National Bank of Belgium
Securities Settlement System

NBBSSS

Conditions of Use of the RAMSES Graphical User Interface

Table of Contents

1. Scope

In accordance with Article 6.2.1.1.2 of the Terms and conditions for the participation in the NBB-SSS, any Participant can send instructions manually and can send data to or receive information from the NBB-SSS in U2A modus and in pull and push mode through the RAMSES Graphical User Interface (GUI), having a connection with which is in principle mandatory for each Participant.

This document aims at defining the conditions of connection to and use of the RAMSES GUI, including the related certificates and tokens.

2. Definitions

Unless otherwise stated, the terms in this Annex shall follow the definitions as provided for in Article 2 of the "Terms and conditions for the participation in the NBB-SSS".

Furthermore, for the purpose of this Annex:

- "**BdE**" means the Banco de España, being the national central bank of the Kingdom of Spain;
- "**Certificate**" means an electronic file, issued by the BdE acting in the capacity of sole Certification authority in the framework of the RAMSES GUI and operator of the related PKI infrastructure, which binds a public key with a Certificate holder's identity and which is used for the following purposes:
  a) to verify that a public key belongs to the said Certificate holder;
  b) to electronically verify the identity of (= authenticate) the Certificate holder in order to verify his/her access rights to the NBB-SSS;
  c) to check a Certificate's holder signature.
- "**Certificate applicant**" means the physical person in favour of whom the issuance of a Certificate has been requested by the Participant to the BdE via the NBB acting in its role as Registration authority;
- "**Certificate holder**" means the physical person in favour of whom a Certificate has been issued by the BdE via the NBB acting in its role as Registration authority;
- "**Certificate user**" means either a Certificate holder or a Certificate applicant;
- "**Certification authority**" means the BdE it its capacity of entity trusted by the users of the certification services (Participants and Certificate users) to create, issue, manage, revoke and renew valid Certificates in the framework of the RAMSES GUI;
- "**CP**" stands for "Certificate Policy" and means the set of rules that define the applicability or use of a Certificate within a community of users that have a series of security requirements in common. The CP details and completes the CPS, containing the rules to which the use of the Certificates defined in this policy are subject, as well as the scope of application and the technical characteristics of this type of Certificate;

- “**CPS**” stands for “Certification practice statement” and means the set of norms and procedures that regulate the entire life-cycle of the Certificate used in the framework of the NBB-SSS, from its request to its end of subscription or revocation, as well as the relations that are established between the Participant, the NBB acting in its role as Registration authority, the Certificate applicant, the Certificate holder, the BdE acting in its role of Certification authority and the other Participants as relying parties of the said Certificate;
- “**ESCB**” means the European System of central banks, as ruled by the Treaty on the working of the European Union;
- “**Participant’s member**” means a natural person who is either a member of the staff of a Participant or a member of its decision making bodies;
- “**PIN code**” means the personal identification number delivered with the Token to the Certificate user, which serves as a Token password preventing the use of the Token by another person than the Certificate holder by locking the Token after repeatedly and consecutively entering wrong PIN codes;
- “**PKI**” stands for “public key infrastructure” and means the set of individuals, policies, procedures, and computer systems necessary to provide authentication, integrity and non-repudiation services by way of public and private key cryptography and digital Certificates, used by the NBB for the secure access to and use of the RAMSES GUI by Participants;
- “**PKI services**” means the services performed by the NBB and, for a part, by the BdE on behalf of the NBB, in the framework of the proper operation and maintenance of the PKI;
- “**Public key**” means a random number which is attributed to the Certificate applicant and is made accessible to any relying party via a publicly accessible directory held by the BdE. The public key is mathematically and uniquely related, by a cryptographic technique to the private key, being another random number which is attributed to the Certificate applicant and which is not disclosed to any third parties, so that a set of data that is encrypted with a public key may only be decrypted by its corresponding private key and vice versa;
- “**PUK code**” means the personal unlock key number delivered with the Token to the Certificate user, which serves as an administration Token password allowing the Certificate holder to unlock a Token that has been locked after repeatedly and consecutively entering wrong PIN codes;
- “**Registration authority**” means the NBB in its capacity of entity trusted by the users of the certification services (Participants and Certificate users) to verify the identity of the Certificate applicant before requesting the issuance of the Certificate by the BdE acting in its role of Certification authority;
- “**Token**” means the data carrier device (including USB-devices), on which the Certificate is stored, and the use of which is conditioned by the entry of the personal identification number (“PIN code”) of the Certificate holder;
- “**Trusted agent**” means the physical person who is appointed by the Participant to materially exert the competences resulting from the power of attorney entrusted by the NBB to verify on its behalf the identity of the Certificate user before physically delivering the Token to the latter.

