Requirements and Testing Procedures		Guidance
3.3 Sensitive authentication data (SAD) is not stored after authorization.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** SAD is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Therefore, the storage of SAD upon completion of the authorization process is prohibited. **Definitions** The authorization process completes when a merchant receives a transaction response (for example, an approval or decline).
3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	**3.3.1.a** If SAD is received, examine documented policies, procedures, and system configurations to verify the data is not retained after authorization.	
Customized Approach Objective	**3.3.1.b** If SAD is received, examine the documented procedures and observe the secure data deletion processes to verify the data is rendered unrecoverable upon completion of the authorization process.	
This requirement is not eligible for the customized approach.		
Applicability Notes		
This requirement does not apply to issuers and companies that support issuing services (where SAD is needed for a legitimate issuing business need) and have a business justification to store the sensitive authentication data. Refer to Requirement 3.3.3 for additional requirements specifically for issuers. Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.		