo and are performed through a compliant procedure.

4.3 Key generation procedure

Each type of key listed in art. 5 of [DPCM] are generated, stored and used within the secure devices, which are compliant with the security requirements set out in the applicable laws and regulations.

The keys have the characteristics laid down in [DPCM].

4.3.1 Certification key[1] generation procedure

The generation of the certification keys is performed in compliance with the applicable laws and regulations, and in particular:

- the certification keys are generated by employees expressly appointed by the Certification Authority;
- a specific qualified certificate for electronic signature is generated for each pair of certification keys, as set forth in the paragraph 4.1, signed with the corresponding private key of the pair, which is sent to AgID in accordance with the procedures agreed beforehand between the Certification Authority and AgID.

4.3.2 Time stamp key generation procedure

As regards the time stamp service connected to the digital signature services provided to the Banks, Intesa Sanpaolo uses a certification authority that meets the necessary requirements to provide services in the country where the relevant Bank is located.

4.4 User identification and registration procedure

The issuance of the qualified certificates for electronic signature is valid only for those who qualified as User, namely someone that enter into Agreement on Provision of Certification services with Bank .

Individual User's qualified certificates for electronic signature contain personal information about the Holder.
Legal Entity End User's qualified certificates for electronic signature could contain both personal information about the Holder as well as information about the Legal Entity.

The User’s identification and registration procedures are carried out by the relevant Bank in accordance with the applicable laws and regulations, including but not limited to the anti-money laundering regulation, which shall be observed at the time of entering into a contractual relationship with the same.
For Legal Entities, anti-money laundering regulation is applicable to the Legal Entity and not to the Holder. In this case, the Holder identification is performed face-to-face.

The identification of Holder and/or Applicant will be carried out either (i) in person, by way of physical presence of the User at the premises of the Bank, or (ii) remotely, by way of using identification methods that are recognised as providing equivalent assurance in terms of reliability. These activities are performed through an AML compliant procedure or face-to-face procedure, which means also taking into account Article 24 1.(d) of Eidas Regulation.

4.4.1 User identification and registration

User is identified through predefined procedures that differ depending on the channel of the digital bank.
The identification of the User is performed either through a physical presence or via remote. In particular:

- During the identification in person at the Digital Branch, a mobile number provided by the User is certified by sending OTP via sms to it and asking User to provide it. The User may also be identified by scanning his debit card on the card reader;
- During the online identification at Remote Digital Banking Services, the User authenticates on Mobile/Responsive with Login ID and OTP generated by inserting the PIN on his/her TOKEN in according to Digital Banking Service and additional OTP that the User receives via sms on his certified mobile number;

[1] Keys used by the Certification Authority to issue qualified certificate for electronic signatures, upon Holders’ requests.

- During the video identification for the Digital Acquisition, a mobile number provided by the User is certified by sending OTP via sms to it and asking User to provide it.

All the identification procedures are performed following the local Banking regulation and through an AML compliant procedure or face-to-face procedure.
The identification of the User is performed by the relevant Bank before qualified certificate for electronic signature enrollment.
Upon successfully identification, User is able to proceed with activation of the Remote Digital Signature service and signing of the relevant contract

4.4.2 Individuals Activation of the Remote Digital Signature service and signing of the relevant contract

In order to activate a remote digital signature and sign the Agreement on Provision of Certification services, the Applicant has to fulfil the following procedural steps on different channels.

Remote Digital Banking Services:

- access a Digital Banking Service using the authentication procedures defined by the relevant Bank;
- if required, acknowledge the rules governing the Agreement on Provision of Certification services;
- if required, check and confirm the correctness of his/her personal data with the aim to activate the qualified certificate for electronic signature;
- request the certificate enrolment;
- generate the OTP created by TOKEN inserting a PIN, depending on the Digital Banking Service. This flow guarantees the Strong Authentication mechanism;
- examine the Agreement on Provision of Certification services, enrol the qualified certificates for electronic signature and sign it digitally by entering the OTP generated by TOKEN inserting a PIN;
- additional OTP that the End-user receives via sms on his certified mobile number is requested for supplementary controls;
- the Bank signature confirms the activation of the RDS service.