3. Conditions for Access to the RAMSES GUI

The Participant can access the RAMSES GUI if:

- it has installed and maintains a domestic IT infrastructure allowing a proper connection with the NBB-SSS;
- it has subscribed to the NBB-Net TCP/IP secured data transport network set up by the NBB in order to be connected with the NBB's IT infrastructure and networks;
- it has provided to the NBB the duly completed static data collection forms and any additional information required or deemed useful by the NBB for the Participant's registration;
- at least one Trusted agent appointed among the Participant's members has undersigned and sent to the NBB the sub-Annex 8.3 of the Terms and conditions;
- it has acquired the dedicated Tokens and Certificates in order to get authenticated and to validly and irrevocably sign instructions and notifications passed through the RAMSES GUI; and
- it has successfully passed the Participant certification tests.

The NBB shall notify the Participant of its registration for direct access to the RAMSES GUI or, as the case may be, its rejection. Any rejection decision shall be reasoned.

4. Use of Certificates in order to access the RAMSES GUI and to pass valid instructions

4.1. Applicable rules: CPS, CP

As a rule, each Participant shall be held liable in the case of breach of the obligations contained in the CPS, in the CP and, in general terms, in any mandatory legislation or regulation that should apply with regard to the possession and use of Certificates, by Certificate users or by the Trusted agent belonging to its organisation.

As the NBB-SSS makes a local use of the ESCB-wide PKI infrastructure operated by the BdE for the account of all national central banks of the Eurosystem, among which the NBB, the Participant acknowledges and agrees that in its relations with the NBB, with the BdE in its capacity of certification authority, and with all other Participants of the NBB-SSS, it shall be bound by the ESCB-PKI CPS and by the ESCB-PKI CP for the non-ESCB users' Certificates, which are fully applicable by analogy to the NBB-SSS. However, it is understood – and accepted by the Participant – that for the analogical application to the NBB-SSS of the said CPS and CP:

- the BdE shall be the sole Certification Authority, as referred to in Article 1.3.2 of the CPS, entitled to issue valid Certificates to be used in the NBB-SSS;
- the NBB shall be the sole Registration Authority, as referred to in Article 1.3.3 of the CPS, entitled to verify the identity of the Certificate applicants Certificates to be used in the NBB-SSS;
- the Participants are External Organisations for the application of the CPS;

- Certificate holders are Certificate Subscribers as referred to in Article 1.3.6.1 of the CPS; the Certificates delivered by the NBB will be advanced Certificates stored on a cryptographic device (USB-key) in the sense of Article 1.3.6.1 of the CP;
- all Participants of the NBB-SSS (including the NBB itself) are Relying Parties as referred to in Article 1.3.6.2 of the CPS;
- "the ESCB" must be understood as "the NBB" (in particular the NBB-SSS) for the application of Article 1.4 of the CPS;
- except when explicitly otherwise provided for in this Document, contacts between the Participants, the Certificate users and the BdE shall only occur through the compulsory intermediation of the NBB;
- the Articles 9.1, 9.2 and 9.7 of the CPS are not applicable, but only the relevant provisions of the Terms and conditions for the participation to the NBB-SSS relating to the same items;
- for the application of Article 3.2.3 and Article 4.2.1 of the CP, it is understood that the identity authentication of an individual Certificate applicant shall occur either through a direct face-to-face identification process of the said Certificate applicant, either through an indirect identification process based on the communication of the evidence required by the said Article 3.2.3 by the Trusted agent after a face-to-face identification of the Certificate applicant by the Trusted Agent. No Token shall be delivered to the Certificate applicant but by means of a physical handover either by the NBB or by the Trusted agent (no expedition by mail or courier);
- a query for a Certificate can only be initiated by using the ESCB-PKI web interface, not by means of the ESCB Identity Access Management as referred to Article 4.1.2.1 of the CP;
- each Participant is validly entrusted with a power of attorney to request either the issuance of a Certificate, the delivery of a Token and/or the revocation of a Certificate on behalf of any Certificate user who belongs to the said Participant.

