CFONB
Comité Français d'Organisation
et de Normalisation Bancaires

Common Acceptance Policy

CAP

Politique d'Acceptation Commune

PAC

Ref. : Version 3.1 En

CONTENTS

1. Preamble

Today, internet technology is at the heart of issues relating to the open access, interconnection and collaboration of information systems. These new concepts are increasing the scope of the extended enterprise approach - a network made up of the company and its community: customers, partners (strategic and financial), suppliers, Government Department, etc.

Organisations want to improve the economic efficiency of their processes by implementing applications that dematerialise data and flows. As well as reducing costs by moving away from the "paper trail" (workloads, postage costs, archiving limitations, etc.), these applications can improve responsiveness and quality of service, and, most importantly, create more streamlined business processes.

Applications to dematerialise data flows are, of course, numerous and concern all sectors of the economy. They involve setting up trusted spaces, in which the different parties involved can be technically identified and authenticated, and where the quality of transactions and the parties issuing them can be checked.

The digital certificate is key to building trusted spaces; it allows the holder to authenticate their identity (ID certificate), to sign (signature certificate), to establish a secure connection, and more. The application uses the certificate as a means of identifying its holder and to check the integrity of information when approving access or checking a signature.

There are now many parties that issue certificates (banking sector, Government Department, businesses, etc.). In general, an application must be able to accept certificates from different certification authorities; in an increasingly open world, it would be both too costly and too burdensome to require the same holder to obtain one certificate per application.

It is essential, when a certificate is presented to an organisation or to an application, to know its level of security (level 1, level 2, etc.), the level of commitment of the associated Certificate Authority, and its possible limitations (liability insurance, etc.).

An Acceptance Policy is a set of rules that defines the requirements applicable to a Certificate Authority so that their certificates can be accepted by a particular community and/or category of applications that have common security requirements.

The Common Acceptance Policy (CAP) has been introduced by the French banking sector, for the banking sector, to meet the needs of banking application Issuers and to allow them to use, as a means of identification and of signing certificates, different families of certificates (issued according to different certification policies) by giving these certificates a minimum level of quality; in particular, the Acceptance Policy considers the quality of certificates accepted and thus the Certification Policies (CP) defining the conditions under which the certificates were issued.

The CAP Committee will be responsible for upgrading the CAP, either when the market changes its demands or needs, for example following regulatory developments, or when the banking community has to adapt its requirements to new banking needs. The new CAP version will be sent out with enough time to achieve the required changes before implementation.

In France, the Government Department, in consultation with stakeholders, has defined the PRIS/RGS (Inter-Sectoral Security Standards Policy/General Security Requirements), which characterises the key elements that a CP must observe, in accordance with the level of quality of the certificates with which it is associated.

The rules Frameworks in force, mentioned in this document, are:

- The PRIS until 19 May 2016.
- the RGS V1 until 1st July 2016.

The CFONB, *Comité Français d'Organisation et de Normalisation Bancaire*, adopted the PRIS/RGS as a universal benchmark for the banking sector in the matter of issuing digital certificates. This reference to the PRIS/RGS helps to build on work already carried out and to provide for coexistence and consistency with trusted infrastructures set up as part of online services and the remote procedures of the French Government Department.

For a CA to qualify as CAP compliant, the CA must also be listed with the PRIS/RGS or have been given a certificate of PRIS/RGS compliance by a COFRAC-accredited organisation, or equivalent. It is, however, important to take into account the specific nature of the PRIS/RGS and, when needed, be able to incorporate other national or European standards.

This CAP will be updated in the light of European Regulation 910/2014 known as eIDAS adopted on 23 July 2014, which will apply from 1st July 2016, once all of its implementing acts have been published.

The CAP sets out a number of principles, which the different parties involved in this policy undertake to observe.

The CAP meets the needs of Issuers of common or individual applications for banking and financial institutions declared as accepting CAP certificates, but can be rolled out to specific applications to meet the needs of:

- Banking and financial institutions in other countries
- Non-banking third party partners (French or from other countries)

The CAP does not address:

- Validation principles, which are defined in the best practices validation guidelines for signature certificates
- The rights, attributes and limitations associated with the holder, which are managed at application level (and/or possibly at the level of the certificates themselves)

In addition, the CAP allows:

- An entity issuing certificates certified as consistent with the CAP to disseminate its certificates more widely
- A certificate holder to expand the circumstances in which its certificates are used

SOME DEFINITIONS

Acceptor:

- The organisation or application that, in response to a risk level assessed by the application Issuer, uses certificates certified as CAP compliant
- The acceptor is, in the context of this CAP, the Issuer of the application using the certificate

Application:

- An application is a program or set of programs used to accomplish one or more tasks

Common Applications:

- Applications common to banks and financial institutions, or in the Banque de France definition, common to credit institutions and investment firms (e.g. the COREP, COFINREP, BAFI applications).
  - A common application may be an application issued specifically by an institution to fulfil a common need and a single purpose.
    - o Common applications include interbank applications.

Individual Applications:

- The individual applications of a bank or financial institution or credit institutions and investment firms, other than Common Applications (e.g. securities management).

Applications accepting CAP certificates:

The types of application that can be declared as accepting CAP certificates are:

- applications common to banking institutions
- individual applications that meet the needs of:
  - o Banking and financial institutions in other countries
  - o Non-banking third party partners (French or from other countries)
- specific to a banking and financial institution that is part of the CAP

Certificate Authority (CA):

- An organisation trusted by one or more entities to manage the life cycle of a certificate: producing, distributing, revoking, suspending, renewing, or archiving digital certificates (Definition CFONB- 12/2003)
- ***RGS definition***: Within an electronic certification service provider, a Certificate Authority (CA) is responsible, on behalf of and under the responsibility of this provider, for the application of at least one certification policy and is identified as such, as the "issuer", in certificates issued under this Certification Policy.

Rules framework

The rules framework define the conditions applicable to certificates to ensure their compliance with the principles of the CAP.

For France, the framework in question is the PRIS/RGS.

Digital certificate:

- Digital attestation that links all data related to verifying the signature for a person and confirming the identity of that person (Article 2 of European Directive 1999/93/EC)
- Entitles the holder to authenticate and sign electronic transactions
- Is characterised by its associated security level (level 1, 2 or 3)

Qualified certificate:

- A qualified certificate is issued by a certification service provider that meets the requirements laid down in the European directive of 1999, transposed into French law by the Law of 13 March 2000 and Decree No. 2001-272 of 30 March 2001

The CAP Committee

This committee is responsible for definition of the CAP and its developments. It defines the CAP reference and the procedures for processing CAP compliance requests.

The address of the CAP Committee is:

CFONB
Comité PAC
18 rue Lafayette
75002 PARIS

CAP Registration Committee

This Committee checks compliance with the CAP rules framework, defined by the CAP Committee in accordance with the established procedures, and delivers the CAP listing to a Certificate Authority of family of certificates, and even the acceptance of CAP certificates by an application.

The address of the CAP Committee is:

CFONB
Comité d'Enregistrement PAC
18 rue Lafayette
75002 PARIS

COFRAC:

- French Accreditation Committee: a French organisation responsible for the accreditation of laboratories, certification and inspection bodies.

Compliance:

- Compliance concerns:
  - Organisations, through an application that accepts CAP certificates or a CA or family of certificates declared compliant; the organisation is thus CAP compliant;
  - CAs or families of certificates declared compliant;
  - Categories of applications that accept CAP certificates.

Correspondent:

- A contact person representing the CA or the application with a mandate on behalf of their entity.

CRL:

- The CRL (Certificate Revocation List) lists certificates that have been revoked by the Certificate Authority.

eIDAS (electronic identification And trusted Services):

- EU Regulation No. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, coming into effect on 1st July 2016.

Issuer:

- The CA in a position to issue certificates or families of certificates.

Family of certificates:

A set of certificates, sometimes with different levels, each responding to a clearly defined certification policy of the issuing CA.

Quality level:

The quality of a certificate is defined by:

- The certificate's security level;
- The organisation's level of commitment regarding the certificates for which it is responsible.

Level of commitment:

The organisation's level of commitment regarding the certificates for which it is responsible is defined as part of the CP. The organisation states that its level of commitment includes financial guarantees and insurance policies tailored to its activities and the resulting responsibilities.

Security level:

Three security levels are defined for certificates:

- Level 1: A software certificate that can be issued without a face-to-face transaction;
- Level 2: A paper certificate issued after a face-to-face transaction;
- Level 3: A paper certificate with a very high level of security, proving the quality of a qualified certificate to enable the implementation of an advance signature with presumption of reliability.

OCSP:

(Online **C**ertificate **S**tatus **P**rotocol). An online verification protocol of the current status of the certificate without requiring CRLs.

