PCI Compliance on Encryption and Database Access

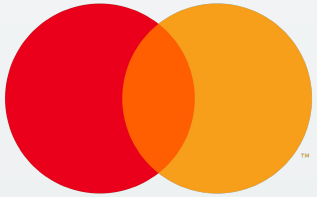
PCI-DSS Introduction

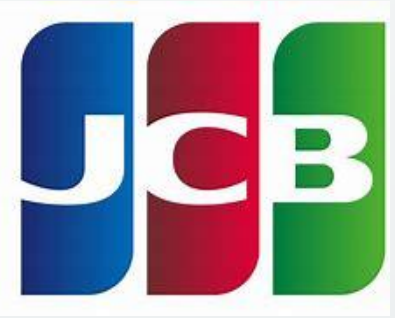
Background

- PCI-DSS is a credit card industry standard that governs how cardholder data is protected information systems

- All organizations that are in possession of credit card related data must meet PCI-DSS.

- PCI DSS v4.0 goes into effect March 31, 2024. Changes from v3.2.1 are “best practices” until March 31, 2025, when they convert to requirements.



PCI Levels

	Annual Credit Card Transactions*	Self-attestation or QSA?
Level 4	< 20,000	Self-attestation**
Level 3	20,000 to 1M	Self-attestation**
Level 2	1M to 6M	Self-attestation**
Level 1	> 6M	QSA required

* American Express and JCB thresholds are lower. AmEx > 2.5M transactions is Level 1.
** Unless they suffered a significant breach that compromised credit card data

Credit Card Data

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

- Cardholder data can be stored, but with the requirements of PCI-DSS (network segmentation, encryption, etc)
- Sensitive Account Data (SAD) must even be encrypted while waiting for authorization and can't be stored for any reason (even if encrypted) after authorization.

PCI-DSS Non-compliance penalties

- Forensic Investigation - $20,000+
- Fines – per month depending on duration of non-compliance

	1-3 Months	4-6 months	7+ months
Low-volume Merchant	$5,000	$25,000	$50,000
High-volume Merchant	$10,000	$50,000	$100,000

- $50 to $90 per breached card
- Higher future transaction fees
- Possible termination of ability to take credit cards at all
- Government fines and lawsuits
- Customer lawsuits
- Customer trust lost – future business

PCI-DSS is Uniquely prescriptive

1. Most frameworks tell you to identify your assets and sensitive data.

   In PCI, credit card data is the concern. Assets are anything that contains that data. End of discussion.

2. Most frameworks tell you to create access controls “commensurate to the risk” and consider defense-in-depth.

   PCI defines the perimeter (Card data environment) and the prescribes layers of defense required within it.

PCI-DSS

1. Network Security controls (Firewalls)
2. Apply Secure Configurations to all system components (hardening)
3. Protect Stored Account Data
    a. Encrypt data-at-rest
    b. RBAC of CC data displays and remote access
    c. Key Management
4. Data-in-transit (TLS, VPN) over public networks
5. Anti-Malware
6. Secure Systems and Software (Lower environments)
7. Restrict Access …. by Business Need to Know (Least Privilege)
8. Identify Users and Authenticate (strong passwords, mfa, time-out, etc)
9. Physical Access
10. Log and Monitor
11. Test Regularly
12. Have an Information Security Policy

    Appendix 1. Service Providers

My Encryption Definitions

Traditional encryption - Traditional AES with counter-mode and 256-bit key.

CCN 1111-1111-1111-1111 => y&NLD#))(<@@>FW (U#NM F…arr93#@g

Tokenization - Cipher text has same datatype (even character set) as the plaintext. Baffle uses format preserving encryption (FPE)

CCN 1111-1111-1111-1111 => 5426-6244-7689-5357
CCN 1111111111111111 => 5426624476895357

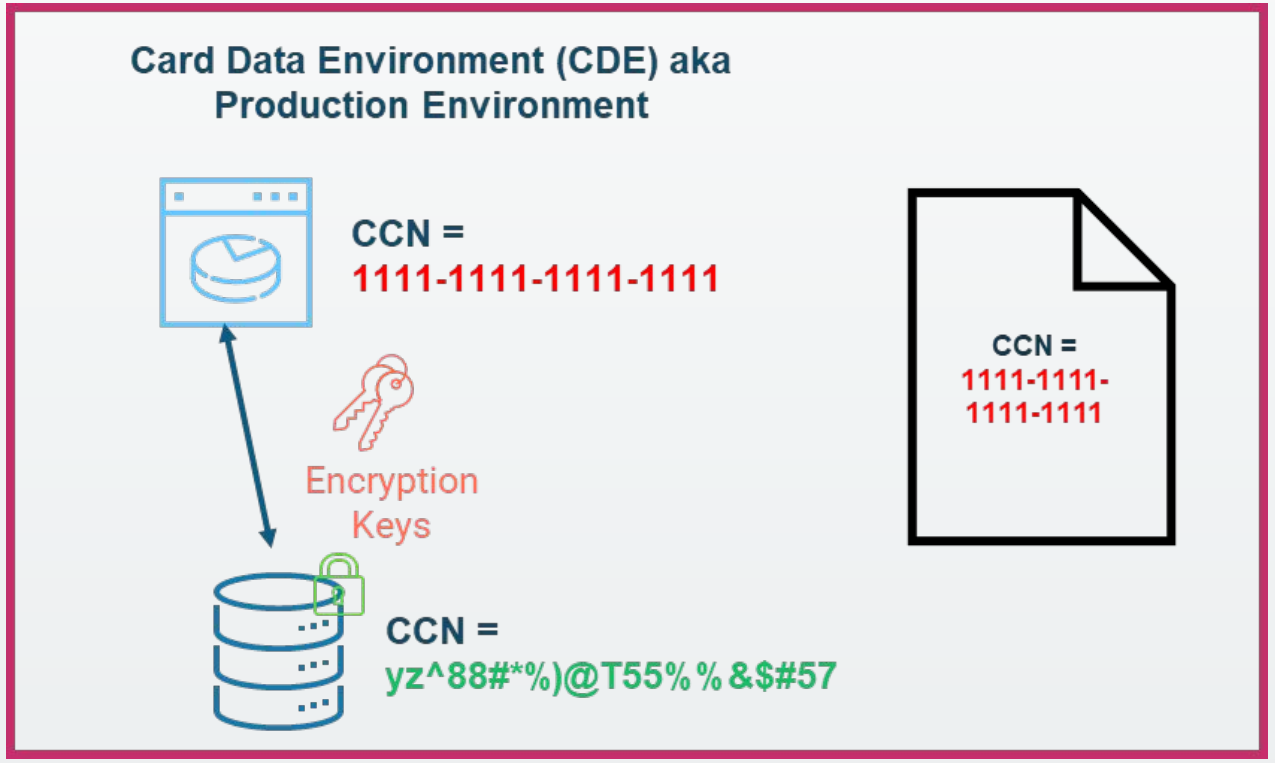
Masking - Substitution of all or part of the plaintext. Original data destroyed.

