Payment Credential Ecosystem and PEMKey – Questions and Answers

Positioning note: PEMKey is the programme responsible for delivering the Payment Credential Ecosystem (PCE). The PCE helps enable trusted participation in digital payments through verifiable digital credentials. It allows people and organisations to securely share verified information when needed, reducing fraud and improving inclusion in digital payment services.

Content

1. What this is

1.1 What is the PCE?

The Payment Credential Ecosystem (PCE) helps enable trusted participation in digital payments through verifiable digital credentials. It allows people and organisations to securely share verified information when needed, reducing fraud and improving inclusion in digital payment services.

Trusted information can be shared when needed without requiring every organisation to integrate directly with one another or repeatedly request copies of physical documents.

The purpose of the PCE is to make digital payments safer, more inclusive and more trusted.

1.2 What problem is the PCE trying to solve?

The PCE is focused on supporting safer and more inclusive digital payments.

- **Inclusion:** Many people experience barriers when accessing digital payment services as they cannot easily demonstrate the information required for onboarding or participation. The PCE supports trusted digital credentials that can help make participation more accessible.
- **Safety and fraud prevention:** The PCE supports trusted digital proofs that help payment service providers verify participants and reduce certain types of fraud while maintaining privacy and user control.

In simple terms, PCE helps create a safer and more trusted environment for digital payments by enabling verified digital credentials to be used when participating in payment services.

2. What PCE is not

2.1 How does the PCE co-exist with trusted authorities?

The PCE provides the ecosystem through which authoritative organisations can issue trusted digital credentials to individuals. It builds upon trust already established by foundational credentials and trusted authorities.

2.2 Where is information stored within the PCE?

Credentials remain under the control of individuals and are not stored in a central repository by the PCE. The ecosystem may require shared services such as registries and verification services. However, these are not intended to create a national database of personal information, identity records or payment activity.

3. How the PCE works

3.1 Where do my credentials come from?

- Trusted institutions issue digital credentials directly to individuals.
- Credentials are envisaged to be provided by payment service providers and other authorised participants.
- The ecosystem may also support additional credential types beyond digital payments, enabling innovation in other areas (for example, loyalty programmes).
- Credentials are stored in a digital wallet controlled by the individual.

3.2 What role does PCE play?

The PCE provides a trust and verification ecosystem that allows credentials to be checked safely during onboarding and digital payments. It supports trusted interactions between credential issuers, credential holders and organisations that need to verify information.

4. Privacy and control

4.1 Who controls my information?

You do. Credentials sit in your own digital wallet. You choose what information to share, who to share it with and when.

4.2 Can I share only part of my information?

Yes. PCE supports data minimisation. For example, you could prove that you are over 18 without sharing your full date of birth.

5. Security and fraud prevention

5.1 How is the PCE more secure than the current systems?

The PCE supports stronger assurance through cryptographic protections, credential verification and controls implemented by participating organisations. These measures help reduce fraud and decrease the need to repeatedly exchange or store sensitive documents. In simple terms, using proven digital credential technology makes digital payments more secure and puts you in control of your information.

5.2 Does the PCE make fraud or crime easier?

No, it does not. The PEC is meant to have the opposite effect. By linking payment participation to verified individuals, it makes fraud more difficult to commit and easier to detect. The ecosystem may also support mechanisms that assist in identifying compromised, revoked or fraudulent participation while maintaining privacy controls.

5.3 Does the PCE replace law enforcement or banking controls?

No. It strengthens and complements existing fraud prevention and law enforcement measures.

6. Revocation and lost devices

6.1 Can credentials be cancelled or revoked?

Yes. Credentials can be revoked immediately by the issuing institution and validity can be checked at the point of use.

6.2 What happens if I lose my phone?

You will not be permanently locked out. After secure re-verification, credentials can be reissued into a new digital wallet, like replacing a lost physical wallet. Where supported by participating issuers and wallet providers, replacement and recovery processes may be completed remotely.

7. Inclusion and access

7.1 Who will be able to use the PCE?

The PCE will be introduced in phases. Initially, it will support people who can be verified through existing trusted systems. Over time and as regulations allow, broader participation will be enabled.

7.2 What about foreign nationals or undocumented people?

The PCE is intended to support participation in digital payments, in a manner that is consistent with applicable legal and regulatory requirements, while enabling proportionate inclusion and appropriate safeguards for different categories of participants.

7.3 What if I do not have an appropriate device or phone?

The PCE is designed to support alternative access options, including kiosks and physical payment credential card options. It is also exploring ways to make capable devices a realistic option for everyone.

8. Choice and compulsion

8.1 Is the PCE compulsory?

No. Cash remains valid and participation in the PCE is not envisaged to be mandatory for all electronic activities. The PCE is positioned to support specific fast digital payment services by helping ensure that faster and more accessible payments do not translate into increased opportunities for fraud. It does this through verifiable digital credentials and associated trust services.

9. Surveillance concerns

9.1 Does the PCE track or monitor spending?

No. The PCE is not designed to track spending behaviour, monitor how people use their money or build behavioural profiles. The PCE is used only when a person chooses to be onboarded to a payment-related service or, in certain cases, when making or receiving digital payments. The purpose for which personal information is used will be clearly disclosed and information will only be shared with authorised parties, in accordance with applicable rules and consent requirements.

10. The PEC in simple terms

10.1 What does PCE really do?

PCE supports the use of digital credentials in digital payments. It provides a trust framework that enables participating organisations to issue, verify and rely on digital credentials when onboarding customers and enabling payment services.

In simple terms, it enables people and organisations to share verified information more safely, efficiently and with greater control, without requiring direct integration between all parties or clients repeated exchange of document copies.