Acceptance Policy:

- An Acceptance Policy is a set of rules that defines the requirements applicable to a Certificate Authority so that their certificates can be accepted by a particular community - primarily the banking community in this case - and/or category of applications that have common security requirements

Certification Policy (CP):

- The Certification Policy, implemented by the Certificate Authority and with which it is committed to comply, is a text that defines the quality of a certificate and in particular its security level (level 1, 2 and 3, equivalent to the 1, 2 or 3-star levels in the PRIS/RGS framework)
- ***Definition taken from the RGS***: A set of rules, identified by a name (OID), which defines the requirements with which a CA must comply, for the implementation and provision of its services and indicating the applicability of a certificate to a particular community and/or category of applications with common security requirements. A CP can also, if necessary, identify the obligations and requirements on other stakeholders, including the holders and users of certificate.

Validation Policy:

- The Validation Policy is the set of texts that establish the duties and responsibilities of the entity (the validating authority) responsible for managing it.

  This Validation Policy can be implemented by one or more entities, on one or more physical platforms.

  The main responsibilities of the entity in charge of validation will focus on:

  - the definition of the sequence of proof management functions depending on the application and the certificate used;
  - administration of management rules;
  - monitoring of the chain of trust for the certificate;
  - data monitoring and extensions;
  - checking the status of the certificate;
  - validation of the signature;
  - monitoring of the acceptance policy adopted by the application.

Electronic Certification Service Provider (PSCE):

- ***PRIS/RGS definition***: Any person or entity who is responsible for the management of digital certificates throughout their term of validity, vis-à-vis the holders and users of these certificates. A certification service provider can provide various families of certificates corresponding to different purposes and/or different levels of security. A certification service provider includes at least one CA but can actually comprise several, depending on its organisation. The different CAs of a certification service provider can be independent of each other and/or related by hierarchical or other links (Roots CAs/Intermediate CAs). A certification service provider is identified in a certificate, for which it is responsible through the CA that issued the certificate, and which itself is directly identified in the "Issuer" field of the certificate.

PRIS:

- PRIS: *Politique de Référencement Intersectorielle de Sécurité*, or Inter-Sectoral Security Standards Policy, initially published by the ADAE (French Electronic Administration Development Agency) and since taken over by the DGME (General Directorate for State Modernisation);
- This rules Framework is historic. It was originally created to enable the private sector to equip businesses to use remote procedures using the certification.

Program:

- In computing, a program is a sequence of predetermined operations to be executed automatically by a computer device for the purpose of carrying out work and arithmetic or logic calculations, or simulate an operation.

Application Issuer:

- In the context of the CAP, the application Issuer is responsible for a particular application that uses certificates listed as complying with the CAP;
- The application Issuer takes the role of certificate acceptor.

CAP Compliance Accreditation

To list a family of certificates as CAP compliant, a request is made by the organisation supporting the Certificate Authority that is issuing the certificate for CAP compliance.

The accreditation is confirmed by the CAP Registration Committee, according to the rules established by the CAP Committee in the "Common Acceptance Policy" document.

RGS:

- RGS V1: *Référentiel Général de Sécurité* or General Security Requirements, published by Decree No. 2010-112 of 2nd February 2010, under the responsibility of the DGME and ANSSI (French National Computer Security Agency).
- The French banking sector refers to the RGS, successor to the PRIS, without, however, there being a systematic alignment of the CAP with future versions of the RGS;
- The CAP Committee will consider, case by case, the benefits of taking into account new frames of reference (particularly in Europe).

SSCD (Secure Signature Creation Device)

A cryptographic hardware device used by the holder to store and implement their private key and whose security level is defined by ANSSI.

See Article 1, paragraph 6 of Decree 2001-272 of 30 March 2001.

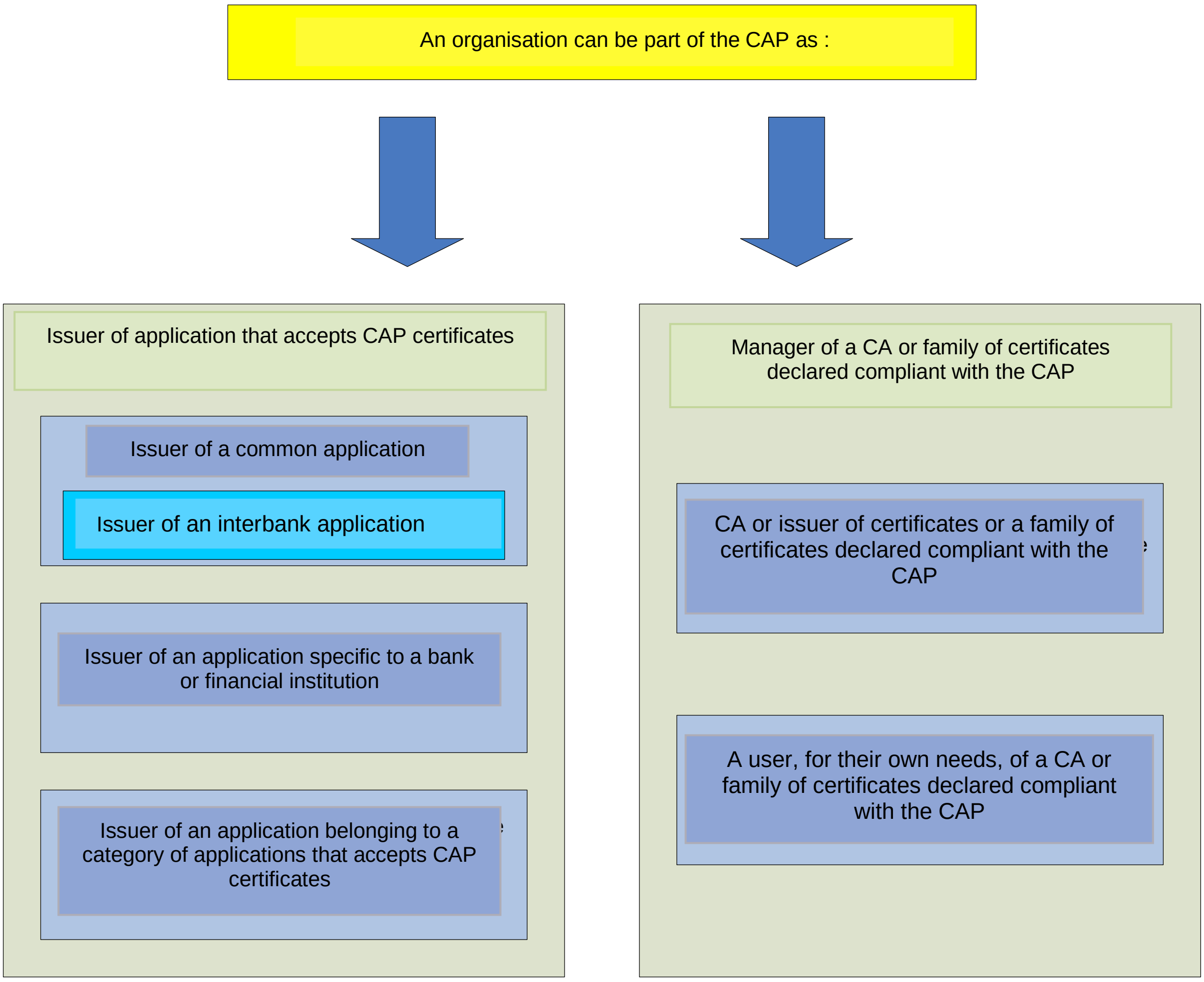
SCVP (Server-based Certificate Validation Protocol)

A standardised internet protocol (RFC 5055) for exchanging information on the validity of certificates used by an application. This protocol determines a certification path between the application and one or more validation servers.

2. THE COMMON ACCEPTANCE POLICY

The Common Acceptance Policy

The Common Acceptance Policy (CAP) has been defined by the French banking sector, for the banking sector, to meet the needs of application Issuers in the banking sector and to allow them to use different families of certificates (issued according to different certification policies) by giving each family of certificates a minimum level of quality.



An organisation can be part of the CAP as :

Issuer of application that accepts CAP certificates

Issuer of a common application

Issuer of an interbank application

Issuer of an application specific to a bank or financial institution

Issuer of an application belonging to a category of applications that accepts CAP certificates

Manager of a CA or family of certificates declared compliant with the CAP

CA or issuer of certificates or a family of certificates declared compliant with the CAP

A user, for their own needs, of a CA or family of certificates declared compliant with the CAP

It is essential to note that the concept of compliance is different for certificates and user applications:

- CAs and families of certificates are listed as compliant with the CAP;
- Applications that use certificates declare themselves compliant, with reference to the CAP.

The objectives of the CAP

The CAP is used by:

- The banking sector in developing a trusted space around electronic signatures, a multi-acceptance approach, and in the quest for better control of the risk;
- Application Issuers will thus be able to:
  - Determine the quality level of a certificate in line with the security requirements they deem necessary to reduce or hedge their risks;
  - Use certificates listed as compliant with the CAP.

It helps to strengthen the rules Framework for trusted spaces attached to the Banking Sector.

The CAP allows the different stakeholders to know:

- The list of compliant CAs and families of certificates both within and outside the French banking sector.
- The minimum levels of security and quality for certificates:
  - Security level 1, 2 or 3;
  - Level of commitment of the issuer.