CCN 1111-1111-1111-1111 => **confidential**
CCN 1111-1111-1111-1111 => XXXX-XXXX-XXXX-1111

Card Data Environment

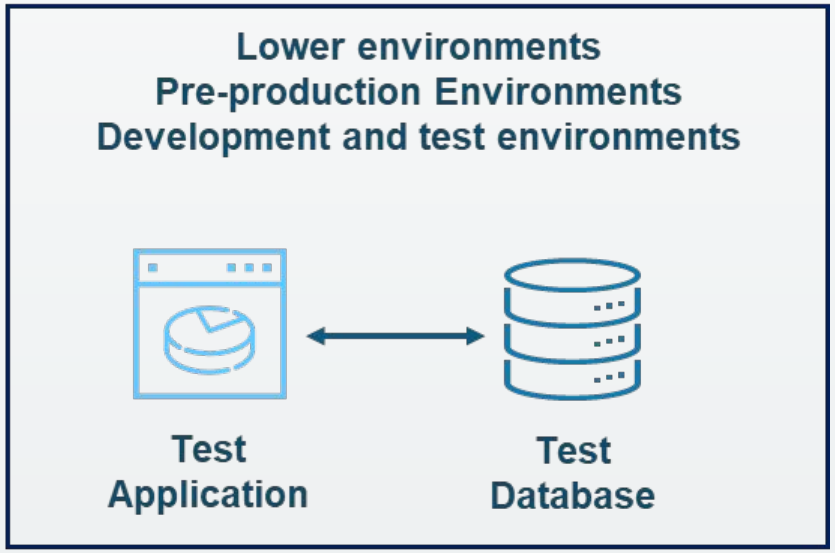
Encryption and Scope

#	Requirement Description
PCI Scope	The following are each in scope for PCI DSS: • Systems performing encryption and/or decryption of cardholder data, and systems performing key management functions • Encrypted cardholder data that is not isolated from the encryption and decryption and key management processes, • Encrypted cardholder data that is present on a system or media that also contains the decryption key • Encrypted cardholder data that is present in the same environment as the decryption key • Encrypted cardholder data that is accessible to an entity that also has access to the decryption key

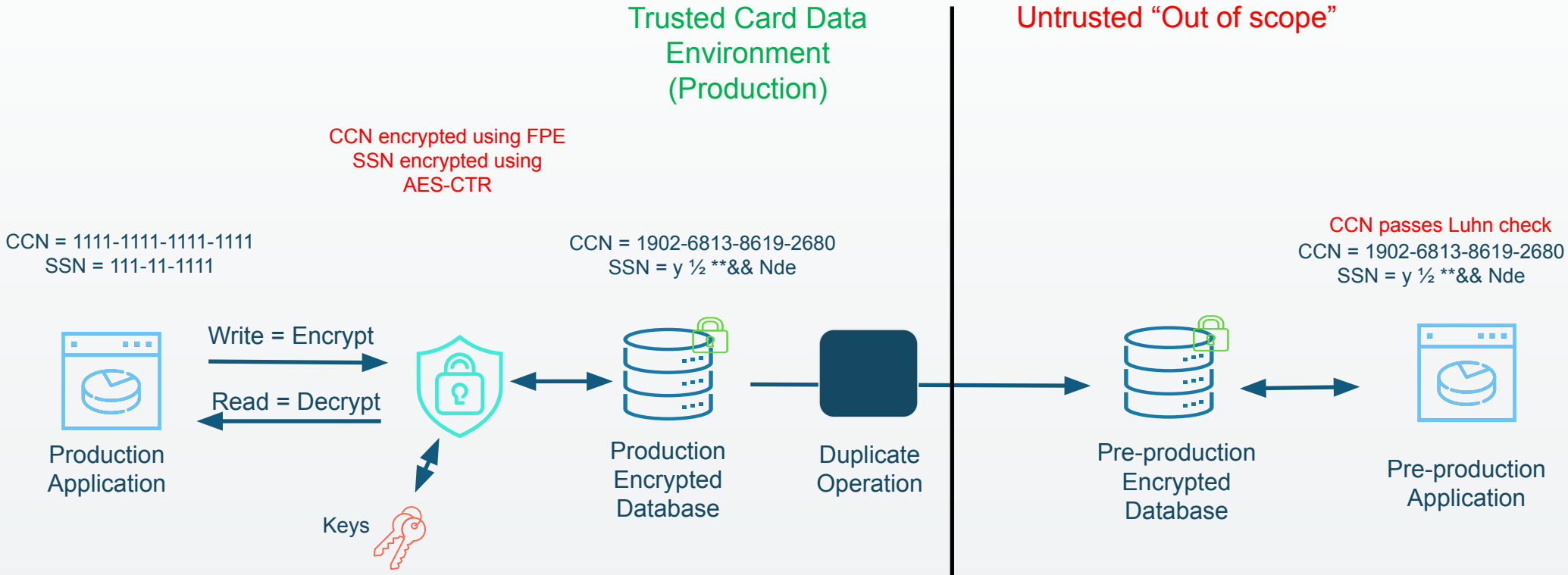


Encryption for “out of scope” environments

#	Requirement Description
Third-party service provider (not in scope)	Where a third-party service provider (TPSP) receives and/or stores only data encrypted by another entity, and where they do not have the ability to decrypt the data, the TPSP may be able to consider the encrypted data out of scope if certain conditions are met.
6.5.3 6.5.5	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.



