Dynamic CVV2 Guide

Version: 1.0

05 July 2024

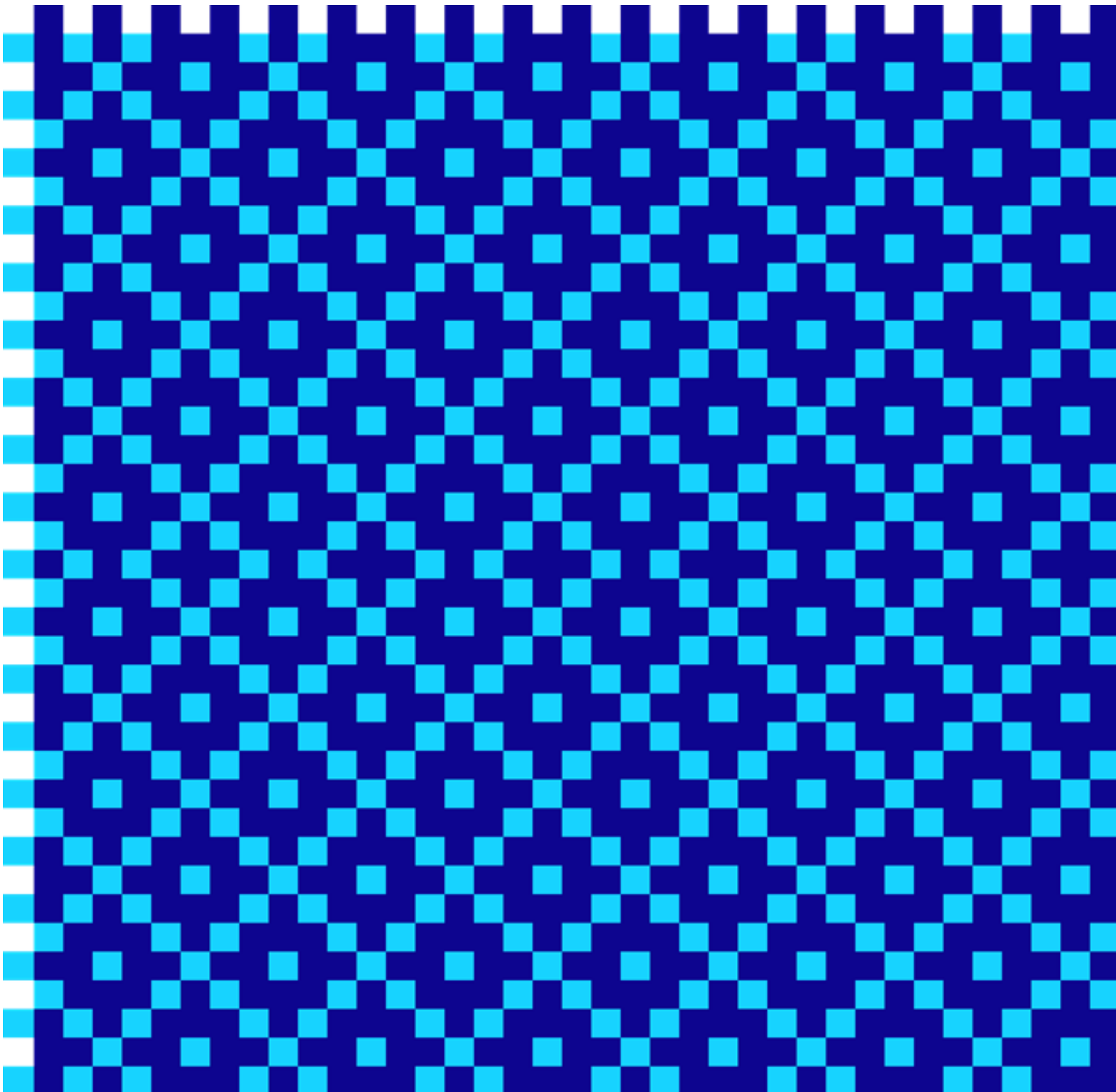
Publication number: DCVV-1.0-7/5/2024

For the latest technical documentation, see the Documentation Portal.

Thredd , Kingsbourne House, 229-231 High Holborn, London, WC1V 7DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682



Copyright

1.1 Dynamic CVV2

The Card Verification Value 2 (referred to by Visa as CVV2 and Mastercard as CVC 2) is a 3 digit code displayed on the back or front of the card. The cardholder must enter or provide the CVV2 during a card-not-present transaction, as a way of verifying that they have the card in their possession. Since the CVV2 is a static number, this makes it more susceptible to fraud.