The CAP concerns authentication, signature and encryption certificates. In reference to the PRIS/RGS, we will accept "dual use" certificates, used both in authentication and signature.

The building blocks of the CAP

To facilitate updates, the CAP is structured around:

- A fixed document content that stipulates:
  - The criteria to be met by families of certificates and their issuers on the basis of quality levels;
    - The Certification Policy, with reference to the PRIS/RGS;
    - The level of commitment of the issuer.
  - The minimum checks that applications will need to carry out on certificates
    - These checks are required for all applications that use the CAP.
- A series of appendices to this document:
  - A review of the context;
  - Requirements related to the certificate's security level;
  - The characteristics of certificates based on their security level;
  - Checks to be made on the certificate as part of the CAP;
  - Reference documents.
- Lists published alongside the CAP to clarify:
  - A list of compliant CAs and families of certificates which will gradually grow;
    - The associated Certification Policy;
    - The associated commitment level;
    - A correspondent;
    - A list of applications accepting CAP certificates for which strict compliance with the CAP is necessary.
  - A list of CAP member organisations:
    - Issuers of CAP listed certificates;
    - Issuers of applications that accept CAP certificates.
  - A list of official publication websites.

The reference documents

The CAP is based on:

- The Certification Policies of banks (and possibly non-banks) listed with the PRIS/RGS or declared as PRIS/RGS compliant following an audit by a COFRAC-accredited organisation or equivalent.
- Documents outlining the templates of certificates
- The ethical rules framework defined by the CAP
  - Regulatory compliance;
  - Compliance with the general ethical principles defined in the paragraph on "Compliance Principles".

3. THE KEY ELEMENTS OF THE CAP

The CAP is structured around a set of principles:

- Structural principles
- Technical principles
- Principles of certificate quality
- Organisational principles
- Principles of liability
- Acceptance principles
- Principles of compliance
- Principles of publication
- Principles of reimbursement
- Principles of renewing a CAP accreditation

All CAP stakeholders undertake to strictly observe these principles.

Structural principles

Organisations

An organisation is said to be a member of the CAP if, and only if, it includes:

- An application accepting CAP certificates
- A CA or a family of certificates that is listed as compliant with the CAP

In case of suspicion (key compromise, fraud, etc.) the person in charge of the application and/or the CA shall notify the CAP community via the CAP Registration Committee, by any electronic means (information on the CFONB web server, notification email).

Applications

It is essential to clearly separate the different categories of applications:

- ***Common applications,*** for which the Issuers of the common application in question will define, in liaison with authorities concerned, the risk levels that they are willing to accept, and get these validated by the community
    - The application Issuer agrees that these common applications will strictly observe the principles of the CAP when it uses CAP certificates.
- Individual applications specific to a bank or financial institution that are part of the CAP, which can use the CAP as rules framework
    - Each entity remains in control, for each of its individual applications, of the risks it is willing to bear and the families of certificates it will accept
- Applications are free to use CAP certificates without being accredited but they will not be able to declare themselves CAP compliant.
    - The Issuer of this application will have to request CAP accreditation in advance.

The Common Acceptance Policy (CAP) is used by an application Issuer to identify CAs and families of certificates that enable it to meet the risk level assessed as part of their application.

The analysis of the application's risk level and, consequently, the quality level of the certificates used, are the strict responsibility of the application Issuer.

The CA listed as CAP compliant cannot object to the use of its families of certificates by an application that itself accepts CAP certificates.

CAs and families of certificates

To comply with the CAP, the CA or family of certificates must meet one of the following rules:

- The Certification Policy (CP) is based on the PRIS/RGS guidelines: as the CA is qualified as compliant with the PRIS/RGS, it must produce the qualification certificate provided after an audit by a COFRAC-accredited organisation.

  The security level of the certificate (level 1, 2 or 3) is therefore recognised, as it is consistent with the definitions of the PRIS/RGS.
- The CP is based on a rules Framework other than the PRIS/RGS
  - If this rules Framework is already certified as compliant with the CAP (with its level of quality certified as equivalent or superior to that of the PRIS/RGS), as the CA is qualified using this framework, it must produce the qualification certificate provided following an audit by a COFRAC-accredited body or equivalent.

    The security level of the certificate (level 1, 2 or 3) is therefore recognised, as it is consistent with the definitions of the PRIS/RGS.
  - If this rules Framework is not yet recognised as compliant with the CAP, the first step is to define the framework's equivalency with the levels of the CAP. The new framework, after identifying any discrepancies, will then be incorporated into the CAP standards after an audit by a COFRAC-accredited body or equivalent has given a positive result. The result of the audit must be submitted to the CAP Registration Committee.
- The CP is not based on any rules Framework and there is no request or reason to create a new framework. The CA must provide the positive result of an audit carried out by a COFRAC-accredited body or equivalent, in line with the CAP framework.

In all cases, the CP associated with the CA or family of certificates must also comply with the CAP.

The compliance of a CA or family of certificates will be based on:

- An audit of the associated CP when it is not based on a rules Framework (PRIS/RGS or equivalent standard already recognised by the CAP Committee);
- The financial soundness of the issuing organisation;
- An assessment of the level of commitment from the organisation responsible;
- Validation of the organisation's consistency with the rules of compliance.
- The provision, where applicable, of a physical acceptance certificate to verify interoperability with CAP compliant applications (see Appendix 1).

Technical principles

'Certificates Issuer' functions

The CAP defines three levels of security for certificates (level 1, 2 or 3) based on the principles defined by the French Government Department as part of the PRIS/RGS. These three levels are specific to the CAP and the banking sector; they can, in particular, differ from PRIS/RGS definitions.

Each level is a superset of the lower level; as such, a certificate certified as level 2 compliant can be used in applications requiring both Level 1 and Level 2.

The fundamental element for defining the security level of a certificate is the Certification Policy with which it is associated.

An Issuer of applications that accept certificates from a CAP-compliant CA is assured that the certificate complies with a minimum security level.

Aside from constraints related to the design and management of the CA, level 1, 2 and 3 certificates will mainly be characterised by the three following criteria:

	Level 1 certificate	Level 2 certificate	Level 3 certificate
The handover principle	Any means of handover with a minimum of security may be considered (face to face or remote enrolment)	Handover is necessarily face to face	Handover is necessarily face to face
Certificate containment system	Software certificate	Certificate on cryptographic hardware device.	Certificate on a SSCD device
Key size[1]	1024 or 2048-bit RSA	2048-bit RSA[2]	2048-bit RSA minimum

For more information, see Appendix 4 and 5 of this document.

The Certification Policy (CP)[3] of the applicant CA must:

- be based on a framework recognised by the CAP Committee as being able to ensure the quality of certificates issued,
- specify the key usages of certificates

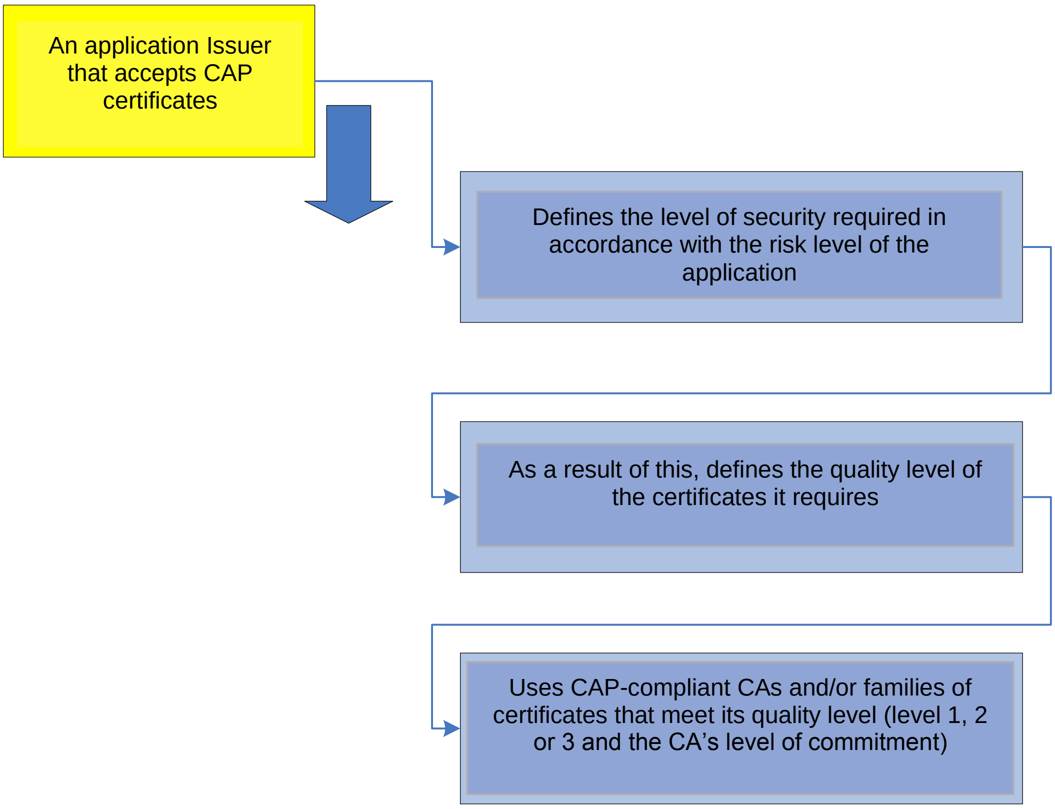
[1] The issuance of certificates with specific key sizes is currently governed by ANSSI in France.
[2] A 1024-bit key length is tolerated in a transitional phase until the certificate is next renewed.
[3] The CP may be specific to the organisation

The fact that a CA is qualified/listed as compliant with the PRIS/RGS helps to ensure the security level of the certificate, without the CAP Registration Committee having to order a specific and thorough audit.