Lower Environments (PCI-DSS compliant) and Tokenizaton



Encryption for “out of scope” environments cont’d

#	Requirement Description
4.2.1	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.

Least Privilege

Least Privilege (Section 7)

#	Requirement Description
7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.
7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.
7.2.6	All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.

PCI-DSS and Least Privilege

Should the DBA have access to:

- The same company financials that the CFO has?
- Social security numbers that only HR should have?
- Credit card numbers that only some in Finance should have?

What they should really say is the business owner.

What if we want to outsource the database management or move to managed databases in the cloud to cut CapEx costs?

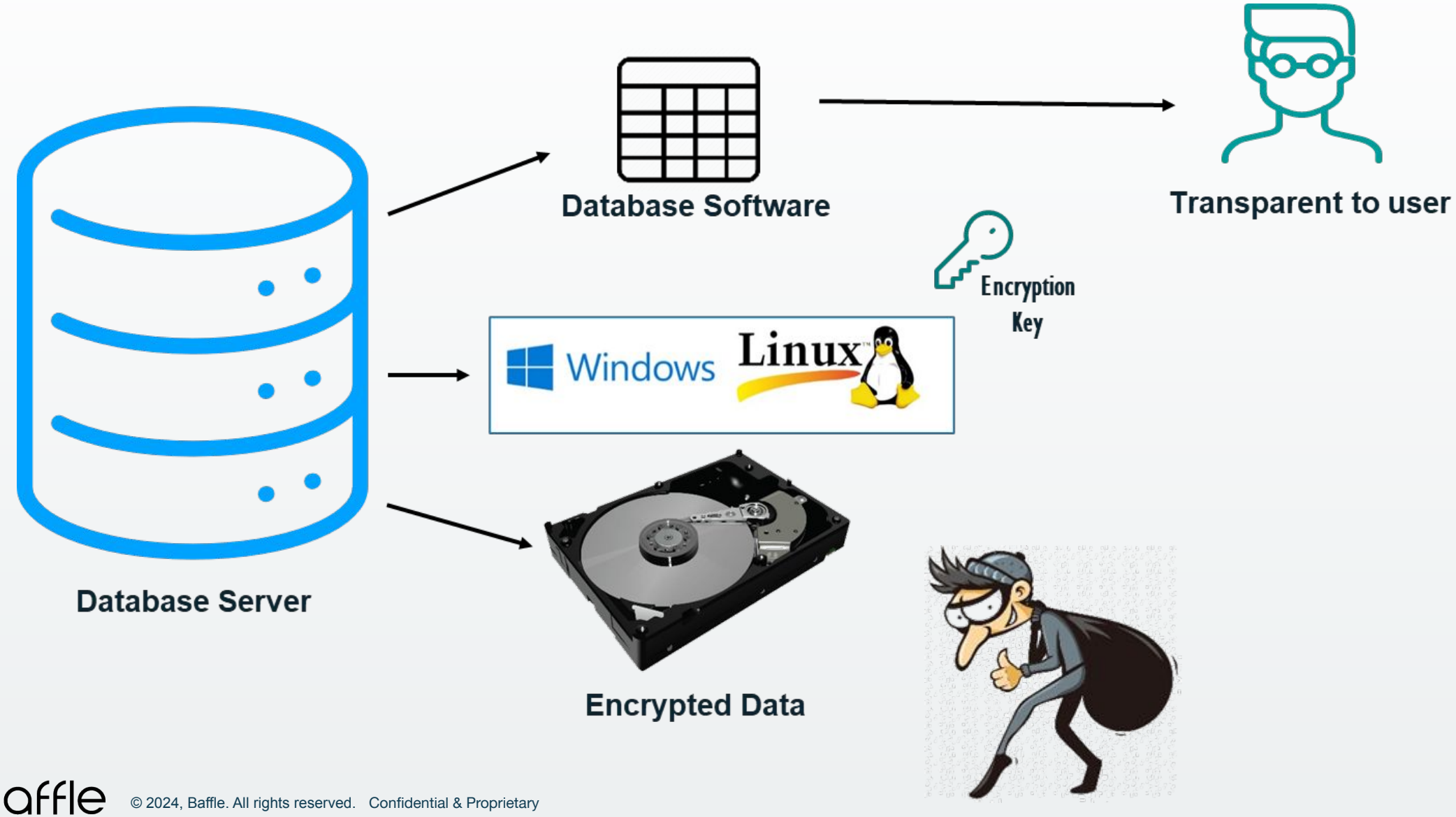
This is a blind spot in all security and privacy frameworks because there hasn’t been a good solution for it.

