

## Kartläggning kassa-applikationers lagring av kortinformation

För att kartlägga och utvärdera hur era kassa-applikationer och dess versioner hanterar lagring av kortinformation skall bifogad **PCI DSS Statusmatris kassa-applikation** fyllas i.

Den här matrisen avser enbart kassa-applikationen. Motsvarande matris för KI fylls i av PSP.

Gruppera alla versionerna av kassa-applikationerna utifrån betalmodul/kortmodulens version. Per gruppering skall matrisen fyllas i.

Nedanstående begrepp skall anges i respektive ruta:

- **Open** = Fylls i om data lagras i klartext okrypterat. Open skall även fyllas i om det går att aktivera lagring vid felsituation eller liknande
- **Encrypt** = Lagras krypterat
- **Offline** = Lagras krypterat tillfälligt för alla transaktioner och så länge det behövs för offline till dess att clearing transaktionen är genomförd.
- **None** = Lagras aldrig

För PAN rutan kan även nedanstående begrepp fyllas i:

- **Enligt PCI 3.4** = PAN lagras enligt 3.4 och använder t ex trunkering eller annan godkänd form se PCI 3.4.

### PCI DSS krav avseende lagring av kortinformation.

**Källa: PCI Security Council, version 1.1.** <https://www.pcisecuritystandards.org/>  
Läs Kapitlet 3 och 4 i PCI DSS regelverket för att få en ökad förståelse av denna matris.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
<b>Cardholder Data</b>	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
<b>Sensitive Authentication Data**</b>	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

\* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.

\*\* Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).