European Commission

Smart Tachographs: New Security Features

Joint Research Centre (JRC)

The European Commission's in-house science service

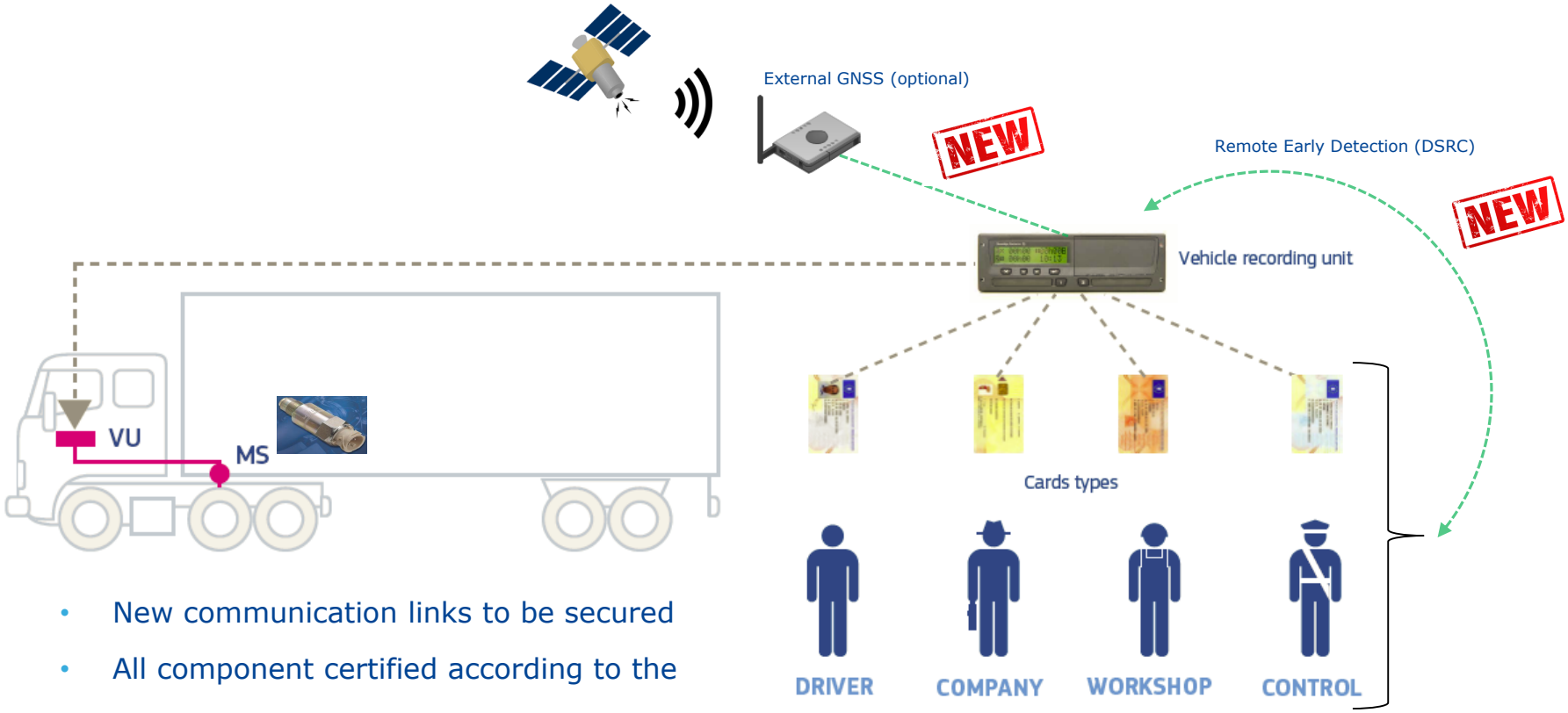
www.jrc.ec.europa.eu

Serving society - Stimulating innovation - Supporting legislation

Joint Research Centre

TACHOGRAPH FORUM
28 November 2016