Policies in the CDE

Transparent Data Encryption and Full Disk Encryption

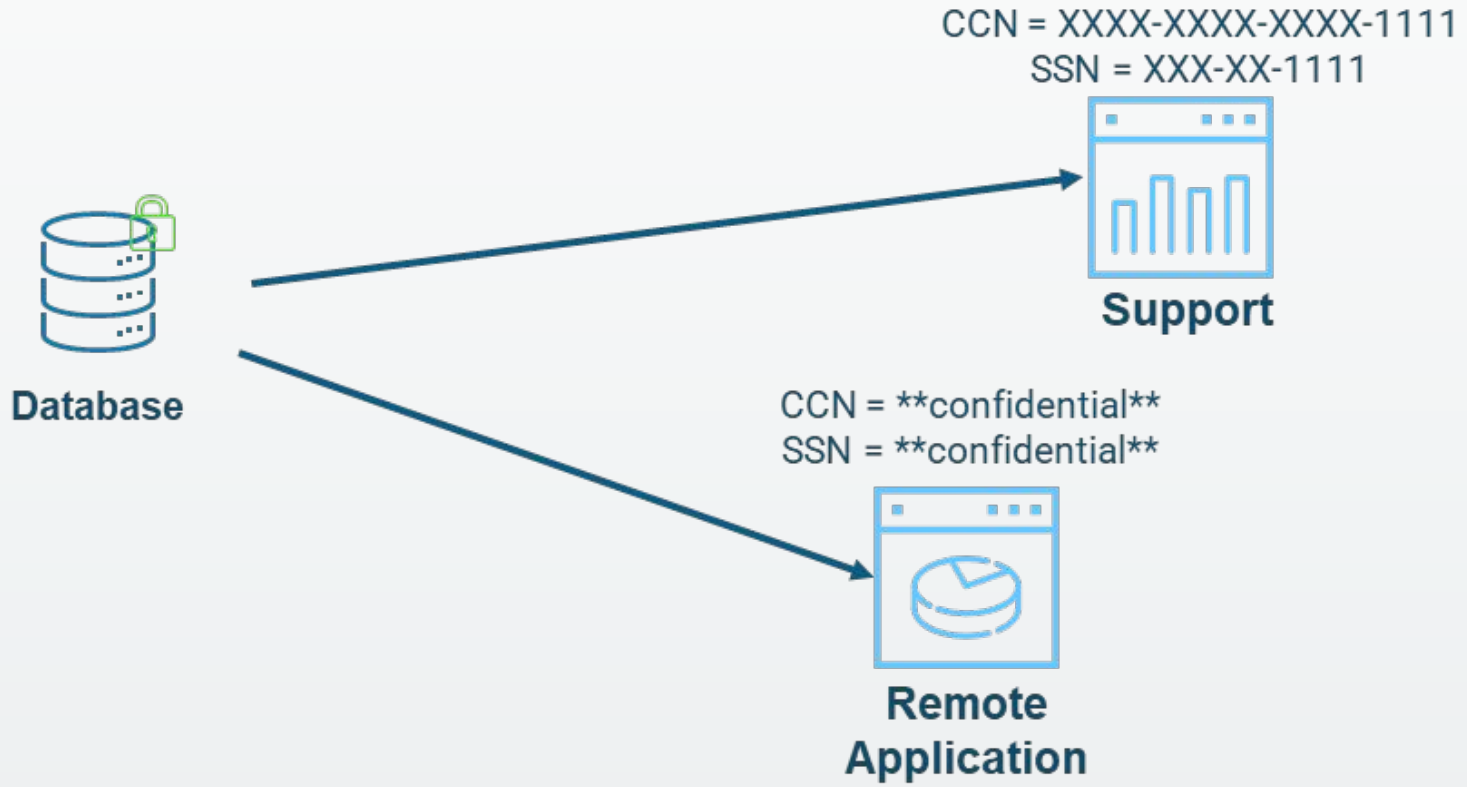
#	Requirement Description
3.5.1	PAN is rendered unreadable anywhere it is stored by using any of the following approaches: … • Strong cryptography with associated key management processes and procedures.
3.5.1.2	If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media OR • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.
3.5.1.3	3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.

TDE/FDE



Access Controls in the CDE

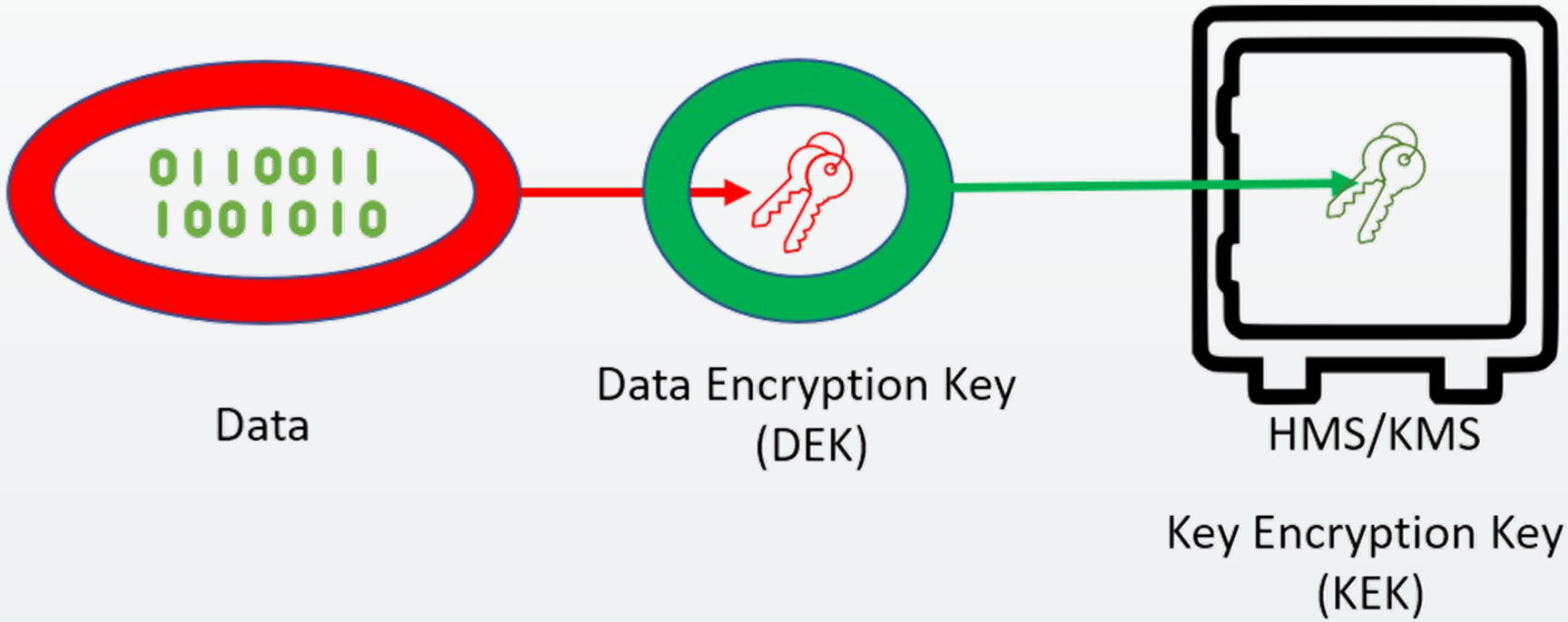
#	Requirement Description
3.4.1	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that **only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN**
3.4.2*	When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate,defined business need.



*Requirement 3.4.2 is new to v4.0 and becomes a hard requirement in March 31, 2025.

