Payment Card Industry
3-D Secure (PCI 3DS)

PCI 3DS Data Matrix
For use with PCI 3DS Core Security Standard v1.0

Version 1.1

October 2019

Document Changes

Date	Version	Description
October 2017	1.0	Initial release of the PCI 3DS Data Matrix 1.0 for use with PCI 3DS Core Security Standard v1.0.
October 2019	1.1	Updated footnote for *Table 1: 3DS Sensitive Data,* to clarify the permitted temporary storage of the Authentication Value by the 3DSS.

Introduction

This data matrix describes a number of data elements common to 3DS transactions and is intended for the following 3DS entities: 3DS Server (3DSS), 3DS Directory Server (DS), and 3DS Access Control Server (ACS). The information in this document is intended for use with the *PCI 3DS Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* (PCI 3DS Core Security Standard).

This document is organized as follows:

- **Table 1: 3DS Sensitive Data** – A subset of data elements from the *EMV® 3-D Secure Protocol and Core Functions Specification* that are subject to specific requirements in the PCI 3DS Core Security Standard.
- **Table 2**: **3DS Cryptographic Keys with HSM Requirements** – A subset of cryptographic key types from the *EMV® 3-D Secure Protocol and Core Functions Specification* that are required to be generated and stored in an HSM.

Table 1 identifies storage permissions for the applicable data elements. Table 2 identifies 3DS cryptographic key types with HSM requirements.

Note: *If PCI Account Data is present, this data would need to be protected in accordance with PCI DSS. Refer to Appendix B of the PCI 3DS Core Security Standard for guidance on PCI DSS applicability.*

Table 1: 3DS Sensitive Data

The data elements identified in Table 1 are subject to PCI 3DS Core Security Standard requirements that apply to 3DS sensitive data.

Data elements defined in the *EMV® 3-D Secure Protocol and Core Functions Specification* that are not included in Table 1 are not currently subject to the PCI 3DS Core Security Standard. Such data elements should be evaluated to determine sensitivity and be protected accordingly, as defined by the 3DS entity's risk-management policy.

CATEGORY	3DS Data Element	Description	Storage Permitted		
			3DSS	DS	ACS
3DS Authentication Data	Authentication Value	A cryptographic value generated by the ACS to provide a way, during authorisation processing, for the authorisation system to validate the integrity of the authentication result. The AV algorithm is defined by each Payment System.	Temp[1]	Yes	Yes
	Device Information	Device information gathered by the 3DS SDK from a Consumer Device. This is JSON name value pairs that as a whole is Base64 encoded. Only appears as clear text under this data element name in AReq between DS and ACS.	N/A	Yes	Yes
	SDK Encrypted Data	Device Information in encrypted form as it appears between SDK and DS. Not in itself sensitive, other than the context that it contains Device Information. No value for 3DS Server to log or store.	No	No[2]	N/A
Public Key Data	ACS Ephemeral Public Key (QT)	Public key component of the ephemeral key pair (dT, QT) generated by the ACS and used to establish session keys between the 3DS SDK and the ACS.	No	No	No
	SDK Ephemeral Public Key (Qc)	Public key component of the ephemeral key pair (dc, Qc) generated by the 3DS SDK and used to establish session keys between the 3DS SDK and ACS.	No	No	No

[1] Data may be temporarily stored and/or retained in logs only until transaction authorization and clearing is complete. If the transaction is ended prior to authorization (for example, due to cancellation or failure), the data must not be retained beyond this point.

[2] May be temporarily stored for troubleshooting until the issue is resolved.