The New Digital Tachograph System

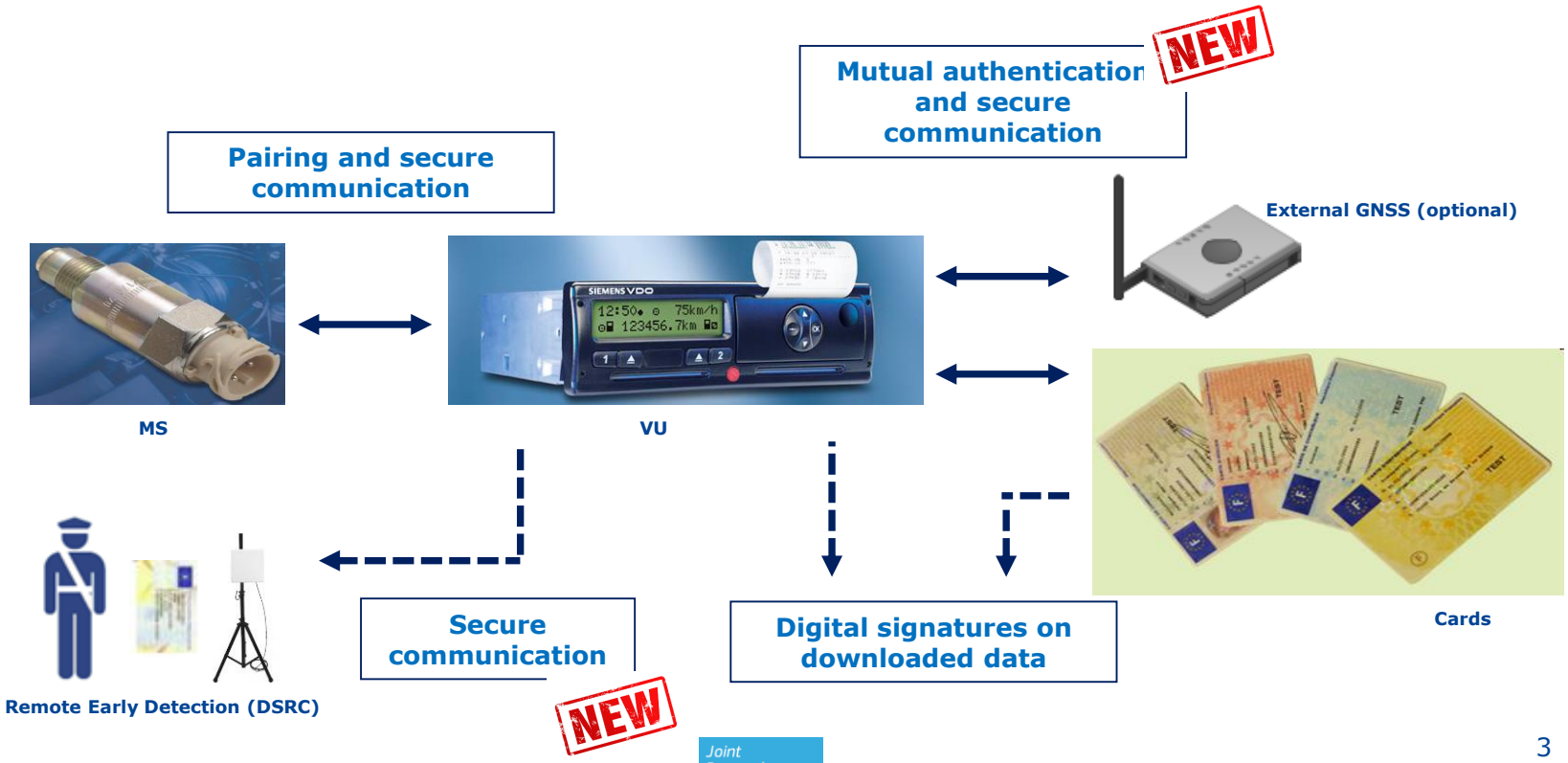


- New communication links to be secured
- All component certified according to the **Common Criteria** security scheme

NEW

Security Mechanisms

- Introduced mechanism to secure new communications links
- Existing security model kept for communication links already present