The version 1.2 of the ESCB-PKI CPS (dated December 10, 2013) is joined as sub-Annex 8.1 of the Terms and conditions, and the version 1.1 of the ESCB-PKI CP for the non-ESCB users' Certificates (dated January 11, 2013) is joined as sub-Annex 8.2 of the Terms and conditions. The Participant explicitly acknowledges and agrees to be fully aware of the existence and of the content of the said documents, which can be unilaterally amended from time to time without prior notice by the ESCB, in which case an actualised version is published on the website of the ECB[1] and is made available on the NBB-SSS team site.

4.2. <u>Respective roles and responsibilities of the involved Parties</u>

Without prejudice of the application of the CPS and CP as referred to in Article 4.1, which shall in any case enjoy precedence on the provisions of this Article, the following involved Parties are responsible for the provision of the following services:

[1] Address: http://pki.escb.eu/epkweb/en/repository.html. This hyperlink may be modified at any time without notice.

4.2.1. The BdE

In its capacity of Certification authority and of Verification authority, the BdE is e.g. responsible for the following tasks:

- generating advanced Certificates on request of the NBB in favour of the Certificate applicants according to the CPS and the CP and informing both the NBB and the concerned Certificate applicant of this issuance;
- revoking Certificates on request of the NBB acting as Registration authority and publishing this revocation in real time via the online ESCB-PKI repository (OCSP) as well as periodically through downloadable Certificate revocation lists, as soon as possible after the revocation request has been received;
- confirming the validity of the Certificate used by the Certificate holder in order to authenticate himself or to sign an instruction;
- keeping an up-to-date directory containing all Certificates and information about their current pending, validity, expiration and revocation status.

In the execution of the said services, the BdE commits itself to:

- refrain from keeping, processing, copying, disclosing or forwarding information about the Certificate user other than strictly necessary for the provision of its PKI-related services;
- abide by the applicable personal data protection laws;
- inform the Certificate holder at least three months in advance of the expiration of the validity of his/her ongoing Certificate;
- follow the validation mechanism supplementary to the publication of the Certificate revocation lists; and
- in general, abide by all the obligations imposed by the CPS, CP and applicable legislation to any Certification authority and to any Verification authority.

Notwithstanding this list, the Participant acknowledges and agrees that the BdE only performs PKI services on behalf and in the capacity of sub-contractor of the NBB, so that no single legal boundary shall exist between the Participant and the BdE. The NBB shall therefore exclusively and solely bear any liability resulting from an evidenced non-performance of the PKI services materially performed by the BdE, however within the liability limits defined in the Terms and conditions.

4.2.2. The NBB

The NBB is e.g. responsible for the provision of Token Management services and Account management services toward each Certificate user.

In its capacity of Registration authority, the NBB is e.g. responsible for the following types of services toward each Certificate user:

- adjusting its internal systems and interfaces to interoperate with the ESCB-PKI infrastructure in the framework of the RAMSES GUI;

- appointing NBB staff members in the role of PKI security officer, local identity administrator, personal Certificate requestor and registration officer before the start of operation of the RAMSES GUI and provide them with the adequate technical equipment;
- verifying the Participant’s identity and its ongoing eligibility status with regard to the adherence to the NBB-SSS;
- verifying the Certificate applicant’s and the Trusted agent’s identity and registering their identity and other related data in the PKI;
- submitting each Certificate request to the BdE;
- registering the serial number of each delivered Token, the hereto related PIN and PUK codes, the identification data relating to the Certificate applicant on behalf of whom the Token is issued, and the identification data relating to the Participant to which the concerned Certificate applicant belongs;
- delivering, either physically, by postal mail or by courier and against written receipt, to the Certificate applicant or to the Trusted agent empowered by the NBB to verify the Certificate applicants’ identity, one envelope per Certificate applicant with a view to the use of the RAMSES GUI in production environment, containing one Token, together with its initial PIN code and its PUK code, as well as the data needed to allow the download of the Certificate from the ESCB-PKI website, and;
- managing the replacement of lost, stolen, destroyed or damaged Tokens and revoking the Certificate stored on the said lost, stolen, destroyed or damaged Token;
- managing the blocking of a Token due to a loss of the PIN code or a repeated entry of a wrong PIN code;
- informing the Certificate holders about the working, functionalities, technical characteristics and requirements of the use of Certificates in the framework of the RAMSES GUI; and
- providing the service desk technical assistance to the Certificate holders via a single point of contact (SPOC), in case of an incident impeding or affecting a Participant’s access to the NBB-SSS, which is not imputable to either SWIFT, the NBB-Net or the Participant’s network service provider.

