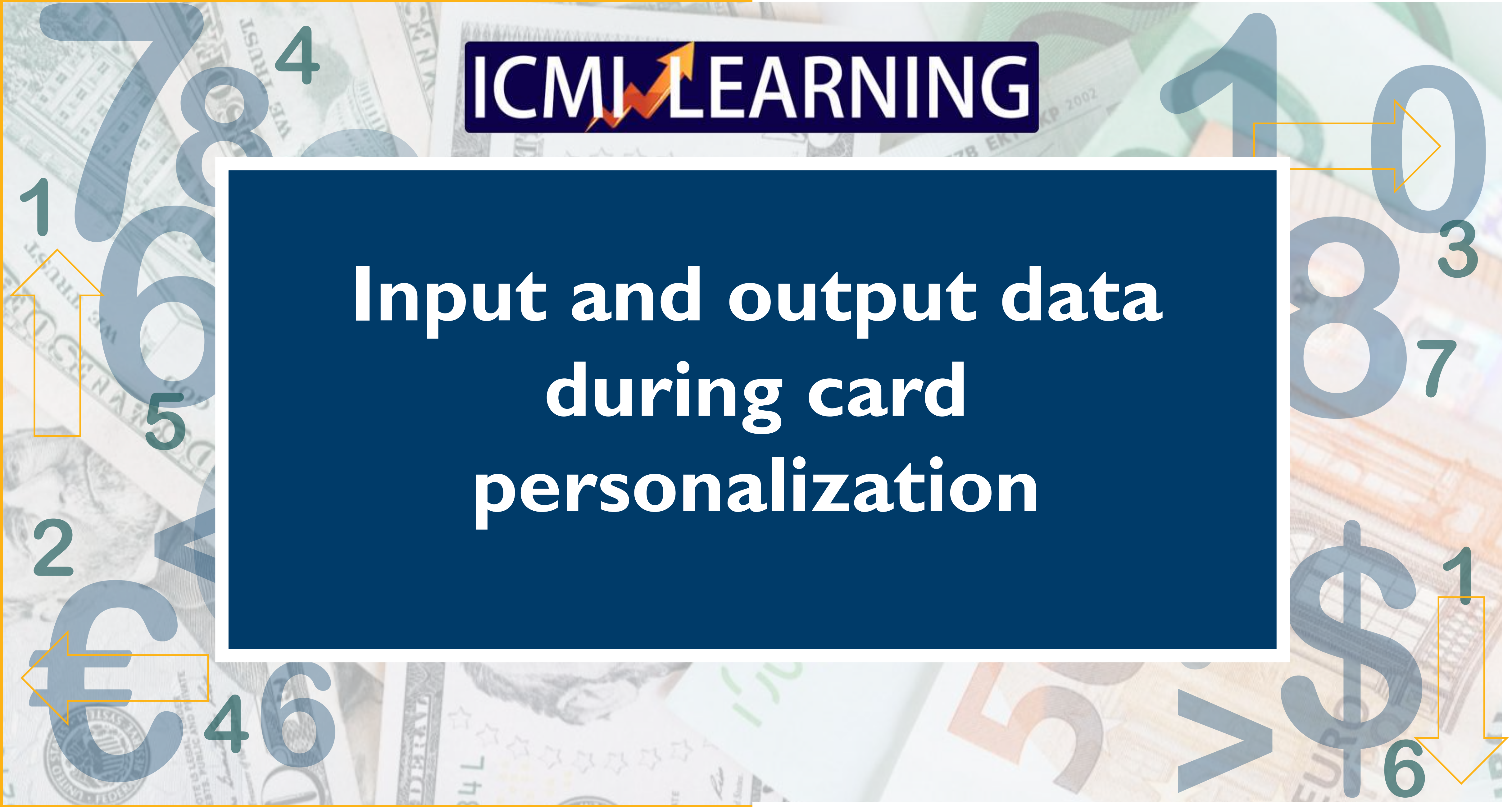


ICMI LEARNING

Input and output data during card personalization

Input and output data during card personalization

Input data include

Card application data profiles

RSA, 3DES, and AES keys and cryptographically generated data

RSA PK certificate

EMV / magstripe images

Used in the process of creating the personalized data that is stored on an EMV chip card

Input and output data during card personalization

Card application data profiles

Information about the specific application that will be installed on the card including

- Application Identifier (AID)
- Application parameters
- Other relevant information

Input and output data during card personalization

RSA, 3DES, and AES keys and cryptographically generated data

These are keys used to encrypt and decrypt data on the card

decryption of data

Encryption of data

As well as other cryptographically generated data used for security purposes

Input and output data during card personalization

RSA PK certificate

This certificate is used to verify the authenticity of the card's public key

Input and output data during card personalization

EMV or magnetic stripe image

Refers to the data that will be written to the card, such as

- Cardholder's name
- Account number
- Other relevant information

Input and output data during card personalization

Output data

Refers to the format that the personalization data will be in, once it has been processed by the personalization device, different formats are