Other rules Frameworks (particularly those from other countries) are acceptable for judging the security level of a certificate. In this case, the CA must provide the results of the audit carried out by a COFRAC-accredited firm (or equivalent in countries other than France) to make sure that these standards provide quality levels at least equivalent to those defined by the PRIS/RGS (N.B. in the latter case, the costs will be borne by the CA in search of CAP approval).

'Applications Issuer' functions

The application Issuer conducts a risk analysis and defines the necessary quality level of certificates (authentication and/or signature, encryption).



An application Issuer that accepts CAP certificates

Defines the level of security required in accordance with the risk level of the application

As a result of this, defines the quality level of the certificates it requires

Uses CAP-compliant CAs and/or families of certificates that meet its quality level (level 1, 2 or 3 and the CA's level of commitment)

Using the identification certificate

Field	Level 1 certificate	Level 2 certificate	Level 3 certificate
Typical contexts for use	Existing but relatively moderate risk of attempted identity theft to gain access to applications and/or property or in order to demonstrate the origin of data	Significant risk of attempted identity theft to gain access to applications and/or property or in order to demonstrate the origin of data	Very substantial risk of attempted identity theft to gain access to applications and/or property or in order to demonstrate the origin of data

Using the signature certificate

Field	Level 1 certificate	Level 2 certificate	Level 3 certificate
Typical contexts for use	Existing but relatively moderate risk of attempted identity theft and loss of integrity in order to unduly sign data	Significant risk of attempted identify theft and loss of integrity in order to unduly sign data	Very substantial risk of attempted identify theft and loss of integrity in order to unduly sign data

Using the confidentiality certificate

Field	Level 1 certificate	Level 2 certificate	Level 3 certificate
Typical contexts for use	to ensure confidentiality of data either during its transport or storage The risk of loss of confidentiality is moderate and there is no need for recovery	to ensure the confidentiality of stored data The risk of loss of confidentiality and the need for recovery are significant.	to ensure the confidentiality of stored data The risk of loss of confidentiality is very substantial and recovery is required.

N.B. The confidentiality certificate is primarily used to exchange keys used by data encryption algorithms such as 3DES or AES. It can also be used to encrypt data but with a performance level that limits its use in specific areas.

The application Issuer defines the necessary level of security and relies on the CAs and families of certificates that comply with the CAP, in line with its needs. In general, the certificates used will be:

- Level 1 certificates, to protect against the moderate risks;
- Level 2 certificates when faced with higher risks;
- Level 3 certificates when faced with substantial risk.

The application Issuer must make sure that the security policy associated with the application defines a technical, procedural and legal framework, taking into account the level of quality of the certificates and:

- the use of secure devices (SSCD), if necessary;
- the usual checks of the certificate, based on the application's requirements (structure, key usage, expiry date, etc.);
- the consultation of certificate's status (CRL, OCSP, SCVP, etc.);
- the use of certified tools, if any;
- the CAP accreditation of the CA's family of certificates used by the application,
- etc.

The application Issuer is responsible for the usual security checks to be carried out regarding electronic certification and transactions.

The application Issuer is responsible for ensuring the quality of the certificate as defined below, and for managing the validation thereof; monitoring of rights, user accreditations and usage restrictions applicable to different users are out of scope of the CAP.

Principles of certificate quality

A certificate-issuing organisation is committed to respect the following principles for the CAs and/or families of certificates it wishes to be accredited:

- A Certification Policy for CAs and/or families of certificates that complies, as a minimum, with the principles of PRIS/RGS
    - The structure of the certificate
        - Compliance with the X509 V3 format
        - Compliance with extensions (particularly in critical extensions)
        - Compliance with the principles of identification
    - Key length
    - The principles of certificate containment:
        - Software Certificate (limited to level 1)
        - Certificate on a cryptographic hardware device, a technical solution required for a level 2 or 3 (smart card, token, etc.)
        - The lifespan of the certificate (and signature CA key)
    - The principles of registration and distribution
        - Naming rules
        - Initial identity validation
        - Processing of the certificate request
        - Face-to-face handover for level 2 or 3 certificates
    - Managing the life cycle of certificates
        - Renewal and issuance of a new certificate
    - Function giving information on the status of certificates
        - CRL management and/or OCSP requests/responses
    - CA management principles
    - Principles of security and management for cryptographic elements associated with the CA

- Level of commitment for its various families of certificates.

With regard to the quality control of a certificate, an application accepting a CAP certificate must, as a minimum, observe the following principles:

- Checks of templates, validity date, extensions
- Checks of the status of the certificate

Organisational principles

Correspondents

The CAP member organisation appoints:

- A manager and a deputy for all CAs and families of certificates recognised as compliant, who will:
    - Assist partners in the implementation of compliant certificates
    - Be notified promptly in the event of an incident
- A manager and a deputy for all applications that accept CAP certificates, which partners can call upon for issues involving the use of certificates.

Publication

See Appendix 2

Principles of liability

The commitments made by a CA are defined in the Certification Policy.

Incidents

An organisation shall immediately inform the CAP Registration Committee when an incident occurs:

- Upon issuance of a certificate
    - Corrupt secret
    - Incidents related to registration
    - Etc.
- During checks carried out by an accepting application

The organisation's obligations and the procedures to follow in the event of an incident are specified by the CP associated with the family of certificates or any document referring to it.

Any organisational changes affecting the CAP must be communicated to members.

Liability of the holder

The liability of the holder is not governed by the CAP but directly by the certificate issuer (CA) as part of its relationship with the holder.

Liability of the issuer

For CAs and families of certificates, a certificate issuer qualifying as CAP compliant must strictly observe the following:

- The CPs associated with the CA and families of certificates declared as compliant
- The criteria regarding the organisation's financial soundness
- The levels of commitment on certificates
- The principles of security, liability and compliance defined in the CAP
- The principles of reciprocity

Liability of an application Issuer

An Issuer is responsible for:

- Setting the level of risk of its application and the quality level of usable certificates
- Complying with certificate validity checks

Dispute management

Any conflicts or disputes are managed directly between the accepting entity and the issuer of the certificates concerned.

In the event of a dispute, the CAP cannot be referred to by:

- An organisation that is not part of the CAP
- A member organisation for applications not declared as compliant with the CAP.

Acceptance principles

A third party application Issuer that accepts CAP certificates may use these without all the certificates accepted by said application necessarily being consistent with the CAP.

Principles of compliance

An organisation that declares an application to be compliant with the CAP is committed to observing the following principles, as a minimum:

- Reference to the CAP and any use of certificates relating thereto in applications using them, is not permitted for applications that are considered as illegal or unlawful by the regulations applicable to them. This principle is an important fundamental principle, and the organisation must agree to fully comply.
- It is up to the organisation to ensure that its applications comply with the regulations in force. Under no circumstances can accreditation be taken as evidence of a compliance check by the CAP Registration Committee. This check is the sole responsibility of the organisation.

In the event of a breach of these principles, the CAP Registration Committee may ask the organisation to make sure the application using certificates makes no reference to the CAP and therefore to remove the possibility of using certificates related thereto.

The same applies if the CA does not respect the rules of the CAP.

Principles of publication

The following stakeholders are permitted to make reference to the CAP (as well as any distinctive signs or other name):

- CAs and families of certificates listed as compliant with the CAP
- Application Issuers as part of a CAP member organisation

If necessary, an agreement will be provided for this purpose.

The CFONB website is the primary website for publishing:

- The CAP in its current version and its previous versions
- The list of rules Frameworks
- The list of CAP member organisations (referring to an application or a CA or a family of certificates listed as compliant)
- The list of applications that accept CAP certificates
- The list of CAs and families of certificates that are listed as CAP, and marketed
  - The minimum levels of security and quality of associated certificates (level 1, 2, 3)
  - A link to the CA's Certification Policy (signed by the CA to ensure its technical integrity)
- The list of representatives and their deputies:
  - Managers of the CAs and families of certificates listed as CAP compliant (one manager and one deputy per organisation)
  - Application Issuers

We will limit ourselves to publishing the correspondent's name and the email address of the CA manager and applications Issuer.

