KEW
DATA CONSULTANTS

STATIC VS DYNAMIC DATA MASKING

Data Security and Privacy Protection

00447500420759

kewdataconsultants.com

ali@kewdataconsultants.com

Static vs Dynamic Data Masking: Key Differences and Examples

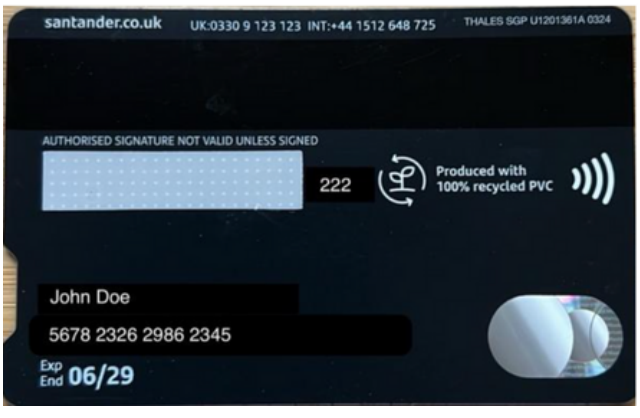
Data security is crucial in protecting sensitive information, and data masking is a widely used technique to help safeguard data in non-production and production environments. The two primary types of data masking are Static Data Masking (SDM) and Dynamic Data Masking (DDM). In this paper, we'll compare both techniques and provide examples to show when and how they are applied.

What is Data Masking and What is the Difference b/w Masking and Encryption?

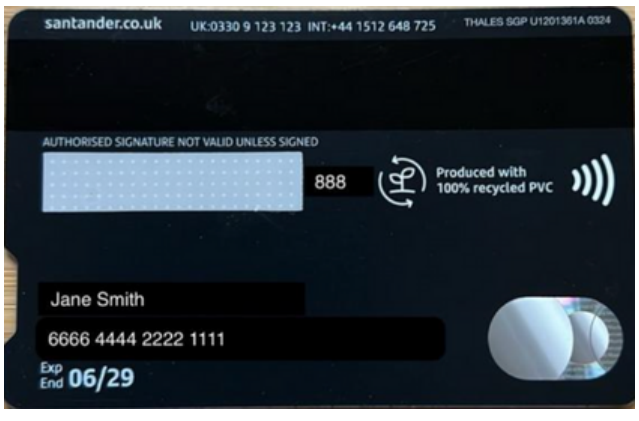
Data masking is the process of replacing sensitive data with fictional but realistic-looking values. It's typically used to protect data in environments like testing, development, or analytics without exposing personal or sensitive information. Data masking could also be used to implement security techniques like Datacentric ABAC.

Data Masking and Data Encryption are both techniques used to protect sensitive information, but they serve different purposes and function in distinct ways.

- Data Masking involves replacing sensitive data with fictitious but realistic values, making it unrecognizable while maintaining its format for use in non-production environments. Masking is irreversible, meaning once the data is masked, it cannot be restored to its original form. For example, in a test environment, a masked credit details of John Doe, 5678-2326-2986-2345, CVV 222 might be replaced with Jane Smith, 6666-4444-2222-1111, CVV 888 to protect real customer data during development or testing.

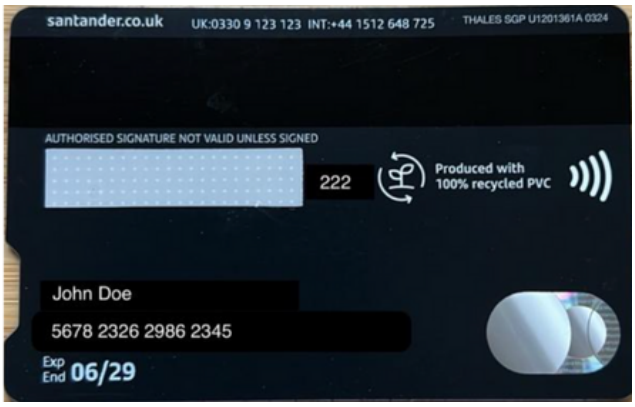


Original Card Details

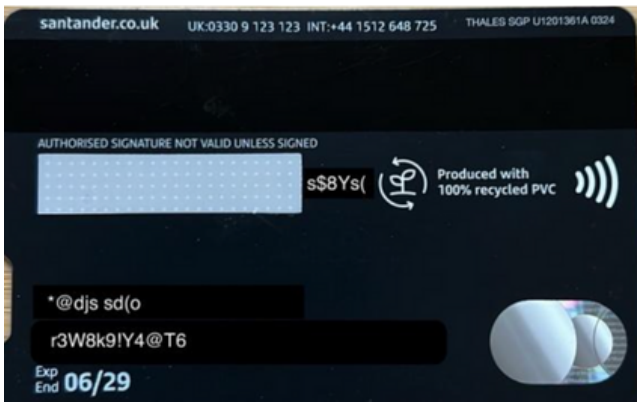


Masked Card Details

- Data Encryption, on the other hand, scrambles the data into an unreadable format using an encryption key. The original data can only be restored or accessed by authorized parties with the decryption key. For example, an encrypted credit card details might look like a random string of characters such as r3W8k9!Y4@T6. Only the user with the correct decryption key can read the original details (John Doe, 5678-2326-2986-2345, CVV 222) again.