- TLV data
- EMVCo CPS format data
- MULTOS Application Load Unit (ALU) format data
- Proprietary format data

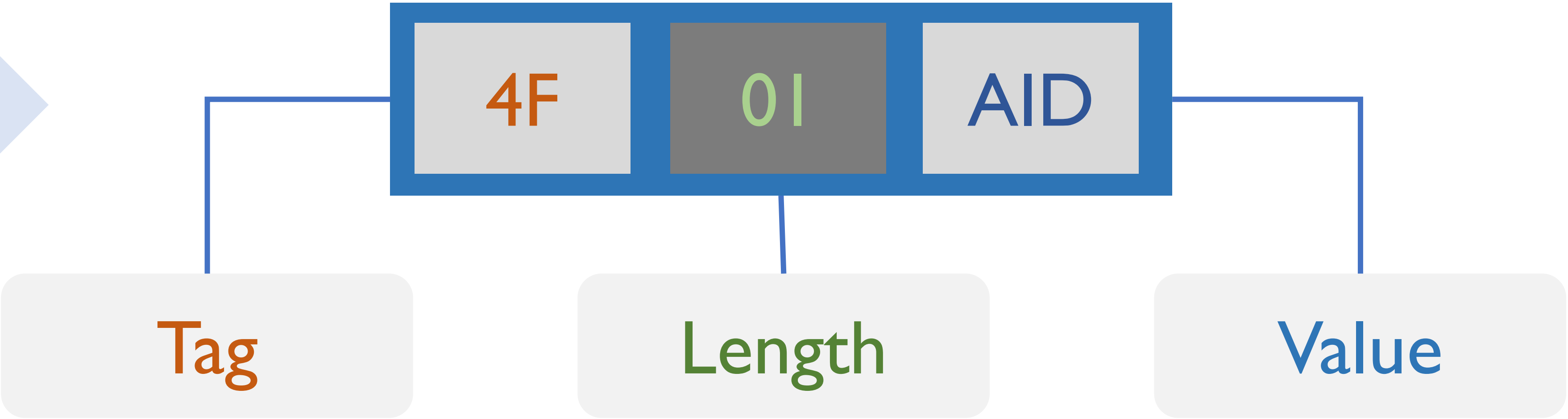
Input and output data during card personalization

❑ TLV data

TLV stands for tag-length-value a format used to encode data on the card

Include the card application profiles and other relevant information

Example



4F

01

AID

Tag

Length

Value

Input and output data during card personalization

- ❑ EMVCo CPS format data

Format is used by EMVCo, to specify the format of the personalization data

- ❑ MULTOS Application Load Unit (ALU) format data

MULTOS

MULTOS is a multi-application operating system used on some chip cards, ALU format is used to load applications onto the card

ICMI LEARNING

Input and output data during card personalization

❑ Proprietary format data

Refers to a format that is specific to a particular card issuer or personalization system

