Payment Card Industry 3-D Secure Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK

In a 3-D Secure payment transaction flow, the 3DS SDK processes plain text account data and cardholder authentication data.

There is an approval program for 3DS SDKs which is focused on interoperability and correct operation. But what about security?

Is the 3DS SDK subjected to PCI DSS, PCI PA-DSS or PCI P2PE requirements?

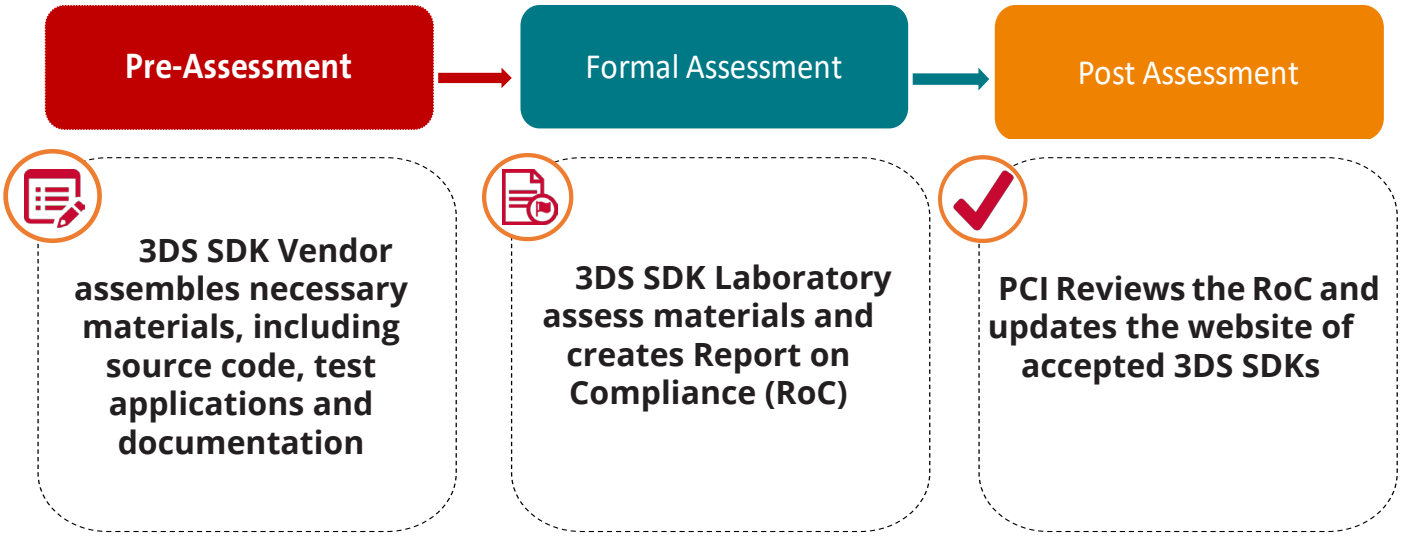
PCI has developed a set of security requirements specific to 3DS SDKs (Payment Card Industry 3-D Secure (PCI 3DS) Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK) and a corresponding approval program (Payment Card Industry EMV® 3-D Secure 3DS SDK Program Guide).

What does the PCI 3DS SDK Security Requirements Cover?

- Protection of cardholder data and reference data
- Minimal storage of sensitive data
- Integrity checks on the application and platform
- Resistance against reverse engineering
- Mitigations on side channel leakage of sensitive information
- Correct use of PCI approved cryptography

Payment Card Industry 3-D Secure Security Requirements and Assessment Procedures for EMV® 3-D Secure SDK

UL can support you at each stage of the evaluation process to optimize performance and efficiency.



UL Helps with

- ✓ On-site workshops addressing the requirements and to prepare for a formal evaluation.
- ✓ Gap analysis to identify potential design issues, scoping challenges or insufficient documentation.

- ✓ Full evaluation with a Report on Validation (RoV) and an Attestation of Compliance (AoC).

- ✓ Delta evaluations in the event of changes to the SDK software, vendor name or branding

To find out more about UL's services or to speak to an UL expert, go to **UL.COM**