Branch or Digital Acquisition portal:

- access to Digital Acquisition or go in person at the premises of the Bank;
- if required, acknowledge the rules governing the Agreement on Provision of Certification services;
- if required, check and confirm the correctness of his/her personal data with the aim to activate the qualified certificate for electronic signature;
- request the certificate enrolment. If User requests certificate activation through Digital Branch channel, appropriate application form will be created before Agreement on Provision of Certification services signing;
- receive OTP via sms on his certified mobile number. For the Identification in person and the video identification, the User won't be required to enter the security PIN. At the Branch, the Applicant may also scan his debit card to perform the first step of authorization through the card reader;
- examine the Agreement on Provision of Certification services, enrol the qualified certificates for electronic signature and sign it digitally by entering the OTP. Agreement on Provision of Certification services could also be signed by handwritten signature;
- the Bank signature confirms the activation of the RDS service.

The supporting documentation related to the RDS service will be made available to the User prior to concluding the Agreement on Provision of Certification services related to the digital signature services.

4.4.3 Legal-Entity User Activation of the Remote Digital Signature service and signing of the relevant contract

In order to activate a remote digital signature and sign the Agreement on Provision of Certification services, the Applicant and the Holder have to fulfil the following procedural steps on different channels.
In order to sign the Agreement on Provision of Certification services through Remote Digital Banking Services, the Holder (regardless if is the same of the Applicant or not) has to fulfil the following procedural steps:

- Get the approval of the Legal Entity, if he/she is not the same as the Applicant;
- access a Digital Banking Service using the authentication procedures defined by the relevant Bank;
- acknowledge the rules governing the Agreement on Provision of Certification services;
- if required, check and confirm the correctness of his/her personal data with the aim to activate the qualified certificate for electronic signature;
- request the certificate enrolment;
- generate the OTP created by TOKEN inserting a PIN, depending on the Digital Banking Service. This flow guarantees the Strong Authentication mechanism;
- examine the Certification Service Agreement, enrol the qualified certificates for electronic signature and sign it digitally by entering the OTP generated by TOKEN inserting a PIN;
- additional OTP that the End-user receives via SMS on his certified mobile number is requested for supplementary controls;
- The Bank signature confirms the activation of the RDS service.

In order to sign the Agreement on Provision of Certification services through Remote Digital Banking Services, in case the Applicant is not the same as the Holder, the Applicant has to fulfil the following procedural steps:

- access a Digital Banking Service using the authentication procedures defined by the relevant Bank;
- acknowledge the rules governing the Agreement on Provision of Certification services;
- generate the OTP created by TOKEN inserting a PIN, depending on the Digital Banking Service. This flow guarantees the Strong Authentication mechanism;
- examine the Certification Service Agreement and sign it digitally by entering the OTP generated by TOKEN inserting a PIN;
- additional OTP that the End-user receives via sms on his certified mobile number is requested for supplementary controls.

In order to sign the Agreement on Provision of Certification services in Branch, the Holder (regardless if is the same of the Applicant or not) has to fulfil the following procedural steps:

- get the approval of the Legal Entity, if he/she is not the same as the Applicant;
- go in person at the premises of the Bank;
- acknowledge the rules governing the Agreement on Provision of Certification services;
- if required, check and confirm the correctness of his/her personal data with the aim to activate the qualified certificate for electronic signature;
- request the certificate enrolment;
- examine the Agreement on Provision of Certification services and sign it with digital signature or handwriting signature;
- In case of digital signature:
    - the Holder receive OTP via sms on his certified mobile number. For the Identification in person, the User won't be required to enter the security PIN;
    - the Holder enrols the qualified certificate for electronic signature and sign it digitally by entering the OTP;
- The Bank signature confirms the activation of the RDS service.

In order to sign the Agreement on Provision of Certification services in Branch, in case the Applicant is not the same as the Holder, the Applicant have to fulfil the following procedural steps:

- go in person at the premises of the Bank;
- acknowledge the rules governing the Agreement on Provision of Certification services;
- examine the Agreement on Provision of Certification services and sign it with digital signature or handwriting signature.

