CFONB

Comité Français d'Organisation et de Normalisation Bancaires

FAQs, Frequently Asked Questions about the Common Acceptance Policy

CAP

Ref. : Version 1.1 En

Contents

1 Purpose of the CAP

1.1 What is the purpose of the CAP?

In order to create an environment of trust and to encourage the use of electronic signatures by customers in banking applications, the Common Acceptance Policy enables:

- a Certificate Authority to follow a set of rules so that its certificates can be accepted by applications from the banking community;
- an application to declare itself part of the CAP, setting the level(s) of risks it agrees to incur, and thus validating the use of any associated CAP certificates.

1.2 What is the role of the CAP?

The CAP provides the banking community with a set of common quality and security criteria for families of certificates likely to used by a banking application. The CAP offers a classification based on three levels related to management of the risk borne by the user applications. The criteria are of a technical and legal nature and specify the respective obligations and responsibilities of the various parties involved (CA, application manager, users, etc.).

1.3 How many security levels are there in the CAP?

The security levels range from 1 to 3. To ensure consistency with other systems, they correspond with the 1, 2 and 3-star levels set out in the RGS (French General Security Requirements) and until May 2013 in the PRIS (Inter-sectoral Security Standards Policy), published by the French Government, with certificates for the latter valid until 19 May 2016.
In the policy, it explains the regulatory framework used as a basis for accrediting a family of certificates.

1.4 How do we integrate new regulatory frameworks and position them within the CAP's three security levels?

Each level of a new framework is compared to those of the CAP to ensure they correspond to the level immediately below or equal to that of the CAP. In this context, a framework's level can be rejected, if it proves to be below the minimum level of the CAP.

2 CAP and Multi-Acceptance

2.1 What is Multi-Acceptance?

Multi-acceptance is the recognition by a banking application of certificates from different certificate authorities which can then become interoperable with said application.
It is therefore the option, and not the obligation, given to banking applications, of accepting certificates for which interoperability is ensured through compliance with CAP criteria (security, technical, legal and responsibility of the parties, including financial responsibility).

2.2 What are the benefits of Multi-Acceptance?

- Using the same certificate across multiple banking applications with compatible security requirements.
- Solving the problem of conflicts related to the installation of several certification methods on the same workstation.
- Solving the problem of choosing which certificate to use in the case of one holder with multiple certificates.
- Promoting multi-banking among customers by providing access to banking applications through a single certificate.
- Freedom of choice for the customer within a CAP certificate level.

2.3 What is the role of the CAP in Multi-Acceptance?

The CAP is the reference document for interoperability criteria favouring Multi-Acceptance for banking applications.

3 The role of regulatory frameworks in the CAP

3.1 What is a framework?

A certification framework is a set of standard documents and security best practices that can be suggested by governments or public or private organisations or communities.
In France, the PRIS and the RGS are promoted by the French government under the control of the ANSSI (French National Computer Security Agency).

3.2 Why is the CAP based on a regulatory framework?

This helps streamline the CAP's accreditation procedures for families of certificates by using the qualifications obtained by processes already in place for this framework.

3.3 Why is the CAP based on the "PRIS/RGS" framework?

The PRIS/RGS is a known and trusted environment used by a high number of Certificate Authorities in the market (compatibility with Government applications). The in-depth analysis of this framework has shown that it is also suited to banking applications (see press release)

3.4 How does the CAP differ from the PRIS/RGS?

Mere correspondence with the French Government's PRIS/RGS frameworks, in terms of security requirements, is not the only criterion used to ensure compliance with the CAP. The CAP can also be used for:

- families of certificates that comply with standards other than PRIS/RGS frameworks, French or otherwise,
- families of certificates whose Certification Policy is not based on a framework, as long as the quality and security level of these families can be matched with a level defined in the CAP.

The CAP is based on frameworks and, where applicable, adds criteria to create the desired environment of trust. The use of existing frameworks aims to facilitate the CAP accreditation procedure.

3.5 What frameworks are currently used by the CAP?

At the time of publishing these FAQs, the CAP has accredited families of certificates based on the following frameworks:

- PRIS V1;
- V2.3 of RGS 1.0.

3.6 Why this dual PRIS/RGS standard?

Since February 2010, the date of the "RGS" decree, the RGS has become the benchmark of the French Government in this matter. The continued reference to the PRIS system is due to the fact that some PRIS certificates are valid until 19 May 2016.

3.7 Will the CAP be compatible with eIDAS Regulations?

The plan is to review the CAP once all the implementing acts of the eIDAS regulation have been published. In any event, the eIDAS regulation will not come into force before 1st July 2016.

4 The CAP and banking applications

4.1 What can the CAP do for banking applications?

The CAP allows banking applications to facilitate management of their trusted environment. Indeed, after performing their risk analysis, they can choose the appropriate certificate level.