With dynamic CVV2[1], the default CVV2 value linked to the card record is ignored; the CVV2 value is verified during transaction authorisation against another value which your systems dynamically supply to the cardholder (e.g., via their card app or SMS). This can improve the security of card-not-present transactions.

1.1.1 How it works

Thredd assigns a static CVV2 to the card record when it is generated. If Dynamic CVV2 is enabled, then we by-pass our CVV2 value checks during the authorisation stage and send the transaction to your systems through EHI to authorise or decline. You should then ignore the card's default CVV2 value, and check the CVV2 value in the EHI transaction record against the dynamic value you provided to your cardholder.

Note: Dynamic CVV2 is only available on Gateway Processing (modes 1, 4 or 5), where you approve the transaction.

1.1.2 How to Configure

In the **Card Usage Rules** tab on your Product Setup Form (PSF), in the **Verification Checks (V)** box, set the **Bypass CVV2/CVC2 Check** field to **Yes**.

Thredd will not verify the CVV2 and instead this will be sent over EHI for you to verify and approve.

Allow? Y/N	Verification Checks (V)
No	Bypass Online PIN Check
No	Bypass Expiry Date Check
Yes	Bypass CVV2/CVC2 Check
No	Blank CVV2 in Card not Present E-commerce
No	Blank CVV2 in Card not Present Phone/Mail Order
No	Blank CVV2 in Card not Present Recurring
No	Blank CVV2 in Card not Present Manual Key Entry
No	Allow Blank DE014
No	Expiry date optional for Recurring Payments
No	Bypass Card Status Check for Refund Authorisations

Figure 1: Card Usage Groups: Verification Checks

If using Dynamic CVV2 with printed cards, then please discuss with your Card Manufacturer if you want them to ignore the default CVV2 value sent by Thredd and print the card without a CVV2 field. For more information on configuration options and card designs for physical cards, see the Physical Cards Guide.

If using Dynamic CVV2 with virtual cards, then you can configure your Virtual Image to not display the CVV2 field. For details, see the Virtual Cards Guide > Virtual Card Image Design.

Dynamic CVV2 can be set at card level by assigning the Card Usage group to the card, and therefore can be applied to cards already issued (the cards must be on a product where you are on Gateway Processing - modes 1, 4, 5).

Please confirm with your Implementation Manager that you require the **send CVV2** option to be enabled on your EHI Configuration. This will ensure the CVV2 value is included in the EHI Authorisation message, so that you can check it. See EHI Configuration Options.

---

[1] Visa refer to this service as dynamic CVV2 (dCVV2) and Mastercard refer to it as dynamic Card Validation Code 2 (dynamic CVC 2). **Important**: You should not confuse this with dynamic CVV1 /CVC 1 or dynamic CVV3 /CVC 3, which are different services.

Note: Large merchants such as Paypal and Amazon may not send CVV2; if you specify that a CVV2 response is mandatory, then this may cause declines. We therefore recommend that in your **Card Usage Rules** you set the **Allow Blank CVV2 in Card not Present E-commerce** to **Yes**. See The Physical Cards Guide > Cards Usage Options.
During the transaction authorisation stage, we recommend that your systems do not decline a blank CVV2 value where the transaction originated from a large merchant such as Payal or Amazon[2].

1.1.3 Checking the CVV2 at the Authorisation Stage

During transaction authorisation (using Dynamic CVV2):

1. The cardholder enters the CVV2 value provided to them by your systems (e.g., via phone app, SMS, web portal or smart card).
2. The Merchant includes the CVV2 value in the authorisation request.
3. When Thredd receives the request from the card scheme, we bypass the CVV2 value checks (as **Bypass CVV2** is enabled in the card Usage Group). Thredd then takes the clear CVV2 value and encrypts it.
4. The Authorisation request is sent to your systems to validate the CVV2 value, along with any other checks; your systems must return an approve or decline decision.
5. Thredd returns your response to the card scheme.

Note: The CVV2 validation result is provided in the 0110 authorisation response message, in the **F44.10** field for Visa and in the **DE048.87** field for Mastercard.

1.1.4 CVV2 Processing at the Card Scheme

Please check with your Implementation Manager for relevant CVV2 processing options that should be configured at scheme level.

---

2 You can use Merch_ID_DE42 or Merch_Name_DE43 to identify the merchant.

Document History

This section contains details of all changes to this guide.

Version	Date	Comments	Author
1.1	05/07/2024	Updated the company address.	JB
1.0	26/06/2024	Updates to content and graphics to align with taxonomy updates on our Documentation Portal.	WS
	22/06/2023	First version	WS