The supporting documentation related to the RDS service will be made available to the client prior to concluding the Agreement on Provision of Certification services related to the digital signature services.

In case of handwriting signature of the Agreement on Provision of Certification services in Branch, the enrollment of the qualified certificate for electronic signature could be done online through Digital Banking Service of Bank. In this case, the Holder has to fulfil the following procedural steps to activate the RDS service:

- access a Digital Banking Service using the authentication procedures defined by the relevant Bank;
- if required, check and confirm the correctness of his/her personal data with the aim to activate the qualified certificate for electronic signature;
- generate the OTP created by TOKEN inserting a PIN, depending on the Digital Banking Service. This flow guarantees the Strong Authorization mechanism;
- enrol the qualified certificate for electronic signature by entering the OTP generated by TOKEN inserting a PIN;
- additional OTP that the End-user receives via sms on his certified mobile number is requested for supplementary controls.

4.4.4 Issuance of qualified certificates for electronic signature

The qualified certificates for electronic signature are issued after the finalisation of the key pair generation, as indicated above.

The issuance of qualified certificate for electronic signature procedure is completely transparent to the Applicant who, in this specific phase does not interact with the Certification Authority.

According to applicable legislation, the request for qualified certificate for electronic signature issuance is stored by the Certification Authority for at least 20 (twenty) years from the issuing date of each qualified certificate for electronic signature. In particular, all traces necessary to demonstrate over time the execution of this operation are electronically stored.

4.5 Qualified electronic signature revocation certificate procedure

According to [DPCM] the revocation of a qualified certificate for electronic signature occurs upon the request of the following parties and as indicated below:

- the Holder;
- the Legal Entity;
- the Certification Authority;
- the Registration Authority.

4.5.1 Request for revocation submitted by the Holder

The Holder can submit a request for qualified certificate for electronic signature revocation by going to the branch.

Once the revocation request has been submitted, the automatic mechanism required for the certificate revocation is initiated in a transparent manner with the Holder.

In case of unilateral termination by the Holder of the Agreement on Provision of Certification services of Bank, the Registration Authority shall promptly notify the Certification Authority that shall proceed with the revocation of the relevant certificate for electronic signature.
As a result of the revocation, the Holder can no longer sign any document using the keys previously assigned to him/her, while all documents signed by the Holder prior to the certificate revocation are and remain valid.
As regards the effectiveness of the certificate revocation, such revocation shall be effective starting from the date when the revocation notice is received by the bank.

4.5.2 Request for revocation submitted by the Legal Entity

The Legal Entity can submit via branch a request for qualified certificate for electronic signature revocation of a Holder of a RDS service on behalf of the same Legal Entity.

Once the revocation request has been submitted, the automatic mechanism required for the certificate revocation is initiated in a transparent manner with the Holder.

In case of unilateral termination by the Legal Entity of the Agreement on Provision of Certification services of Bank, the Registration Authority shall promptly notify the Certification Authority that shall proceed with the revocation of the relevant qualified certificate for electronic signature.
As a result of the revocation, the Holder can no longer sign any document using the keys previously assigned to him/her, while all documents signed by the Holder prior to the certificate revocation are and remain valid.
As regards the effectiveness of the certificate revocation, such revocation shall be effective starting from the date when the revocation notice is received by the bank.

4.5.3 Revocation submitted by the Certification Authority or by the Registration Authority

Except in cases of justified urgency, the Certification Authority or the Registration Authority that intends to revoke a qualified certificate for electronic signature shall notify the Holder/the Legal Entity in advance, specifying the reasons of the revocation.