Example

VISA

card format

Input and output data during card personalization

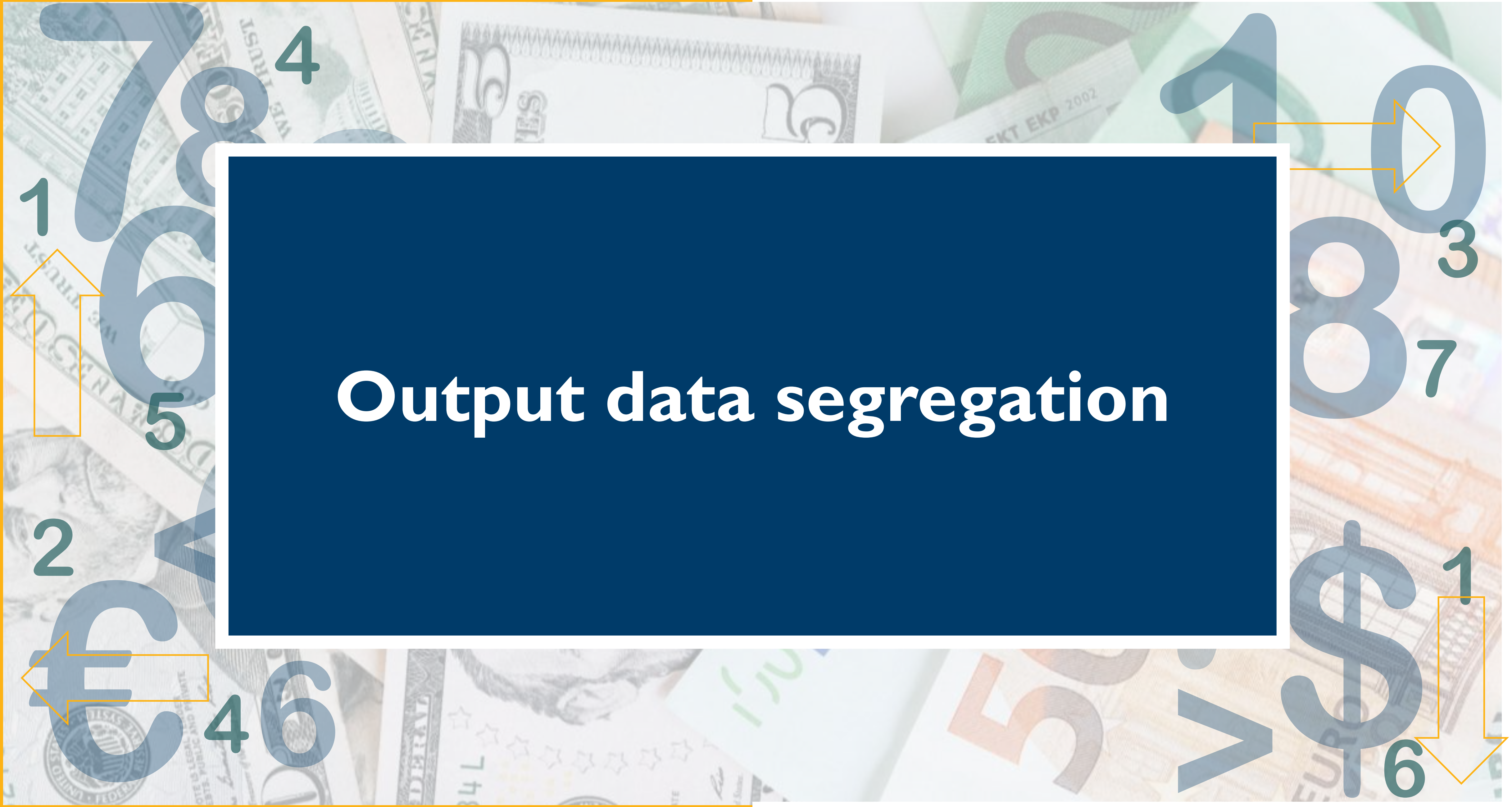
Different formats are used by different chip card platforms and systems

The choice of output data format is typically based on the specific requirements of the card issuer

The output data formats are typically designed to be compact and efficient

Also providing the necessary security features to protect the data stored on the chip

ICMI LEARNING



Output data segregation

Output data segregation

The output data can be segregated into three categories

- Issuer master keys and data
- Application keys and certificates
- Application data

Output data segregation

Issuer master keys and data

Data and keys are required for the personalization process to take place, This category is used in two ways

Secure transmission of personalization data

Create application-level data

Output data segregation

Application keys and certificates

To enable secure transactions with EMV cards, application keys and certificates must be generated during the data preparation process

Output data segregation

Application keys and certificates

To enable secure transactions with EMV cards, application keys and certificates must be generated during the data preparation process

Issuer Rivest-Shamir-Adleman (RSA) key pair

Certified by the Payment System Certification Authority

Output data segregation

Application keys and certificates

Issuer Rivest-Shamir-Adleman (RSA) key pair

Certified by the Payment System Certification Authority

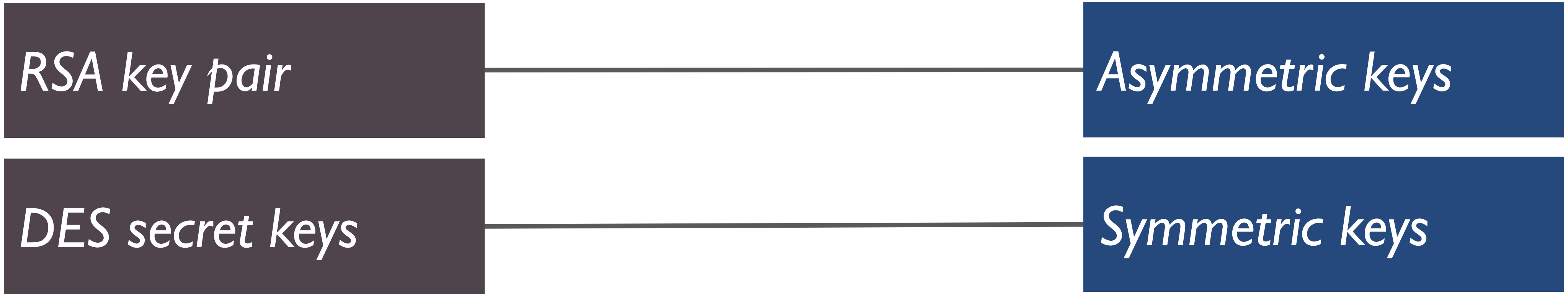
- *Static data authentication (SDA)*
- *Dynamic data authentication (DDA)*
- *Cryptographic dynamic authentication (CDA)*