New Cryptographic Algorithms

- Cryptographic algorithms to secure the communication links completely renewed
- Public key cryptography → Elliptic Curve Cryptography (ECC), Symmetric-key cryptography → AES, Hash → SHA-2
- New format for digital certificates

ECC, SHA-2, AES, Digital Certificates

Mutual authentication and secure communication

AES

Pairing and secure communication

MS

VU

External GNSS (optional)

Cards

Early Remote Detection (DSRC)

Secure communication

AES, SHA-2

Digital signatures on downloaded data

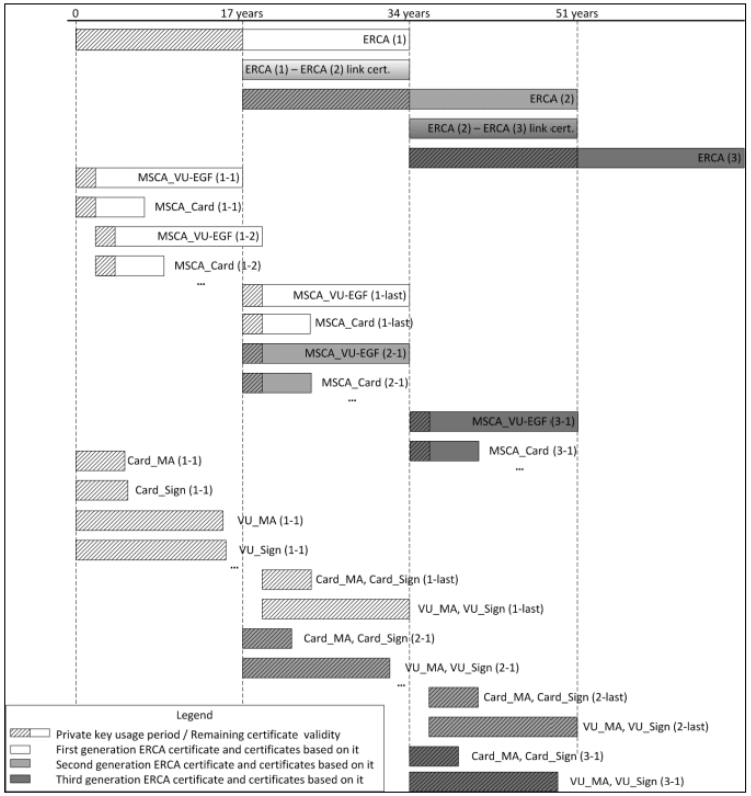
ECC, SHA-2, Digital Certificates

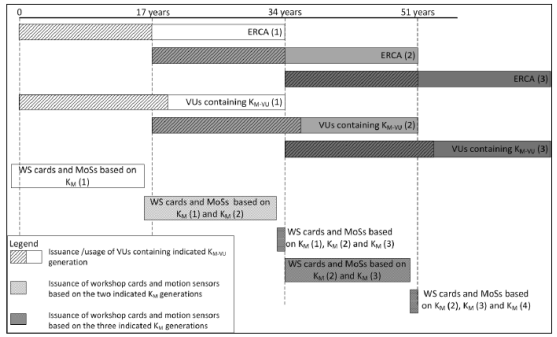
New Digital Certificates format NEW

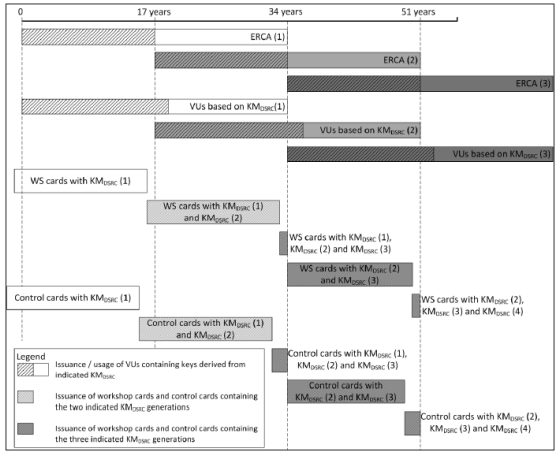
Field	Field ID	Tag	Length (bytes)	ASN.1 data type (see Appendix 1)
ECC Certificate	C	'7F 21'	var	
ECC Certificate Body	B	'7F 4E'	var	
Certificate Profile Identifier	CPI	'5F 29'	'01'	INTEGER(0..255)
Certificate Authority Reference	CAR	'42'	'08'	KeyIdentifier
Certificate Holder Authorisation	CHA	'5F 4C'	'07'	CertificateHolder Authorisation
Public Key	PK	'7F 49'	var	
Domain Parameters	DP	'06'	var	OBJECT IDENTIFIER
Public Point	PP	'86'	var	OCTET STRING
Certificate Holder Reference	CHR	'5F 20'	'08'	KeyIdentifier
Certificate Effective Date	CEfD	'5F 25'	'04'	TimeReal
Certificate Expiration Date	CExD	'5F 24'	'04'	TimeReal
ECC Certificate Signature	S	'5F 37'	var	OCTET STRING

Cryptographic Keys and Digital Certificates Validity

- All keys and certificates have an end of validity
- No cryptographic objects with undefined end of validity in the system