CATEGORY	3DS Data Element		Description	Storage Permitted		
				3DSS	DS	ACS
Authentication Challenge Data (CReq/CRes) **App-Based**	ACS HTML		HTML provided by the ACS in the CRes message. Utilized in the HTML UI type during the Cardholder challenge.	N/A	N/A	Yes
	Challenge Additional Information Text		Additional text provided by the ACS/Issuer to Cardholder during the Challenge Message exchange that could not be accommodated in the Challenge Information Text field.	N/A	N/A	Yes
	Challenge Data Entry	CVM	Contains the data that the Cardholder entered into the Native UI text field.	N/A	N/A	No
	Challenge HTML Data Entry		Data that the Cardholder entered into the HTML UI.	N/A	N/A	No
	Challenge Information Header		Header text that for the challenge information screen that is being presented.	N/A	N/A	Yes
	Challenge Information Label		Label to modify the text provided by the Issuer to describe what is being requested from the Cardholder.	N/A	N/A	Yes
	Challenge Information Text		Text provided by the ACS/Issuer to Cardholder during the Challenge Message exchange.	N/A	N/A	Yes
	Challenge Selection Information		Selection information that will be presented to the Cardholder if the option is single or multi-select. The variables will be sent in a JSON Array and parsed by the SDK for display in the user interface.	N/A	N/A	Yes
	Expandable Information Label 1		Label displayed to the Cardholder for the content in Expandable Information Text 1.	N/A	N/A	Yes
	Expandable Information Text 1		Text provided by the Issuer from the ACS to be displayed to the Cardholder for additional information and the format will be an expandable text field.	N/A	N/A	Yes
	Issuer Image		Sent in the initial CRes message from the ACS to the 3DS SDK to provide the URL(s) of the Issuer logo or image to be used in the Native UI.	N/A	N/A	Yes
	Message Extension		Data necessary to support requirements not otherwise defined in the 3-D Secure message must be carried in a Message Extension.	N/A	N/A	Yes

CATEGORY	3DS Data Element	Description	Storage Permitted		
			3DSS	DS	ACS
Authentication Challenge Data (CReq/CRes) **App-Based (cont'd)**	OOB App URL	Mobile Deep link to an authentication app used in the out-of-band authentication. The App URL will open the appropriate location within the authentication app.	N/A	N/A	Yes
	OOB App Label	Label to be displayed for the link to the OOB App URL. For example: "OOBAppLabel" : "Click here to open Your Bank App"	N/A	N/A	Yes
	OOB Continuation Label	Label to be used in the UI for the button that the user selects when they have completed the OOB authentication.	N/A	N/A	Yes
	Payment System Image	Sent in the initial CRes message from the ACS to the 3DS SDK to provide the URL(s) of the DS logo or image to be used in the Native UI.	N/A	N/A	Yes
	Resend Information Label	Label to be used in the UI for the button that the user selects when they would like to have the authentication information resent.	N/A	N/A	Yes
	Submit Authentication Label	Label to be used in the UI for the button that the user selects when they have completed the authentication. This is not used for OOB authentication.	N/A	N/A	Yes
	Why Information Label	Label to be displayed to the Cardholder for the "why" information section.	N/A	N/A	Yes
	Why Information Text	Text provided by the Issuer to be displayed to the Cardholder to explain why the Cardholder is being asked to perform the authentication task.	N/A	N/A	Yes
Authentication Challenge Data (CReq/CRes) **Browser-Based**	Message Extension	Data necessary to support requirements not otherwise defined in the 3-D Secure message must be carried in a Message Extension.	No	N/A	Yes
Cardholder Challenge Data	Challenge HTML Data Entry CVM	During a challenge, this is the HTML data exchanged between the Browser and the ACS that contains the cardholder data entered in the browser UI.	No	N/A	No

Table 2: 3DS Cryptographic Keys with HSM Requirements

The 3DS cryptographic keys included in Table 2 are required to be generated and managed in an HSM, in accordance with the PCI 3DS Core Security Standard HSM requirements, and are also subject to all other cryptography and key management requirements in the PCI 3DS Core Security Standard.

Cryptographic keys/certificates defined in the *EMV® 3-D Secure Protocol and Core Functions Specification* that are not included in Table 2 are not required to be generated and managed in an HSM; however, such keys/certificates are subject to all other cryptography and key management requirements in the PCI 3DS Core Security Standard. While an HSM is required only for the keys in Table 2, use of an HSM for other 3DS keys is strongly recommended. All 3DS keys should be evaluated in accordance with the 3DS entity's risk-management policy to determine whether they should be managed in an HSM.

Key generated and used by	Key	Key Description
ACS	ACS Private Key*	Private key Pv_{ACS} used by the ACS for the ACS Signed Content JWS. The ACS shares public key Pb_{ACS}, with DS CA in a CSR.
DS	DS Private Key* (RSA or EC)	Private key used by DS to decrypt sdkEncData received in AReq from SDK. The public key is used by the SDK to encrypt sdkEncData.

** Note: Public/private key pair to be generated in an HSM. Private key to also be stored/managed in HSM.*