Input and output data during card personalization

Application keys and certificates

Symmetric DES secret keys created at the application level for generating transaction certificates

Keys and certificates help to ensure the security and authenticity of transactions

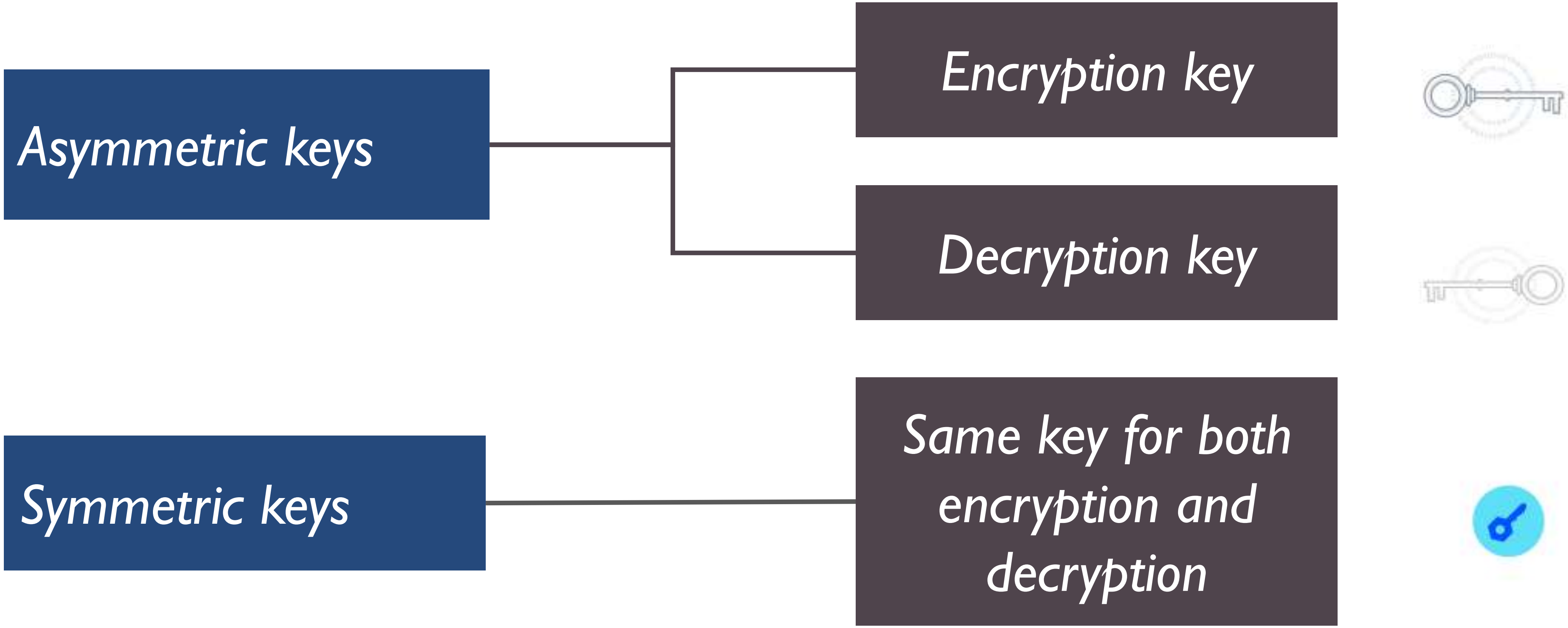


RSA key pair — *Asymmetric keys*

DES secret keys — *Symmetric keys*

Output data segregation

Application keys and certificates



Asymmetric keys

Encryption key

Decryption key

Symmetric keys

Same key for both encryption and decryption

Output data segregation

Application data

Generated during the personalization process is divided into two categories

Common data

Unique data

Output data segregation

Common data	Unique data
• *Data that is common across all IC cards issued by a particular issuer*	• *Data that is specific to an individual IC card*
• *Example, the identifier of the issuer or the issuer country code can be considered common data*	• *Example, the PAN (Primary Account Number) and expiration date of a debit or credit application are unique*

Output data segregation

Application data

Once the personalization data for an IC card application has been created, it must be grouped

Identified by	Used to
Data Grouping Identifiers (DGIs)	Organize and structure the data

DGI	8F01
Common data	

DGI	9F1A
Unique data	