Original Card Details



Encrypted Card Details

In summary, masking makes data unusable for unauthorized users by replacing it, while encryption keeps data secure by transforming it into a format that can only be reversed with the correct key.

Static Data Masking (SDM)

Static Data Masking creates a masked copy of the data, which is stored separately for use in non-production environments.

Example of SDM:

Original Data	Masked Data
John Doe, 1234-5678-9101	Jane Smith, 9876-5432
JohnDoe@Acme.com	email@domain.com
SSN: 313-45-6989	SSN: 987-65-4321

Advantages of SDM:

- Complete protection in non-production environments.
- Ensures regulatory compliance by preventing exposure of real data.
- Reduces risk of data breaches in development or testing environments.

Limitations:

- **No real-time updates:** The masked copy doesn't change as the original database does.
- **Storage requirements:** It creates additional data storage for the masked version.

Dynamic Data Masking (DDM)

Dynamic Data Masking masks data in real-time based on user permissions, without modifying the actual database. It's applied when users query data, ensuring that only authorized personnel can see sensitive information.

Example of DDM:

Original Data	User Role	Masked Data (for unauthorized users)
John Doe, 1234-5678-9101	Admin	John Doe, 1234-5678-9101
email@example.com	Tester	email@****.com
SSN: 123-45-6789	Analyst	SSN: XXX-XX-XXXX

Advantages of DDM:

- Real-time masking: Protects sensitive data while allowing live access.
- No data duplication: Works directly on the production database.
- Scalable: Can be implemented for various users with different roles.

Limitations:

- **Performance overhead:** Real-time masking can impact database performance.
- **Requires proper access control** to ensure only authorized users can see unmasked data.

Key Differences b/w SDM and DDM:

Feature	Static Data Masking (SDM)	Dynamic Data Masking (DDM)
Data Copy	Creates a permanent masked copy of the data	Masks data dynamically during queries
Storage Requirement	Requires additional storage for the masked data	No additional storage needed, works on the production database
Real-Time Access	Not applicable, data is fixed once masked	Provides real-time access with data masking based on roles
Performance Impact	Minimal impact (only during masking process)	Can affect performance, especially on large databases
Use Case	Ideal for development and testing environments	Ideal for live production environments and customer-facing apps

When to Use SDM vs DDM?

Scenario	SDM (Static Data Masking)	DDM (Dynamic Data Masking)
Testing/Development	Best for creating sanitized copies for testing purposes	Not suitable, as real-time access isn't required
Regulatory Compliance	Required when working with non-production data	Best for ensuring compliance while maintaining live operations
Production Environment	Not recommended due to the need for real-time data access	Ideal for real-time access control without duplicating data
Data Access Control	N/A (data is static once masked)	Ideal for controlling who can view sensitive information. In other words, datacentric ABAC

Conclusion

Both **Static Data Masking (SDM)** and **Dynamic Data Masking (DDM)** are critical tools in ensuring data security, but they serve different purposes. **SDM** is perfect for non-production environments where data integrity and compliance are essential, while **DDM** is ideal for production environments where real-time, role-based access control is needed without impacting performance or creating duplicate data.

Choosing the right approach depends on your organization's needs, whether you prioritize **data security** in testing environments or require **real-time protection** for live production data.

📞 **Contact Us:**

If you like this document, please visit our website at www.kewdataconsultants.com for more resources designed to empower your organisation's data security strategy. From comprehensive white-papers on Data-Centric ABAC and Data Security Posture Management (DSPM) to detailed customer use cases, we offer valuable insights that you can start using right away.

👉 **What We Offer:**

• Free Downloads: Access our latest research and practical guidelines without any commitments.
• Expert Guidance: Learn how our vendor-agnostic solutions can be tailored to your specific needs.
• Ongoing Support: We provide continuous support to ensure your data security strategies are effective and compliant.

📧 **Ready to enhance your data security?**

Contact us for a free consultation or to discuss how we can assist with your specific needs. Reach out to us at contact@kewdataconsultants.com

Kew Data Consultants | Your partners in securing data integrity and compliance.

Email: contact@kewdataconsultants.com
Phone: 0044-3333395993
Location: Richmond, UK

Thank You for Choosing Kew Data Consultants