4.2 What commitments do banking applications have with regard to the CAP?

Banking institutions are not required to get their applications qualified by the CAP. Each is free choose whether or not to use CAP qualified certificates in their applications.

4.3 Is there a requirement to conduct a security risk analysis for applications?

No, but this procedure is recommended as good practice to help choose the appropriate level of certification for the application.

4.4 What happens if a CAP family of certificates is no longer operational?

A family is no longer operational when the CA goes out of business following a compromise, or due to a business decision. With the CAP, customers can then choose an alternative solution from the list of families with an equivalent level.

4.5 EPC-approved CAs and Trusted List

In the context of payment services (e-mandates, SEPA e-payment), server certificates are implemented in message exchanges. These certificates meet the requirements set by the EPC and are published in the EPC Trusted List of Approved CAs. Qualification for this list relies on the approval of the Certificate Authority Approval Panel (CAAP).
The process developed by the EPC is similar to the one offered by the CAP in the French banking community but, for the time being, is reserved for server certificates only.

4.6 Where to find CAP certificates compatible with the technical requirements of the EBICS TS

The list of certificates compatible with the technical requirements of the EBICS TS (CAP and non-CAP) can be found on the CFONB website in the section on documents/organisation of exchanges/communication protocols

4.7 Does a family of CAP certificates also have to be PRIS/RGS?

No, this is not necessary. CAP certificate families can rely on a different framework to the PRIS or RGS, or have no designated framework.

4.8 Is a PRIS/RGS certificate family automatically CAP?

No, because the CAP is not just a technical requirement, and a CA could be technically compatible but fail to meet the other CAP criteria.

4.9 How to achieve CAP accreditation outside of the PRIS/RGS

A CAP accreditation request is identical and compulsory for all families of certificates.
If an existing framework is used, the audit report for this framework can be used for the CAP accreditation request.

4.10 How to do a CAP accreditation audit when the family of certificates concerned is not based on an existing framework

In this case, the audit process, necessarily conducted by an accredited organisation, such as COFRAC in France, must be based on the characteristics of the CAP, as well as the frameworks on which the CAP is based.

4.11 Can other frameworks be used?

Yes, any framework compatible with the characteristics of the CAP can be used as a basis for auditing families of certificates that rely on these standards, whatever their geographical origin and/or sector. Today, the PRIS/RGS frameworks are used in France.

4.12 Should all documents produced necessarily be written in French?

No, they can be written in or translated into French or English.

5 The Acceptance Policy and Common principles for validating electronic certificates and signatures

5.1 What is the role of the certificate validation guide?

The guide to common principles for validating certificates and electronic signatures has been developed by the French banking community for banking applications.
It defines the principles of verification of an electronic signature and/or electronic certificate. During the signature verification phase of the audit, evidence of this verification is produced and archived with the implementation of a time-stamp. Verification is carried out either directly by the application, or by a dedicated server shared across all applications.
The guide is based on the application's signature policy for verifying the signature.
The guide is based on an acceptance policy or on one or more certification policies for validating certificates.
In addition, the guide may refer to time-stamp and archiving policies.

5.2 Do all banking applications have to follow the recommendations of the guide to common principles of validation?

No, because this guide is not mandatory.

5.3 Does the CAP always require a guide to common principles of validation?

No, the guide is complementary to the CAP. A banking application can accept CAP certificates and apply a different validation policy to the guide to common principles of validation.

5.4 Does the guide to common principles of validation only apply to CAP certificates?

No, the guide to common principles of validation can be applied to any family of certificates accepted by a banking application.

6 Publication of CAs

6.1 Are all CAP-compliant families of certificates included in the list?

To be included in the list, a family of certificates must meet the requirements of the CAP, and have been the subject of an accreditation request made to the CAP Registration Committee by the manager of the CA. So if a CA does not follow this approach, a family of certificates can be compatible but not be in the list.

6.2 How to find the right certificates for using an application?

Using a risk analysis, the application defines the minimum level of certificate that can be used by customers. There is a list of CAP certificates by level.

7 Publication of applications

7.1 Are all applications that accept CAP certificates included in the list?

As the procedure for publishing applications is declarative, the only applications published are those that have taken this step, so they are not all there.

7.2 Are banking applications required to be CAP-accredited?

No, banking applications and banking institutions have no obligations regarding the CAP. A bank is free to decide whether or not to get its applications listed. A banking application declared as CAP-accredited gives visibility to the certificates that may be used.

7.3 Can a banking application that uses CAP certificates also use other certificates?

Of course, the CAP certificates are not exclusive. An application can decide, depending on the level of associated risk, to accept other certificates or other authentication or signature systems.