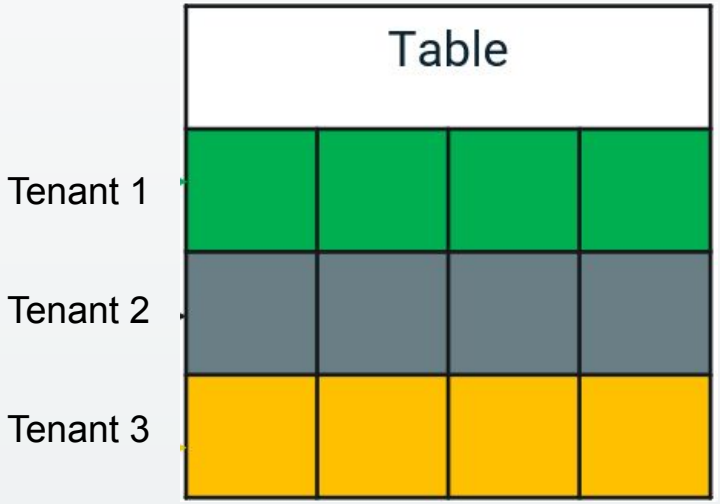
Key Management in the CDE

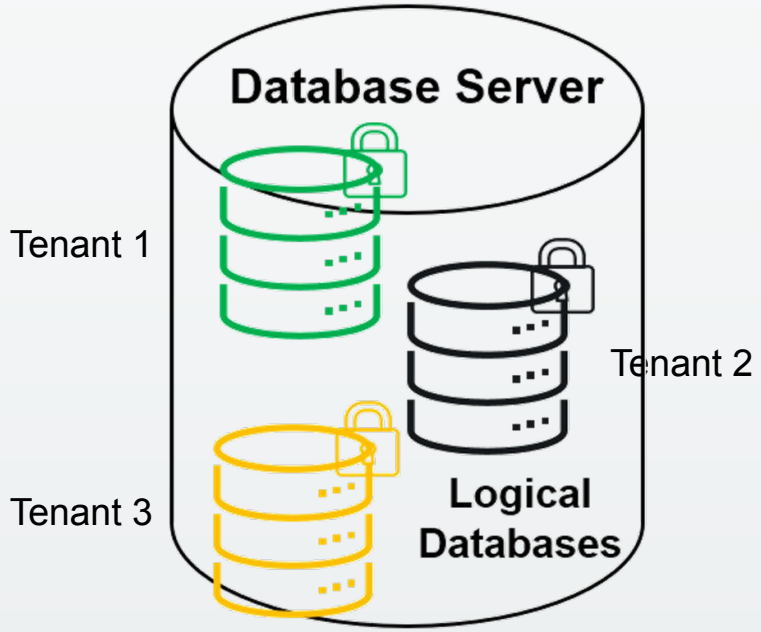
#	Requirement Description
3.6.1	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.



Multi-tenant Databases

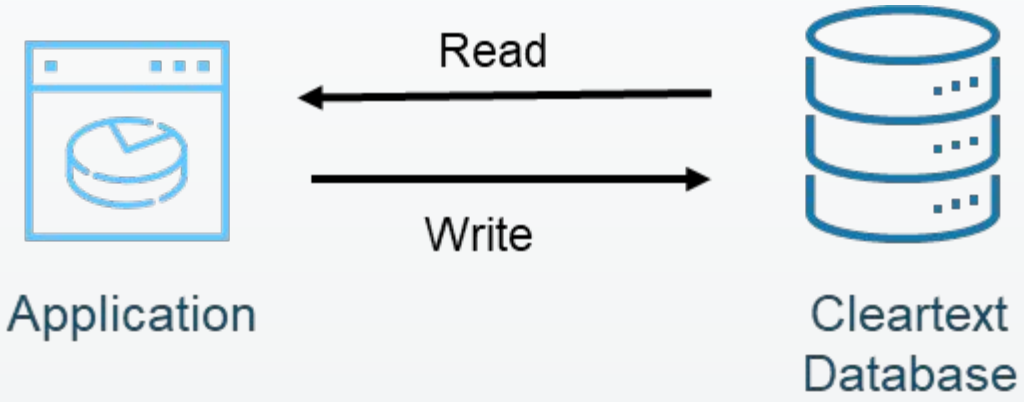
#	Requirement Description
Appendix A 1.1.1	Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization. • Customers cannot access the provider's environment without authorization
Appendix A.1.1.2	Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.