The Registration Authority must promptly notify the Certification Authority about the necessity to revoke a qualified certificate for electronic signature.
The Certification Authority has to revoke the certificate in the following cases:

- when the Holder explicitly requests it;
- when the Legal Entity who the Holder gets the Certificate on behalf of explicitly requests it;
- in case it establishes that the Holder's data are incorrect or incomplete in the Certificate Record;
- in case of receiving an official notice of the Holder's death;
- in case of receiving an official notice of the Holder's loss of business ability;
- in case the Legal entity cease to exist;
- in case of termination of the Agreement on Provision of Certification services;
- in case it determines that the Holder used false data for the issuance of the certificate.

4.5.4 Completion of the qualified certificate for electronic signature revocation procedure

Upon completion of the certificate revocation procedure, a new CRL is created, which is published in the relevant directory available through the internet connection.

CRL is published as indicated in paragraph. 4.9.2. Furthermore, the effective revocation of a qualified certificate for electronic signature is recorded in the control log.

4.6 Qualified certificate for electronic signature suspension procedure

According to [DPCM] the suspension of a qualified certificate for electronic signature occurs upon the request of the following parties and as indicated below:

- the Certification Authority;
- the Registration Authority.

Except in cases of justified urgency, the Certification Authority or the Registration Authority that intends to suspend a qualified certificate for electronic signature shall notify the Holder/the Legal Entity in advance, specifying the reasons of the suspension.

4.7 Procedure for PIN and OTP (TOKEN) device loss

The Holder may have the chance to use, as one of the authentication methods, the OTP device
In the event of loss or theft of the OTP device, the Holder has to act according to Digital Banking Service Agreement.
The procedure for the PIN loss is the same one as the OTP device loss one.

4.8 Keys replacement procedure

4.8.1 Replacement of Holders' signature keys

Pursuant to [DPCM], the Certification Authority shall determine the expiration of the qualified certificate for electronic signature and the period of validity of the keys based on the length of the keys and the services such keys are to be used for.

The validity period of the keys coincides with the validity period of the corresponding qualified certificate for electronic signature, which is 3 (three) years.

A request for the issuance of a new qualified certificate for electronic signature is permitted only if the previous certificate has been expired or revoked.
The Holder can't have 2 (two) active qualified certificates for electronic signature at the same time for the same Legal Entity.

4.8.2 Replacement of certification keys

The replacement of the certification keys is performed by the Certification Authority in compliance with the applicable laws and regulations.

4.9 Management of the qualified certificated for electronic signature directory

4.9.1 Qualified certificates for electronic signature directory

All valid qualified certificates for electronic signature issued by the Certification Authority are saved inside a "certificates register".

The public directory contains instead the following information:

- the certificates for the Certification Authority's keys;

- the certificates related to the certification agreements;
- the certificates for AgID's signature keys;
- the list of the revoked qualified certificates for electronic signature.

The list the revoked qualified certificates for electronic signature is also published via HTTP protocol (http://crlcl.ca2.intesasanpaolo.com/qc/CRL$$.crl related to CA "Intesa Sanpaolo Qualified Electronic Signa-ture CA 2"
http://crl2.ca.intesasanpaolo.com/FirmaQualificata/CRL$$.crl related to CA "CA Intesa Sanpaolo S.p.A. Fir-ma Qualificata"

The Certification Authority uses reliable systems for the management of the qualified certificates for electronic signature directory and the public directory and uses methods that ensure that:

- only authorised persons can input data and make changes;
- the authenticity of the information is verifiable;
- the certificates are available for public consultation to the extent permitted by the Holder;
- the operator can be aware of any event which compromises the security requirements.

NB: $$ indicates the progressive number of the CRL (the number relating to the corresponding CRL is specified within each certificate, ex http://crl.ca2.intesasanpaolo.com/qc/CRL11.crl)

4.9.2 Publication of qualified certificates for electronic signature and CRL

The qualified certificates for electronic signature are published according to the procedures laid down in art. 34 of [DPCM].

CRL is created and is published in the public directory on an hourly basis, except in case of a technical impediment which is beyond the Certification Authority's control.

The access to the public directory is permitted through the public internet network at the address specified in the CRL Distribution Point Extension in the qualified certificate for electronic signature.

To allow you to check the revocation status of the certificate without making a request to the CRL, Intesa Sanpaolo makes OCSP services available.