Principles of reimbursement

The work of the CAP Committee and CAP Registration Committee is not subject to any reimbursement:

- All audit expenses, if any are incurred, are borne by the organisation requesting accreditation.

Principles of renewing a CAP listing

CAP accreditation is issued for a period of **one year**.

Each year, before the accreditation's anniversary date, the CA must provide:

- a certificate of Professional Liability Insurance
- and
  - either a certificate of conformity corresponding to their rules framework
  - or a certificate showing a positive audit result for the CA with regards to the CAP rules Framework, if the CA is not issuing certificates based on recognised rules framework.

In the event that the rules Framework initially used by the CA has changed (e.g. a new OID), this does not involve a renewal. A new CAP accreditation request must be initiated.

The renewal application must be sent to the CAP Registration Committee by post, by completing a renewal request, together with the certificate as described above.

4. THE PRINCIPLES OF APPLYING FOR ACCREDITATION

Accreditation principles

Members of the CAP can be:

- Applications issuers that accept CAP certificates
- Certificate issuers for CAs and families of certificates declared compliant

Note that application Issuers and issuers of families of certificates listed as compliant can only claim compliance with the CAP for accredited applications or families of certificates.

Only the applications or families of certificates compliant with the CAP will be published on the CFONB website. Those that are not accredited cannot claim CAP compliance.

When joining the CAP, the applicant specifies the organisational scope concerned by the CAP in terms of subsidiaries, mutual benefit organisations, etc. A member organisation notifies the CAP Registration Committee in the event of any changes to its organisational scope or any corporate developments (e.g. change of name) that may impact compliance with the CAP.

Declaring an application's accreditation

CAP-listed certificates are used by Issuers of:

- Common applications in the French banking and financial sector
- Individual applications specific to a bank or financial institution declared as compliant
- Applications belonging to a category of applications declared as compliant

Any new application will be declared to the CAP Registration Committee which will update the list of applications that accept CAP certificates on the CFONB website.

An application can be declared as compliant at the request of an application Issuer:

- From the banking and financial sector in a country other than France
- Not from the banking or financial sector (French or other country)

This request will be presented to the CAP Registration Committee, which will study the quality of the category of applications, based on the principles set out above, and on the basis of a documentary review.

Accreditation of a family of certificates

In support of its accreditation of a family of certificates, the organisation presents the CAs and families of certificates that it intends to declare as compliant

These families of certificates:

- Comply with the PRIS/RGS
- Or have been analysed by an auditor accredited by a body such as COFRAC in France (www.cofrac.fr) or the European cooperation for Accreditation (EA).

  Outside of the above organisations, applications will be considered on a case-by-case basis.

The accreditation control process

Principles for submitting a request

The various documents produced for the accreditation request are written in French or English. In the event that the documents have been translated into English, it is requested that the quality of the translation be certified by an independent body recognised in its industry and with good knowledge of terminology used in the field of electronic certification.

Processes for submitting a request

The process for submitting a request is based on the following steps:

- Request formulated by compiling the following documents:
  - References for the family of certificates that the organisation wants to see accredited
  - The associated CPs
  - The associated rules Framework
- Request sent by the requesting entity to the CAP Registration Committee
- Acknowledgement of submission sent by the CAP Registration Committee
- For CAs that do not comply with the PRIS/RGS guidelines, an audit should be launched at the initiative of the organisation and under its responsibility (the quality of the audit and duration of the assignment are defined by the applicant without any commitment made by the CAP Registration Committee)
- Analysis of the request, using an audit report for CAs that do not comply with PRIS/RGS guidelines.

Analysis of the request

The accreditation request is made for:

- One or more certificate-issuing functions (one or more CA(s), one or more family/ies of certificates, level 1, 2 or 3 certificates) (certificate of compliance)
- One or more applications (declaration)

To start the process of accreditation, the organisation must submit:

- For a certificate issuer (see accreditation package available on the CFONB website):
  - The list of CAs and families of certificates
    - The associated CPs (and if necessary, the documents to which they refer)
    - Its positioning relative to the reference frameworks selected for CPs
    - Certificates which may have already been obtained from official bodies or auditors attesting the family of certificates' compliance with an audit framework
    - The financial guarantees associated with the certificates as specified in the CP, the associated insurance policies and any additional documents.

      The CAP Registration Committee analyses the physical existence of these documents and not their contents
    - The contact details of the correspondent and their deputy (name and email address)

- For an acceptor (application Issuer):
  - The categories of applications in question
  - The contact details of the correspondent (name and email address)

An organisation recognised as compliant (part of the CAP) must obtain approval from the CAP Registration Committee to include the following in its scope:

- A new CA or family of certificates
- A new category of applications

The detailed analysis of the applicant's Certification Policy is a key component of the membership process and associated accreditation form.

Audit costs are supported by the organisation applying for membership, when the CP is not compliant with the CAP framework (PRIS/RGS guidelines or approved equivalent) whether this be to assess the candidate's CP or to assess the reference CP to which its own CP refers.

The member agrees to adhere strictly to the framework of the CAP.

Solutions when a request is rejected

In the event that an organisation sees its request for accreditation rejected, it may resubmit its request after correcting the elements that led to its refusal.

The applicant is free to resubmit their request, explaining and highlighting the changes it has made in relation to its previous submission.

Managing changes

We must distinguish between changes made by:

- The CAP Committee which can change the CAP framework
- The organisation responsible for the application declared compliant or the CA or family of certificates deemed compliant

When the CAP Committee is responsible for a change, it is their role to define the level of change (minor, not requiring a new accreditation, or major, involving new accreditation of the CAs/families of certificates)

- In the event of changes to the CAP framework (for example, deleting a recognised standard, after a security failure), the CAP Registration Committee is required to notify the organisations certified as compliant with the CAP within an appropriate time limit. This time limit for the new policy should be long enough to enable the market to achieve compliance. Accredited organisations will need to align themselves with the new policy within the deadline set for its effective implementation.
- Organisations will present their accreditation request or renewal based on the new policy. The deadline for using the old policy will be specified at publication of the new policy, by the CAP Committee.

.

In the event of changes to the CAP, the CAP Committee, vis-à-vis the Officers of the CFONB board, is responsible for:

- Notifying it in the event of a minor change
- Requesting its approval, in the case of a major development

If the change is brought about by the member organisation, the latter is responsible for qualifying the level of change (minor or major, with a major development involving, among other things, a change to the OID of the CP associated with the CA or family of certificates)

When the member organisation is responsible for the change, the following must be taken into account:

- The shut-down of an application declared to be compliant or of a CA or family of certificates deemed compliant; the organisation shall notify the CAP Registration Committee three months before the cessation of activity, except in cases of *force* *majeure*. In the latter case, the organisation will make its 'best effort' to notify the CAP Registration Committee as soon as possible

- Minor changes (so with no OID change) to the operating conditions (technical and organisational) of a CA or application, without these modifications altering the PRIS/RGS framework (or reference to equivalent rules framework recognised by the CAP Committee as part of the CAP) or an application declared compliant; the organisation is not required to document or present these changes to the CAP Registration Committee

- Major changes (with an OID change) to the operating conditions (technical and organisational) of a CA or application, potentially impacting the PRIS/RGS framework (or reference to equivalent rules framework recognised by the CAP Committee as part of the CAP) or an application declared compliant; in the six months preceding these changes, the organisation is required to:
    - Report these changes to the CAP Registration Committee before any certificates are sent out with the new OID;
    - Request an updated end date for the validity of the accreditation for families of certificates with the former OID, specifying for how long this family[4] can be used (a reasonable period must be provided) **and** producing the certificate or audit report for the new family of certificates, to enable it to obtain a new CAP accreditation.

  The list of CAP-accredited families of certificates will be published with the history of all the OID versions that are still valid. During each family of certificates' period of validity (at least), the corresponding CP must be accessible online.

- Change to a third party framework recognised as compliant with the CAP:
    - If the security level of this framework remains at least same as the PRIS/RGS standard, the Issuer of this framework is simply required to notify the CAP Registration Committee of the changes
    - If the security level of this framework is no longer compatible with that of the PRIS/RGS, the organisation adhering to this framework shall:
        - Advise the CAP Registration Committee of these changes at least three months before the date of their effective implementation
        - Request the withdrawal of its accreditation or present its actions or reasons for keeping it.

Faced with these different situations, the CAP Registration Committee can:

- Maintain its accreditation;
- Withdraw it;
- Request an audit of the new framework, the cost of which will be borne by the organisation wishing to maintain its accreditation.

[4] The period of validity of a Certificate Authority must be at least equal to the lifespan of the most recent certificate issued by said CA.

Audit and review principles

In the event of a change to a CA that is already accredited, the principles of audit and review apply to the following parties:

- CFONB members
- Third parties not members of the CFONB

CFONB members

The monitoring of CAP implementation conditions is the responsibility of the General Inspection Department of each bank; the CFONB, as guarantor of the existence of the CAP, may request an opinion from the General Inspection of the participating bank regarding a specific incident or event.

