

Requirements and Testing Procedures		Guidance
3.2 Storage of account data is kept to a minimum.		
Defined Approach Requirements 3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: <ul style="list-style-type: none"> • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. <i>This bullet is a best practice until its effective date; refer to Applicability Notes below for details.</i> • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable. 	Defined Approach Testing Procedures 3.2.1.a Examine the data retention and disposal policies, procedures, and processes and interview personnel to verify processes are defined to include all elements specified in this requirement. 3.2.1.b Examine files and system records on system components where account data is stored to verify that the data storage amount and retention time does not exceed the requirements defined in the data retention policy. 3.2.1.c Observe the mechanisms used to render account data unrecoverable to verify data cannot be recovered.	Purpose A formal data retention policy identifies what data needs to be retained, for how long, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only account data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. The storage of SAD data prior to the completion of the authorization process is also included in the data retention and disposal policy so that storage of this sensitive data is kept to minimum, and only retained for the defined amount of time. Good Practice When identifying locations of stored account data, consider all processes and personnel with access to the data, as data could have been moved and stored in different locations than originally defined. Storage locations that are often overlooked include backup and archive systems, removable data storage devices, paper-based media, and audio recordings. To define appropriate retention requirements, an entity first needs to understand its own business needs as well as any legal or regulatory obligations that apply to its industry or to the type of data being retained. Implementing an automated process to ensure data is automatically and securely deleted upon its defined retention limit can help ensure that account data is not retained beyond what is necessary for business, legal, or regulatory purposes. <i>(continued on next page)</i>
Customized Approach Objective Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.		