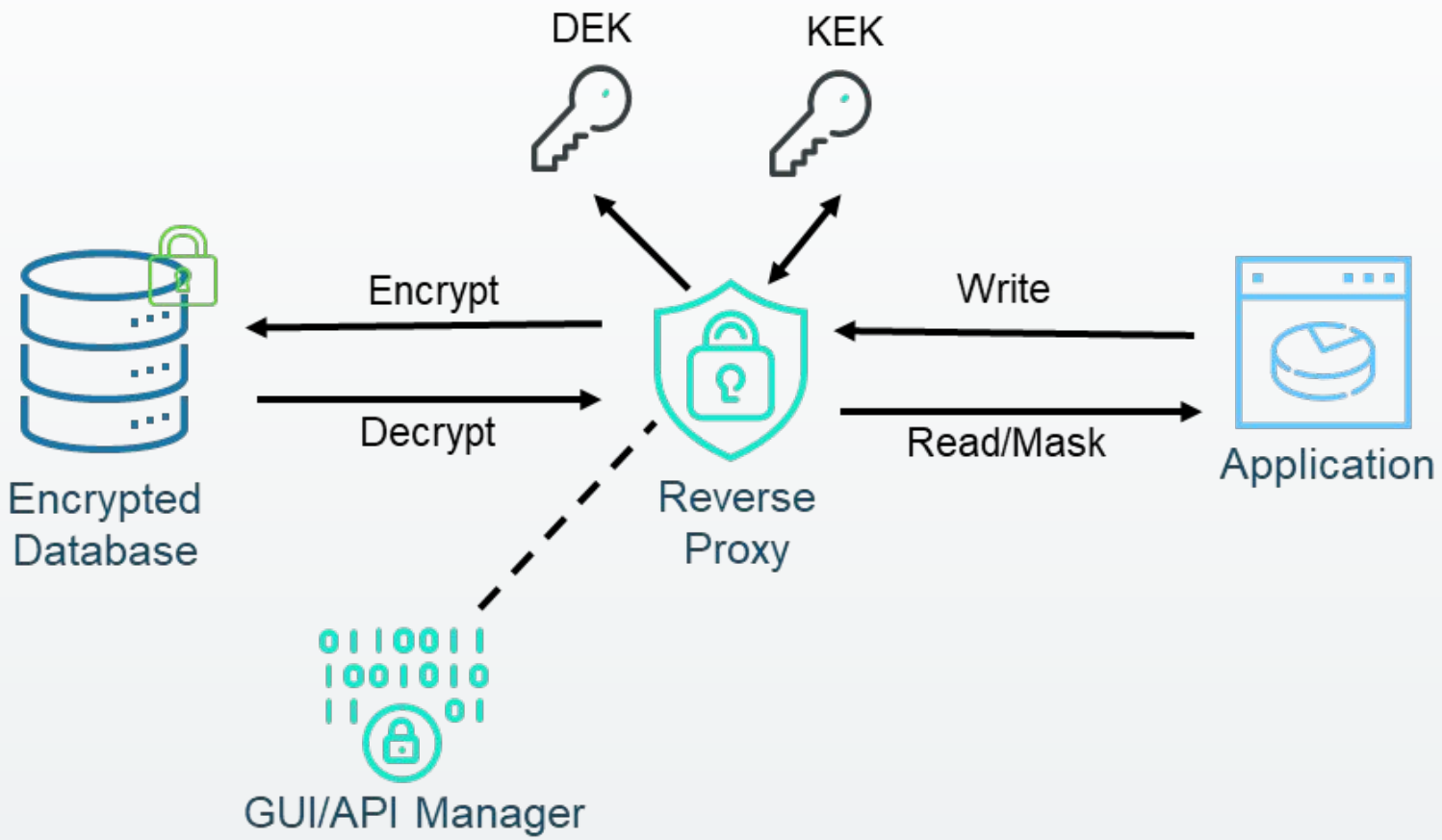


Proposed Solution

Application and Database - Starting point



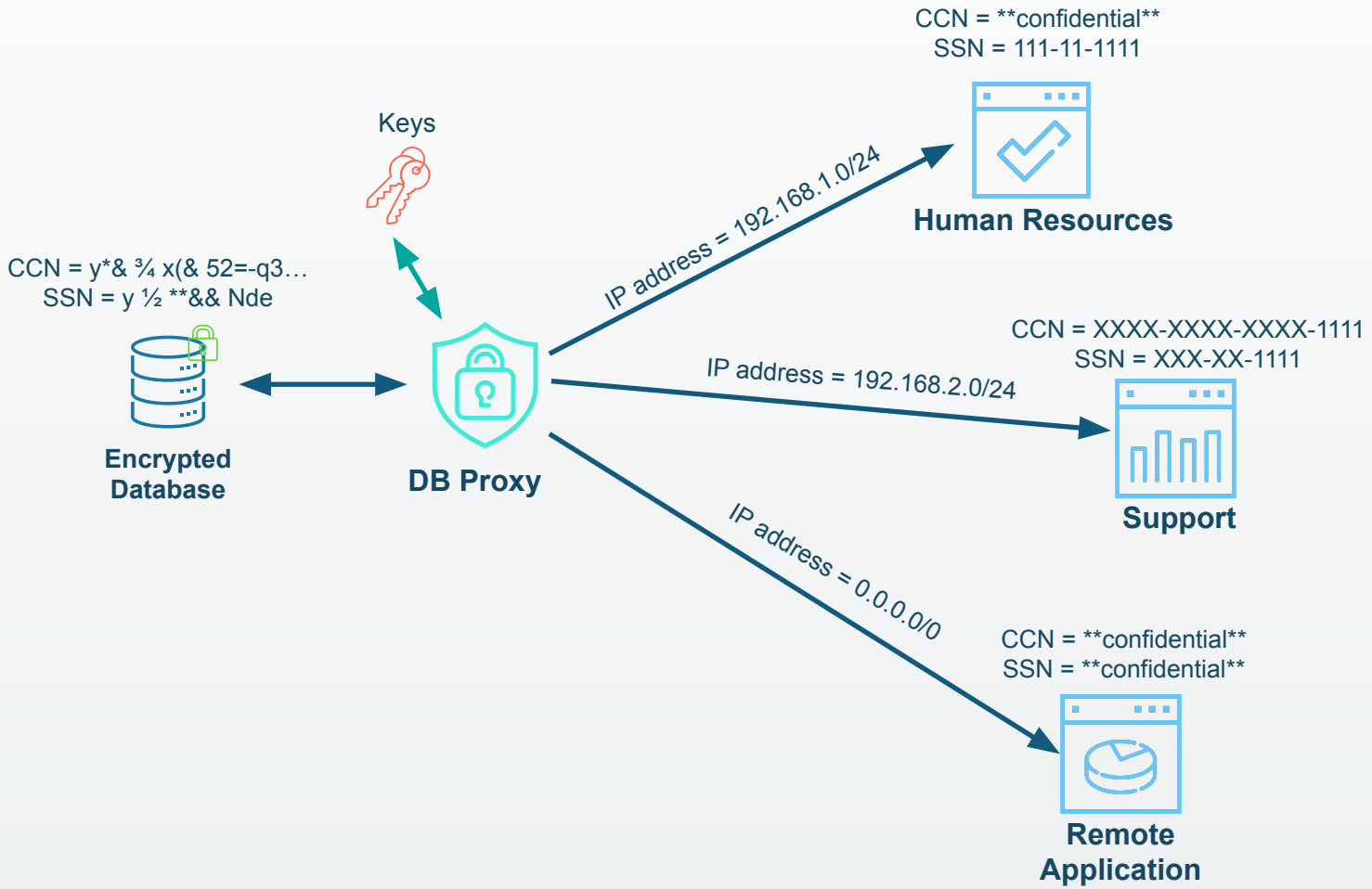
Proposed Architecture



- No application code changes
  - Legacy Code works
  - Third-party applications work
- Key management
  - Centralized control
  - Customer control