The information on the CRL and OCSP profiles is reported in the CP-CPS of the certifier.

4.9.3 Reproduction of the qualified certificates for electronic signature directory on different websites

In accordance with [DPCM], the Certification Authority copies the certificate directory on a number of websites, ensuring the consistency and integrity of the copies.

Please see paragraph 4.13. for more details.

4.10 Personal data protection procedures

Information related to the Holder obtained by the Certification Authority during the performance of qualified certificates for electronic signature services shall be considered, except for the cases where a written consent of the Holder was issued, confidential and will not be published, with the exception of those expressly intended for public use (e.g. public key, date of revocation of the qualified certificate for electronic signature). Based on this RDS

Operating Manual, the Certification Authority does not process "special categories of personal data " as defined in GDPR Regulation

In the area of identification and data protection, activities performed will be compliant to the national law of the Bank which performs the registration authority activities. For clarification, the duration of the storage of certificates and all related documents and information are defined by Italian law, therefore the duration of storage will be compliant with Italian law.

The aforementioned personal data shall be processed by the Certification Authority in compliance with GDPR Regulation.

4.11 Procedure for organising the control log

The Certification Authority records in the control log, either automatically or manually, the events laid down in art. 36 of [DPCM]. In particular, at least the following events are recorded:

- issuance of qualified certificates for electronic signature;
- revocation of qualified certificates for electronic signature, specifying the date and time of publication of the CRL;
- start and end of work session of the systems used for generating qualified certificates for electronic signature;
- personalisation of the signature devices;
- entry in and exit from the secure rooms of the certification system.

The Certification Authority manages the control log in compliance with art. 41 (2) of [DPCM].

4.12 Backup copy management procedure

The Certification Authority has prepared and implemented a continuity plan for the service rendered pursuant to this Remote Digital Signature Operating Manual; the main actions to be taken according to the relevant procedures are described below.

4.12.1 Backup procedure

Backup copies are produced on a daily basis for data, applications, control logs and any other file necessary to completely restore the critical processors of the qualified certificate for electronic signature management system. Concerning these processors, the production of the backup copies is performed remotely and is controlled by a specific centralised system that meets the following requirements:

- minimise the need for human intervention and access to the technical rooms;
- simplify the scheduling of the backup operations and their auditing;
- increase the reliability of the backup operations.

4.13 Procedure for managing accidents and catastrophic events

A general outline of these procedures is provided below.

4.13.1 Computer failures

All the computers used for the provision of the qualified certificates for electronic signature service are covered by a maintenance agreement based on which the computers' reactivation, in case of failure, is guaranteed, within 24 (twenty-four) hours.

4.13.2 Software impairments

In case of impairments (loss or corruption) of programs or data that cannot be otherwise recovered, they shall be recovered from the stored backup files.

4.13.3 Failure of the Certification Authority's signature device

In case of failure of the Certification Authority's signature device, the private key shall be re-established on a new signature device starting from segments of previously generated keys, following a specific procedure that requires a joint intervention of more operators. The key segments are preserved in an encrypted form and in different containers, controlled by different managers.

NB: the key segments does not constitute a "copy" of the certification key ([DPCM]) and can be used only for the purpose of restoring of the entire key according to the procedure described above.

In the event the restoration of the certification key is not possible, the procedure on the impairments of the certification key shall be observed (see the following paragraph).

4.13.4 Certification key impairments

In case of impairments of the confidentiality of the private certification key, the Certification Authority shall:

- revoke the certificate related to the impaired private key;
- notify such revocation to AgID within 24 (twenty-four) hours as at the revocation;
- inform the Holders of all qualified certificates for electronic signature signed with the private key belonging to the revoked pair;
- revoke all qualified certificates for electronic signature signed with the impaired key;
- issue new qualified certificates for electronic signature using the new private key.

4.13.5 Main site compromise

In case of unavailability of the premises, of the building or of the system as a whole, following any type of disaster (fire, flood, collapse, etc.) the disaster recovery plan is activated; such plan applies to all operating resources of Intesa Sanpaolo and to the resources of the third party offering the time stamp service.