Non-CFONB members

An audit or review procedure can be brought about at the request of the CAP Registration Committee following:

- A change to the member organisation's framework which might reduce the level of security to below the level defined by the framework.
- An incident:
  - Corrupt secret
  - Incidents involving organisational processes (registration, renewal, revocation, etc.)
  - Fraudulent use of a valid certificate in an application that accepts CAP certificates
  - Etc.

The audit/review process must respect the following principles:

- The organisation responsible for selecting an auditor that is accredited/recommended by a COFRAC-approved body or equivalent
- The scope of the analysis is defined according to the nature of the problem, by mutual agreement between the two parties
- Reports and records are written in French or English
- The CAP Registration Committee agrees to keep confidential any information obtained on the organisation, its applications, its CA or its families of certificates
- In all cases, audit costs are the responsibility of the organisation that is audited

Following the audit assignment, the auditor reports their findings to the audited organisation, which is responsible for forwarding them to the CAP Registration Committee.

A compliance process may be suggested by the organisation, including a schedule and a further audit procedure.

In the event of excessive deviations from the CAP framework (possibly after the organisation has attempted to correct these deviations), accreditation is withdrawn.

Referral to the CAP Committee

Any CAP member entity may call upon the CAP Committee and ask it to convene an emergency meeting of the CAP Registration Committee, particularly in the event of suspected fraud or embezzlement.

5. For organisations not part of the CAP

Organisations that are not recognised as CAP members are permitted to refer to the CAP, only in an acceptance capacity, i.e. in the role of application Issuer, provided that:

- The organisation very clearly and systematically states that it is not part of the CAP;
- Its applications accept all certificates from CAP-accredited CAs;
- The organisation agrees to comply with the changes to the CAP in terms of issuing functions: new accredited CA, withdrawal of a CA or a range of certificates, etc. Changes must be made within three months of publication of the new version of the CAP on the official websites;
- The organisation complies with the "Principles of Compliance" related to the CAP, both in terms of the application accepting certificates and the organisation itself;
- The organisation notifies the certificate issuer in the event of an incident;
- The organisation respects the intellectual property rights of the CAP.

Under no circumstances can an organisation that is not part of the CAP hold a member organisation liable, by referring to the CAP.

6. PRINCIPLES OF GOVERNANCE

The CFONB is responsible for the following tasks:

- Through the CAP Committee:
  - It guarantees the publication of the CAP and its changes
  - It publishes the CAP on its website
  - It reviews the CAP at least annually and, as required, updates it whenever necessary
  - It manages changes to the CAP (updates, publication, etc.)
- Through the CAP Registration Committee:
  - It publishes the list of accredited CAs and applications accepting CAP certificates
  - It promotes the CAP and, therefore:
    - Recognises the compliance of new applications
    - Certifies the compliance of CAs or families of certificates
  - It studies accreditation requests
  - It requests, where applicable, audits as part of the analysis phase for accreditation requests

The CFONB is in charge of intellectual property issues for the CAP and, in particular, of filing and protecting any distinctive signs or other denominations regarding the CAP (brand, "label", domain name, etc.).

Note that the CFONB is not in any way responsible:

- for compliance with the CAP on the part of organisations, applications, CAs or families of certificates recognised as compliant
- or for any direct or indirect consequences that may result from the above.

Auditors will be responsible for ensuring that the principles of the CAP are applied, either for an initial accreditation request or a renewal, or during a spot check. Audit costs are, in all cases, the responsibility of the entities audited.

As part of their responsibilities under the CAP, members of the CAP Committee and CAP Registration Committee, like those of the CFONB, are bound by an obligation of confidence.

7. APPENDIX 1: REVIEW OF THE CONTEXT

In this appendix, each following policy is positioned with respect to each other:

- The certification policy
- The acceptance policy
- The validation policy

The Certification Policy

The quality of a certificate is governed by the Certification Policy, defined by the Certificate Authority (CA) and with which it agrees to comply.

The CFONB has adopted the French Inter-Sectoral Security Standards Policy (PRIS/RGS), established by the French Government Department in consultation with stakeholders, as a common basis for the banking sector in terms of digital certificates, and particularly for establishing certification policies specific to each Financial Institution. This reference to the PRIS/RGS helps to build on work carried out and to provide for coexistence and consistency with trusted infrastructures set up as part of online services and the remote procedures of the French Government Department.

Note that the PRIS/RGS distinguishes between different types of certificates: identity certificates, signature certificates and encryption certificates.

Building on this rules Framework, each Financial Institution sets its own certification policy for which it is solely responsible.

The CAP defines three security levels for a certificate:

- Level 1, corresponding to a software certificate not necessarily submitted face to face
- Level 2, or "high", schematically corresponding to an authentication secret stored on a smart card or token, and involving a face-to-face interaction
- Level 3, or "qualified", for applications assuming a very high level of security and/or generally responding to strong legal constraints

The PRIS/RGS defines different levels of security based on the following criteria:

- The principles of certificate containment (software certificate or on a smart card)
- The principles of registration and distribution
- CA management principles
- The principles of publication and revocation
- The rules for managing revocation lists
- Security principles (in particular with regard to protecting the certificate authentication secret)

The quality of the certificate is defined by:

- Its security level (1, 2 or 3)
- The commitment made by the CA in the event of non-compliance with the principles of the Certification Policy (e.g. level of Professional RC)

The Acceptance Policy (AP)

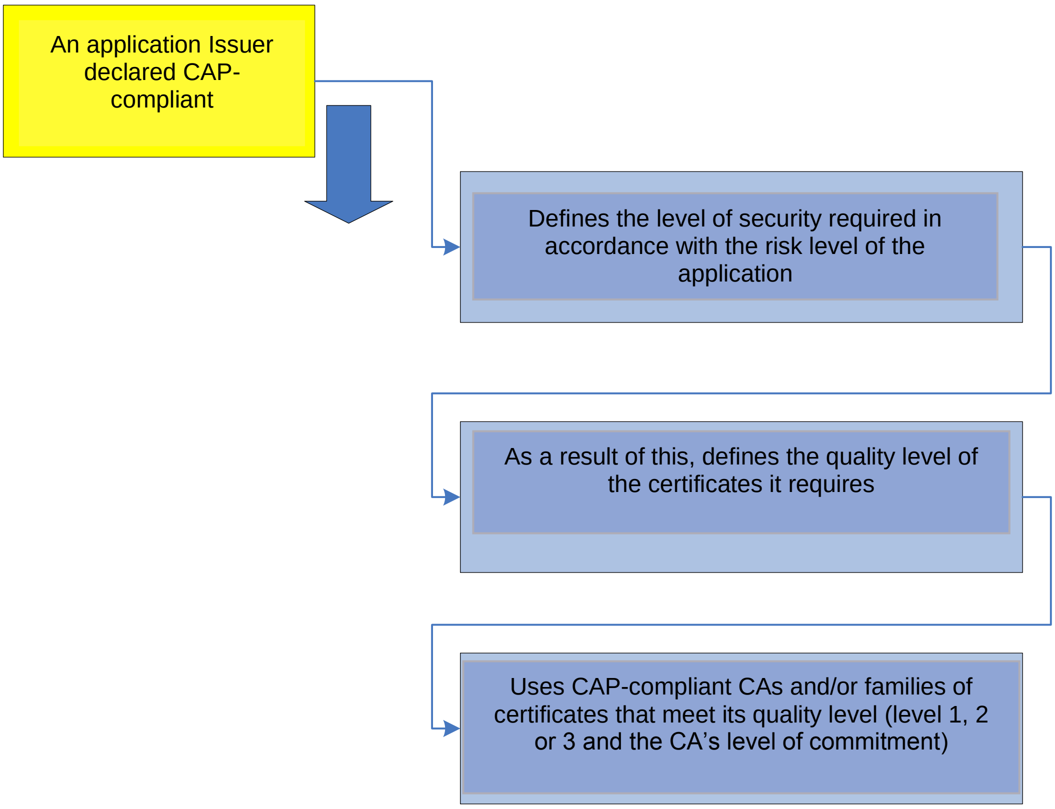
The certificates and associated dual keys will be used by applications to identify and authenticate their users in operations for controlling access or for checking the integrity of instructions received during electronic signatures. Depending on the level of risk accepted by an application, it is important to identify the parties involved to varying degrees and/or ensure a certain signature level and, therefore, to use certificates of an appropriate quality.

An acceptance policy defines the rules to be followed by a CA or a family of certificates so that its certificates can be accepted by an application.

An acceptance policy helps to demonstrate the compliance of families of certificates and to define their level of quality and security, as well as the compliance of any checks regarding the use of these certificates in the applications in question.