4.2.3. The Participant

The NBB shall validly rely on any information or message authenticated by a Certificate delivered to a Certificate holder who is a Participant’s member and shall lawfully carry out instructions and settle transactions signed with such a Certificate in the name of the said Participant on its own behalf or on behalf of the Participant’s clients. The Participant hereby acknowledges and agrees that it shall irrevocably, fully and definitely be bound by information, messages, instructions carried out and transactions settled by the NBB-SSS that are authenticated or signed with a Certificate delivered on behalf of one of the Participant’s members and, therefore, that it bears full and exclusive responsibility and liability toward other Participants and third Parties, if any, for any misuse of the Token after its handover by the NBB to the Certificate applicant or the Trusted agent.

Furthermore, the Participant acknowledges and agrees that the “four-eye principle” is applicable to the signature of instructions so that two electronic signatures are required for the validation of the creation, the modification or the cancellation of each individual instruction.

The use of a Certificate shall be strictly personal to the Certificate holder and may not be shared with third parties, whether being Participant’s members or not. No Certificate may be used as a group or entity-bound Certificate. The Participant shall take all security measures in order to prevent such an abuse of the Certificate. Any Certificate may be immediately revoked without prior warning or notice by the NBB if the latter becomes aware of such an abuse of the Certificate.

The Participant shall appoint at least one (preferably two or more) Trusted agent among the Participant’s members in order to materially exert on the basis of a power of attorney delivered by the NBB, the competence to verify the identity of the Certificate user on behalf of the NBB before physically delivering to the said Certificate user the Token, together with the initial PIN code and the PUK code relating to the delivered Token and the associated user identification data linked with each delivered Token. The Participant shall verify that the Trusted agent has signed the “Terms and conditions relating to Trusted agents”, joined as sub-Annex 8.3 of the Terms and conditions, and shall send the duly signed form to the NBB. Together with the Trusted agent, the Participant shall be responsible for the performance of the said identity verification and Token delivery tasks by the Trusted agent and bears the exclusive responsibility for the use of the said Tokens in order to send instructions and sign transactions in the Participant’s name as soon as the Trusted agent has delivered to the NBB a signed receipt of the concerned Tokens. Therefore, the NBB shall not incur any liability for any damage resulting from a possible misuse of the said Tokens as from the same moment in time.

Without prejudice to the provisions of Article 6.2.1.2 of the Terms and conditions, each Participant shall design, test and implement adequate business continuity and contingency procedures and practicable IT-roundabouts in order to manage any denial of service or hampered operation of the RAMSES GUI.

The Participant shall implement adequate security controls in order to protect and prevent the RAMSES GUI from unauthorised access. The Participant shall ensure the adequate protection of the confidentiality, integrity and availability of its own IT systems.

The Participant shall inform the NBB of any security-related incident in its technical infrastructure and, where appropriate, security-related incidents that occur in the technical infrastructure of third party providers which may have an impact on the confidentiality, integrity and availability of the RAMSES GUI. The NBB may request further information about the incident and, if necessary, request that the Participant takes appropriate measures to prevent a recurrence of such an event. The NBB may also impose additional security requirements on the Participant.

The Participant shall inform the Certificate applicants of:

- the processing by the NBB, and by the BDE acting as sub-contractor on behalf of the NBB, of relevant personal data with the sole purpose of identifying the Certificate applicants in order to link the Token, and the Certificate stored on it, to the concerned Certificate applicant's identity;
- the personal data which are processed, being the Certificate applicant's name, surname, place and date of birth which are extracted from the copy of the Certificate applicant's identity documents joined as an annex to the certificate application form;
- the fact that the NBB is the sole responsible entity for the said processing of personal data;
- the NBB's complete address;
- the Certificate applicants' personal rights to consult and correct the above mentioned personal data processed by the NBB;
- the fact that these personal data shall be irrecoverably removed from the NBB's files one year after the revocation of the latest Certificate issued by BDE in the name of the Certificate user.

5. Change management

As the PKI makes use of the ESCB-PKI infrastructure, new ESCB-PKI features and functionalities, as well as changes to the ESCB-PKI's existing features and functionalities, may be implemented by the NBB in the PKI without prior notice. The NBB shall inform as soon as possible the Participants of the changes that may have a material impact on the provision of the PKI services or the procedures to be followed in this framework.