5. CESSATION OF QUALIFIED CERTIFICATE FOR ELECTRONIC SIGNATURE SERVICE

5.1 Details of the cessation of qualified certificate for electronic signature service

In case of termination of the service of Qualified Trust Service Provider, a specific communication shall be sent to AgID, at least 60 (sixty) days in advance, indicating, the new Certification Authority if such substitute Certification Authority has been identified, and the manager of the certificates register and the related documentation.
At the same time with the communication to AgID, all Holders shall be notified about the cessation of the activity.

Should no substitute Certification Authority has been identified, in the communication it shall be clearly specified that all the qualified certificates for electronic signature not yet expired at the time of the service cessation shall be revoked. The qualified certificates for electronic signature shall be included in the revocation list, at the time they are revoked.

For more details concerning the cessation of the service, reference is made to the Termination Plan prepared by Intesa Sanpaolo.

6. MANAGEMENT OF TIME REFERENCES

6.1 Timestamp service

This section refers to art. 40 (3) letter p of [DPCM].

The Certification Authority ensures a timestamp service in compliance with [DPCM], using the services provided by a certification authority that meets the requirements for operating in the countries where the Banks are located. For the description of the procedures regarding the transmission of the request for the issuance of a timestamp and for its acquisition, in accordance with the applicable laws and regulations, please refer to the operating manual of the provider of this service.

6.2 Accuracy of the time reference

The time reference management system retrieves the time from a radio receiver synchronised with a signal issued by the Isituto Elettrotecnico Nazionale (IEN) "Galileo Ferraris".

When generating a timestamp, the TSA server retrieves the date/time from the system clock, kept aligned with the exact time UTC (Coordinated Universal Time) by virtue of the synchronisation signal obtained by an external receiver that identifies the quality of the signal issued by the GPS satellites network. The time signal thus obtained complies with the accuracy margins required by the applicable laws and regulations.

7. DIGITAL SIGNATURE VERIFICATION PROCESS

This section refers to art. 40 (3) letter r of [DPCM].

7.1 Verification application

Inside “My Documents” area of the direct channels in place within the Banks, the Holder has the possibility to view his/her digitally signed documents. Such documents are saved in PDF format and depending on the remote channel (web, mobile) chosen by the Holder, he/she will always have at his/her disposal the native application for that channel that allows him/her to verify the applied digital signature.
The Holder can also receive the digitally signed documents by email.

As set forth in art. 42 (2) of the [DPCM], the verification systems available to the Holder are interoperable with the documents signed using the digital signature issued by the Certification Authority.

7.2 Documents format

The documents that are submitted to the Holder through the direct channels of the Banks comply with the applicable laws and regulations; in particular, the documents in electronic form, cannot contain "*macro instructions, executable codes, or other elements which may activate functions that can modify the acts, the facts or the data contained therein* ".

7.3 Warnings on CRL consultation

The necessary technical times for updating the information contained in the CRL shall be taken into account by the Holder and Legal Entity during its consultation.

In particular, such necessary technical times are required in case the Holder, the Legal Entity, the Registration Authority or the Certification Authority intend to revoke or reactivate a qualified certificate for electronic signature, as well as in case the Certification Authority carries out the technical/administrative procedures related to the revocation requests and the related update of the CRL.

When signing a document using the qualified certificate for electronic signature, the CRL list shall be checked as to ensure that the respective qualified certificate for electronic signature is not revoked.

8. OPERATING PROCEDURE FOR GENERATING DIGITAL SIGNATURES

This section refers to art. 40 (3) letter s of [DPCM].

The peculiarities of the service do not include the delivery of a signature application to be installed on the Holders' device (personal computer, smartphone, etc.); all the functions that allow the Holder to sign one or more digital document(s) shall be directly included in a specific section in the Digital Banking Service Usage Agreement and/or Agreement on Provision of Certification services utilised by the Banks.

The digital signatures created with the Digital Banking Service meet the requirements foreseen for signature algorithms laid down in art. 4 (2) of [DPCM].