An acceptance policy addresses the needs of:

- Application Issuers, by allowing them to rely on CAs or families of certificates deemed compliant and to ensure a certain level of security in their services
- CAs and organisations issuing certificates, enabling them to create an environment multi-acceptance in which families of certificates accredited by the CAP are recognised by a set of applications held by the various parties involved
- Holders, who will naturally benefit from the creation of multi-acceptance environments


An application Issuer declared CAP-compliant
Defines the level of security required in accordance with the risk level of the application
As a result of this, defines the quality level of the certificates it requires
Uses CAP-compliant CAs and/or families of certificates that meet its quality level (level 1, 2 or 3 and the CA's level of commitment)

The Validation Policy

A validation policy is not limited to the principles of accepting a certificate; it must serve as a benchmark for the application to enable it to validate a transaction or operation, by extending the acceptance policy and helping put this into practice.

A movement or a transaction is validated, in particular, by performing the checks associated with the acceptance and validation policies. Verifying the CAP accreditation of the certificate used is implicit.

The respective scopes of the acceptance and validation policies

Schematically, the acceptance policy defines the criteria that certificates must fulfil, according to the level of quality sought, as well as the criteria to be met by the applications using these certificates.

The acceptance policy defines a reference framework for certificates and their uses, while the purpose of the validation policy is to define methods of implementing this acceptance policy (the 'how' as an extension of the 'what'), in another document.

The validation policy defines the various operations that need to be performed to ensure a certificate's quality and the level of compliance requested by the application for its accreditation. It comes into play

- once the family of certificates has been declared compliant with the CAP;
- for applications accepting CAP certificates.

The validation policy covers a wider scope than the one addressed by the acceptance policy, particularly when it comes to technical validation of the signature and management of evidence of checks carried out.

Control procedures	Acceptance Policy	Validation Policy	Application checks
Families of certificates used	X	X	(X)
Certificate template	X	X	
Validity date	X	X	
Key length	X	X	
Associated certification policy	X	X	
Level 1, 2 or 3	X	X	
Level of commitment of the issuer	X	X	
Revocation lists	X	X	
Key usage	X	X	
Signature		X	
Signature tools		X	
Signature validation tools		X	
Integrity of the signature		X	(X)
The family of certificates' compliance with the level required by the application		X	X
Rights, entitlements and limitations			X

8. APPENDIX 2: LIST OF KEY PUBLICATION WEBSITES

The reference website for the publication of the CAP is now the CFONB website: http://www.cfonb.org

The CFONB ensures that all topics related to the CAP are kept up to date on this site.

9. APPENDIX 3: TECHNICAL ITEMS USED FOR THE CAP

The PRIS/RGS is based on and specifies the requirements of the RFC3280, RFC2560, RFC3739, RFC3647, CWA14167-1 standards.

The following table lists items used to analyse the CAP compliance of CAs and families of certificates; the following have been identified:

- Items whose specifications are detailed in the PRIS/RGS
- Items whose specifications determine the security level of the certificate

Technical items		Definition under the PRIS/RGS	Depends on the certificate's level of technical security
Certificate profiles/CRL/OCSP and algorithms			
Certificate template			
	Format (X509)	yes	no
	Basic fields	yes	no
	Restrictions on identifiers (CA, holder, etc.)	yes	no
	Extensions	yes	no
	Type of certificate	yes	no
CRL format		yes	no
Online Certificate Status Protocol (OCSP)		yes-RFC 2560	no
Algorithms and key lengths		yes	yes
CP			
Definition of entities involved in the PKI		yes	no
Areas of use applicable/not allowed		yes	yes
CP management		yes	no
Principles of provision of information to be published		yes	yes
Identification and naming			
	Naming	yes	no
	Initial validation of the identity	yes	yes
	Identification and validation of a key renewal request	yes	yes
	Identification and validation of a revocation request	yes	yes

Technical elements		Definition under the PRIS/RGS	Impact on the certificate's level of technical security
The operational requirements of the certificate life cycle			
	Certificate request	yes	yes
	Processing a certificate request	yes	no
	Issuing the certificate	yes	yes
	Acceptance of the certificate	yes	yes
	Use of the dual key and certificate	yes	yes
	Renewal of a certificate	yes	no
	Issuance of a new certificate after changing the dual key	yes	yes
	Amending a certificate	yes	no
	Revocation and suspension of certificates	yes	yes
	Function giving information on the status of certificates	yes	no
	End of the relationship between the holder and the CA	yes	no
Non-technical security measures			
	Physical security measure	yes	yes
	Procedural security measures	yes	yes
	Security measures vis-à-vis staff	yes	no
	Data archiving	yes	no
	Changing CA keys	yes	no
	Recovery after a compromise and sinister	yes	no
	End of life of the PKI	yes	no

Technical elements		Definition under the PRIS/RGS	Impact on the certificate's level of technical security
Technical security measures			
	Generation and installation of dual keys	yes	yes
	Protecting private keys and cryptographic modules	yes	yes
	Managing dual keys	yes	no
	Activation data	yes	no
	Information systems security	yes	yes
	Security of systems during their life cycle	yes	no
	Network security	yes	no
	Time-stamp/ system of dating	yes	no
Compliance audits and other assessments			
	Frequency and/or circumstances of assessments	yes	no
	Identities/qualifications of assessors	yes	no
	Relations between the assessors and entities assessed	yes	no
	Topics covered by assessments	yes	no
	Actions taken in response to assessment findings	yes	no
	Communication of results	yes	no

Technical elements		Definition under the PRIS/RGS	Impact on the certificate's level of technical security
Legal and business issues			
	Price list	no	no
	Financial responsibility	no	no
	Confidentiality of business data	yes	no
	Privacy	yes	no
	Law on intellectual and industrial property	no	no
	Contractual interpretations and guarantees	yes	no
	Limit of guarantees	no	no
	Limit of liability	no	no
	Duration and early termination of the CP's validity	yes	no
	Amendments to the CP	yes	no
	Provisions regarding conflict resolution	no	no
	Competent courts	no	no
	Compliance with laws and regulations	no	no
	Miscellaneous provisions	no	no
	Other provisions	no	no
Security requirements of the CA's cryptographic module			
Requirements regarding security objectives		yes	yes
Requirements regarding certification		yes	yes
Security requirements of the authentication and signature device			
Requirements regarding security objectives		yes	no
Requirements regarding certification		yes	yes

10. Appendix 4: Requirements related to a certificate's quality level

The requirements regarding the security levels of certificates are defined by the banking sector, with reference to the PRIS/RGS star rating; they are listed in the table below:

Field	Level 1	Level 2	Level 3
Initial validation of the holder's identity	Registration request sent in paper form (with a photocopy of identity documents) or electronically (e.g. signature with a certificate and a ** tool) or communication of something specific to the future holder in order to identify them in a pre-established administrative database (1)	Identity check • face to face • with an electronic signature at least ** level but preferably *** level (recommended)	Identity check • face to face only
Handover/acceptance of a certificate	❑ Submitted by email ❑ Tacit acceptance	❑ Face-to-face handover if authentication of the holder is done face to face and did not take place during registration ❑ If possible, explicit acceptance of the certificate by the holder ❑ As a minimum, tacit acceptance from a sufficiently reliable handover date	❑ Face-to-face handover if authentication of the holder is done face to face and did not take place during registration ❑ If the CA doesn't generate the dual key, verification that the certificate is indeed associated with the corresponding private key (remote loading on a smart card or token) ❑ Explicit acceptance of the certificate by the holder

Field	Level 1	Level 2	Level 3
Revocation of a certificate	❑ Authentication of the request by checking one or two basic details about the requesting party (telephone number, address, etc.) (2) ❑ Service available at least on working days, with a maximum of 16 (working) hours of downtime per month ❑ Time between validation of the request and the update of status information of less than one working day	❑ Formal authentication of the request (e.g. a series of a few questions/answers (3/4) to remove any doubt, use of a certificate and a * tool...) ❑ Service available 24/7, with a maximum of 4 hours' downtime per month ❑ Time between validation of the request and the update of status information of less than one working day	❑ Formal authentication of the request (e.g. a series of a few questions/answers (4/5) to remove any doubt, use of a certificate and a * tool **…) ❑ Service available 24/7, with a maximum of 2 hours' downtime per month ❑ Time between validation of the request and the update of status information of less than 24 hours, 7 days a week
Certificate status service	❑ As a minimum, publication of the CRL. Recommendation of an online service (OCSP) ❑ Service available on working days, with a maximum of 32 (working) hours of downtime per month	❑ As a minimum, publication of the CRL. Recommendation of the implementation of delta CRLs and an online service (OCSP) ❑ Service available 24/7, with no more than 8 (working) hours of downtime per month	❑ As a minimum, publication of the CRL. Recommendation of the implementation of delta CRLs and an online service (OCSP) ❑ Service available 24/7, with no more than 4 (working) hours of downtime per month