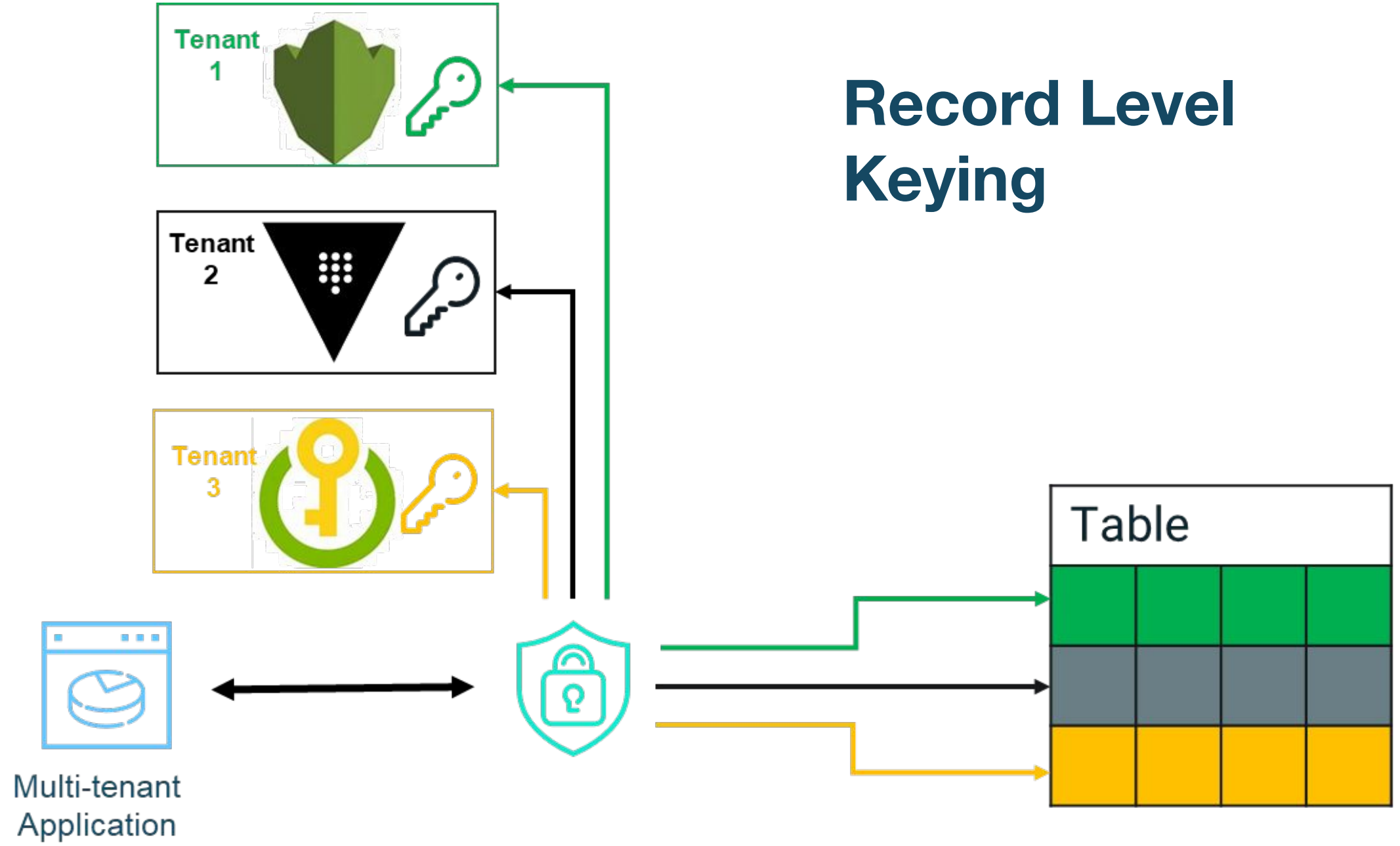
Architecture

DB Proxy RBAC and ABAC (Dynamic Masking)