Field	Level 1	Level 2	Level 3
Protection of CA keys (private/public)	❑ Generation and implementation of keys and CA certificates in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard ❑ Key ceremony by at least one person in a trusted role ❑ Activation of CA private keys by at least one person in a trusted role	❑ Generation and implementation of keys and CA certificates in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard, certified to a level equivalent to EAL2+ and qualified as at least corresponding to a standard level ❑ Key ceremony by at least two people (in a trusted role) and at least one external control ❑ Check of CA private keys by at least two people in trusted roles (authentication secret shareholders) ❑ Activation of CA private keys by at least one person in a trusted role	❑ Generation and implementation of keys and CA certificates in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard, certified to a level equivalent to EAL4+ and qualified as corresponding to a reinforced assurance level ❑ Key ceremony by at least two people (in a trusted role) and at least two external controls (including a recommended public official) ❑ Check of CA private keys by at least two people in trusted roles (authentication secret shareholders) ❑ Activation of CA private keys by at least two people in a trusted role
Private keys generation for holders (if they are generated by the CA outside of the holder's signature creation device)	Generation in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard (Cryptographic Key Management)	Generation in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard, certified to a level equivalent to EAL2+ and qualified as corresponding at least to a standard level	Generation in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard, certified to a level equivalent to EAL4+ and qualified as corresponding to a reinforced assurance level

(1) : In the case of the CAP, registration of the holder in a pre-established database should be understood to mean registration of the holder in a reference database of a CAP member organisation

(2) In the case of an identity certificate, the following checks must be taken into account:

Field	Level 1	Level 2	Level 3
Authentication device	Statement of compliance with the requirements	EAL2+ certification leading to a standard qualification	EAL4+ certification preferably leading to reinforced assurance qualification

In the event of a signature certificate, the following checks must be taken into account:

Field	Level 1	Level 2	Level 3
Signature creation device	Statement of compliance with the requirements	EAL2+ certification leading to a standard qualification	EAL4 certification preferably leading to reinforced assurance qualification

11. APPENDIX 5: THE CHARACTERISTICS OF CERTIFICATES BASED ON THEIR SECURITY LEVEL

The security level of a certificate is dependent both on the certificate and the process of creating the certificate, which depends on the PKI.

Criteria directly linked to certificates with reference to the PRIS/RGS.

Field	Level 1	Level 2	Level 3
Generation of holders' private keys by CA outside of the holders' device	Generation in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard	Generation in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard, certified to a level equivalent to EAL2+ and qualified as corresponding at least to a standard level	Generation in a cryptographic module that meets the requirements of Appendix B2 of the RGS standard, certified to a level equivalent to EAL4+ and qualified as corresponding to a reinforced assurance level
RSA key size of the holder certificate	❑ RSA: 1024 or 2048 ❑ DSA: 1024/q=160 or 2048/q=256	❑ RSA: 2048[5*] ❑ DSA: 1024/q=256 or 2048/q=256	❑ RSA: 2048 ❑ DSA: 2048/q = 256
The holder's device	❑ The device may be software ❑ Statement of compliance with the requirements	❑ Hardware device ❑ EAL2+ certification leading to a standard qualification	❑ Hardware device ❑ EAL4+ certification preferably leading to reinforced assurance qualification

Note that in the French RGS standard, Appendix B1 on "Cryptographic Mechanisms", page 15, the rule "RégleFact-1" states that the keys should have a minimum length of 2048 bits until 2020 and 4096 bits beyond this date.

[5] The use of a key length of 1024 bits is tolerated for certificates already issued until they are renewed

Criteria related to the quality of PKI processes

	Level 1	Level 2	Level 3
Initial identity validation	❑ Sending of a paper request ❑ Request for registration signed by the holder with 2-star quality tools ❑ Communication of something specific to the future holder to identify them within a pre-established database	❑ Physical face-to-face interaction ❑ Method providing an equivalent degree of assurance	Same as level 2
Identification and validation of a revocation request	Verification of the identity of the applicant and their authority regarding the certificate to be revoked ❑ One or two basic details	Verification of the identity of the applicant and their authority regarding the certificate to be revoked ❑ Series of at least 3 or 4 questions/answers on information specific to the applicant ❑ Online authentication using tools qualified as at least level 1 ❑ Electronic signature using tools qualified as at least level 1	Same as level 2
Issuing the certificate	Electronic transmission	Face-to-face handover if a face-to-face meeting did not take place earlier in the life cycle of the certificate	Same as level 2
Acceptance of the certificate	Tacit acceptance after sending the certificate	Confirmation of acceptance of the certificate by the holder, if possible explicitly in the form of a signed agreement (paper or electronic)	Same as level 2

Furthermore, the quality of the certificate depends on:

- The CRL publication frequency
- Physical security measures (control of access to resources)
- Off-site backup
- The distribution of roles between stakeholders in charge of the PKI
- Security measures implemented for protecting private keys and for cryptographic modules
- Security requirements of the CA's cryptographic module.

12. Appendix 6: Respective positioning of the CAP and the PRIS/RGS frameworks

The CAP defines technical, organisational and regulatory requirements for the banking industry to meet the needs of banking applications.

It was also decided to remain compatible, as far as France is concerned, with the Government Department's rules Frameworks, which are:

- The PRIS since 2004, still operational for certificates issued until May 2013 with a validity up to May 2016.
- The RGS 1.0 since May 2010, which is recognised by decree as the Government Department framework in force in France.

For existing Government Department applications, a transitional three-year period has been defined by the French Government Department to take account of these developments.

The current situation means that existing Government Department applications, as well as those of banks, can accept PRIS-accredited certificates.

Since May 2013, new banking applications must accept the certificates accredited by the RGS1.0.

For an application to comply with the CAP, it must accept all CAP certificates that offer the level required by its risk analysis.

Currently the CAP is based on the two standards of the French Government Department.

The CAP may have additional requirements in relation to these two frameworks.

When a family of certificates changes from the PRIS framework to the RGS framework, a CAP accreditation request must be initiated.

Differences between the CAP and the PRIS standard:

- The PRIS standards authorises certificates using both electronic and physical means, whereas the CAP requires physical means for Level 2;
- Professional Liability insurance for which the minimum amount of coverage required is specified in the accreditation request.

Differences between the CAP and the RGS standard:

- The RGS supports the SHA 256 and SHA 1 algorithm. Whole stock of client workstations is now compatible with SHA 256, with minimal key length set at 2048 bits;
- Professional Liability insurance for which the minimum amount of coverage required is specified in the accreditation request.

The use of the PRIS or RGS framework simplifies the CAP accreditation process, since the PRIS or RGS accreditation and renewal audits are accepted by the CAP. In other words, it is not necessary to do a second audit for the CAP.

The differences are small enough to be observed and tested, it is not necessary to carry out an additional audit.

A framework is never imposed. CAP accreditation can be carried out either using another framework, or without a prior framework.

The PRIS/RGS and CAP accreditations are independent from one another:

- CAP accreditation does not lead to PRIS or RGS accreditation
- PRIS or RGS accreditation does not lead to CAP accreditation.

All accreditations must be requested explicitly by submitting a request.

13. APPENDIX 7: CHECKS TO BE MADE ON THE CERTIFICATE AS PART OF THE CAP

The CAP requires the following to be checked:

- The certificate template
- Basic fields
- Identifications
- The extensions (presence is mandatory, criticality)
- Algorithms
- Key lengths
- Revocation Lists/Online Certificate Status Protocol (OCSP)
- Families of certificates
- The CA hierarchy to which the family of certificates is attached
- Authority Revocation Lists (ARL)

The CAP does not take into account the following security measures:

- Protection against viruses, worms, Trojan horse, etc. with regular updates
- Control and limitation of exchanges between the host machine and other machines in an open network
- Restriction, where possible, of access to the machine functions to their administrators (differentiation between user/administrator account)
- Installation and updating of software and components on the machine under the control of the administrator
- Refusal by the computer or terminal's operating system to run downloaded applications that do not come from reliable sources
- Updating software components and systems when provided with security updates for these
- Use of a reader with built-in pin-pad as part of a level 3 signature.

14. APPENDIX 8 RULES FRAMEWORKS

The CAP, in its present form, has been established on the basis of a version of the PRIS/RGS, which the CAP Registration Committee has in its possession. For more information on these documents, requests must be made to the CAP Committee or CAP Registration Committee.

As shown in the paragraph 3 of this document, other standard frameworks, especially those in place in other countries, may be accepted by the CAP committee.

Acceptance of these standard frameworks means they must undergo independent accreditation audits carried out by audit firms recognised by the COFRAC or equivalent body.

15. Appendix 9: Other reference documents

The CAP is based on the following documents:

- French Inter-Sectoral Security Standards Policy:
  - Preamble
  - Example Certification Policies - Certificate profiles/CRLs/OCSP
  - Authentication and Signature Service: Example Certification Policy

- General Security Requirements:
  - General Presentation of the RGS,
  - Example Certificate Policies and time variables,
  - Certificate profiles, CRLs, OCSP and cryptographic algorithms,
  - Versions with updates' log.

- 'CB' Groupement des Cartes Bancaires Acceptance Policy
  OID: 1.2.250.1.79.8.1

- Banks' proposals regarding use of the X509 certificate fields

In addition, the CAP Committee has provided a series of Frequently Asked Questions (FAQs), published on the CFONB website, including details of the framework version numbers.