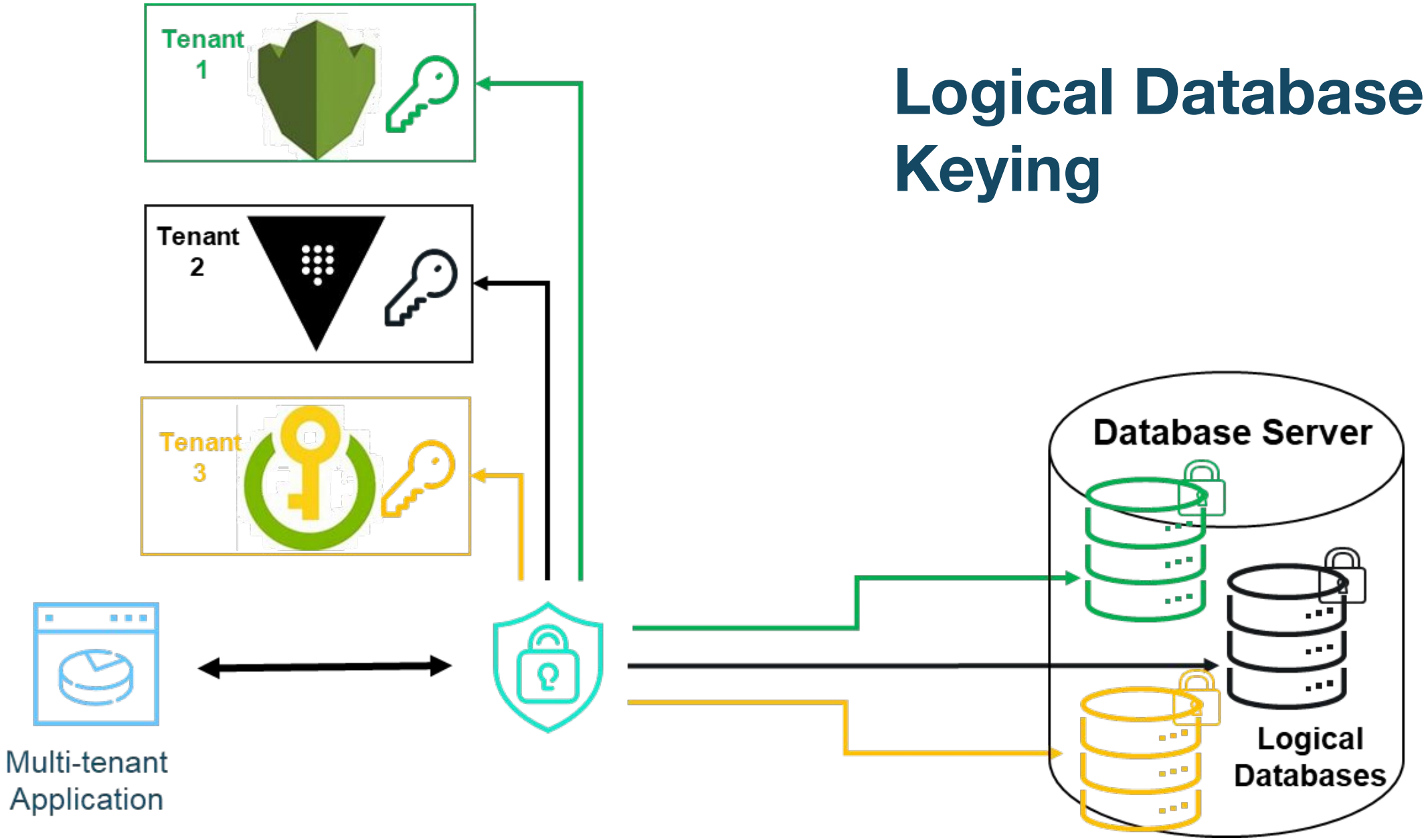


- Least Privilege
  - RBAC for users and applications including the DBA
  - AWS Shared responsibility model

Record Level Keying



Logical Database Keying



Privacy Enhanced Computation (PEC)

Hypothetical Query on Sensitive Data

Unencrypted data before Baffle

Name	Age	Salary	ID
Elise Smith	45	200000	133
Simon Jones	30	80000	134
Alicia Jackson	67	120000	135
James Werner	52	75000	136

Encrypted data set with Baffle

Name	Age	Salary	ID
Rsjskd&^skjd	*&^%$()”><	jin$^¾¾,.</;{}\dd	133
Ikks#%^aydm	}{|(@#%^(	¾klm¾UIU^&$#9	134
Uw%$(skilsixq	%$(!@#<>	¾*&¾¾,.<>/;{}\dd	135
Rsgh#&*urps	*()^$#&*)^	¾hdsi¾¾^&$#6	136

For what are the age statistics for employees with annual salaries over $100,000?

```
SELECT
    AVG(age),
    MIN(age),
    MAX(age)
FROM salaries
WHERE
    Salary > 100000
```

Database Operations on Encrypted Data

Name	Age	Salary	ID
Rsjskd&^skjd	*&^%$()"><	jin$^¾¾,.</;{}\dd	133
lkks#%^aydm	}{|(@#%^(	¾klm¾UIU^&$#9	134
Uw%$(skilsixq	%$(!@#<>	¾*&¾¾,.<>/;{}\dd	135
Rsgh#&*urps	*()^$#&*)^	¾hdsi¾¾^&$#6	136

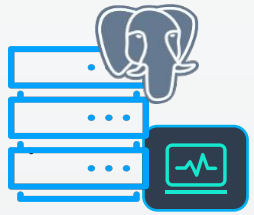
```
SELECT AVG(age), MIN(age),
  MAX(age)
FROM salaries
WHERE Salary > 100000
```

UDFs for Privacy Enhanced Encryption

Name	Age	Salary	ID
Rsjskd&^skjd	*&^%$()"><	jin$^¾¾,.</;{}\dd	133
lkks#%^aydm	}{|(@#%^(	¾klm¾UIU^&$#9	134
Uw%$(skilsixq	%$(!@#<>	¾*&¾¾,.<>/;{}\dd	135
Rsgh#&*urps	*()^$#&*)^	¾hdsi¾¾^&$#6	136

```
SELECT AVG(age), MIN(age),
  MAX(age)
FROM salaries
WHERE Salary > 100000
```

Response: 56, 45, 67



Baffle UDFs

KEY TAKEAWAYS

The proposed architecture is the easiest way to encrypt databases and object stores

- No-code changes required in the application or database
- Postgres does not provide native TDE, but even when available, Baffle is a more complete solution for data-at-rest, in-transit, and in-use
- Keys can be completely separated from the data
- RBAC and ABAC custom masking options for every application
- Format preserving encryption when datatype and length must be preserved
- Database-side operations are possible
- Multi-tenant data isolation based on records in a table or logical databases in a database instance.

Questions?

Backup

Privacy Enhanced Computation Approaches

	Confidential computing / enclaves	Homomorphic encryption and SMPC	Baffle Advanced Encryption
Requires no special hardware or significant storage space	X	X	✔
Data centric protection	X	✔	✔
Prevents DBA/admin access to regulated data	X	✔	✔
Highly performant	✔	X	✔
Supports any and all computations	✔	X	✔

Baffle vs Alternate Approaches

	Feature/Requirement Summary	Baffle	TDE	FDE	pgcrypto
	No application code modifications.	√	√	√	X
Scope	Can the database or application be removed from PCI-DSS scope?	√	X	X	X
6.5.3	Production and in pre-production environments separation enforced with access controls	√	X	X	X
3.5.1	PAN is secured wherever it is stored - database	√	√	√	√
3.5.1	PAN is secured wherever it is stored - flat files (i.e. text files, spreadsheets)	√	X	X	X
3.5.1.3	If FDE is used for 3.5.1, additional access controls are required.	√	√	X	√
3.4.1	PAN is masked to restrict access to least privilege.	√	X	X	X
3.4.2	Restrict remote access privilege.	√	X	X	X
7.2.1 7.2.2	Access control model based on least privilege using RBAC and ABAC.	√	X	X	X
8.2.1	All users are assigned a unique ID before access to cardholder data is allowed	√	X	X	X
A.1.1.1	Provider: The provider cannot access its customers' environments and customers cannot access the provider's environment without authorization	√	X	X	X
A.1.1.2	Provider: Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.	√	X	X	X

PG Crypto

Puts all the burden on the application

Code changes required including all key management
- Not centralized
- Two-tier approach
- Keys in storage, at the application, at the database
- Multi-tenant

DBA can’t get clear data, unless they grab the key.

Can’t do database-side operations