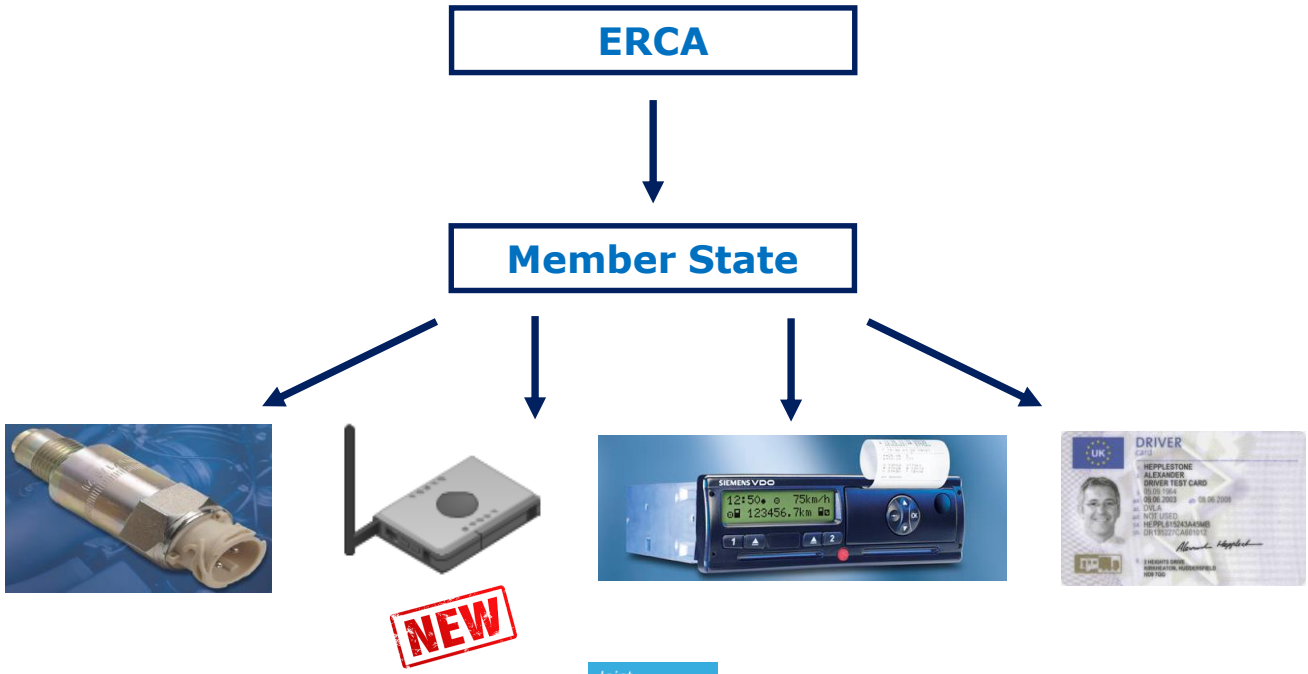






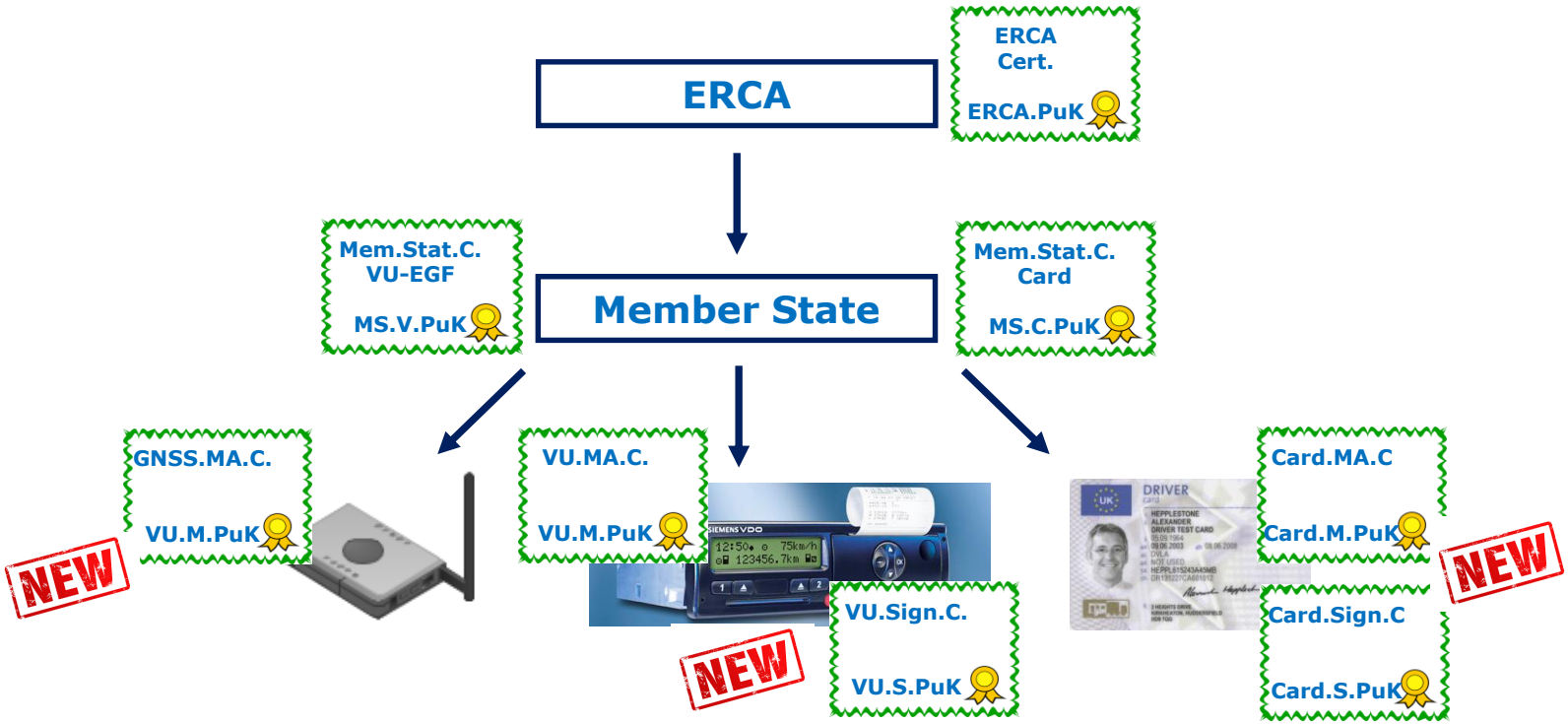
Cryptographic Infrastructure

- As before three layers infrastructure: ERCA, MSCA, DT components
- Two purposes:
  - public key infrastructure (PKI) with certificates and public/private key pairs
  - secret keys distribution
- New component in the infrastructure: external GNSS facility



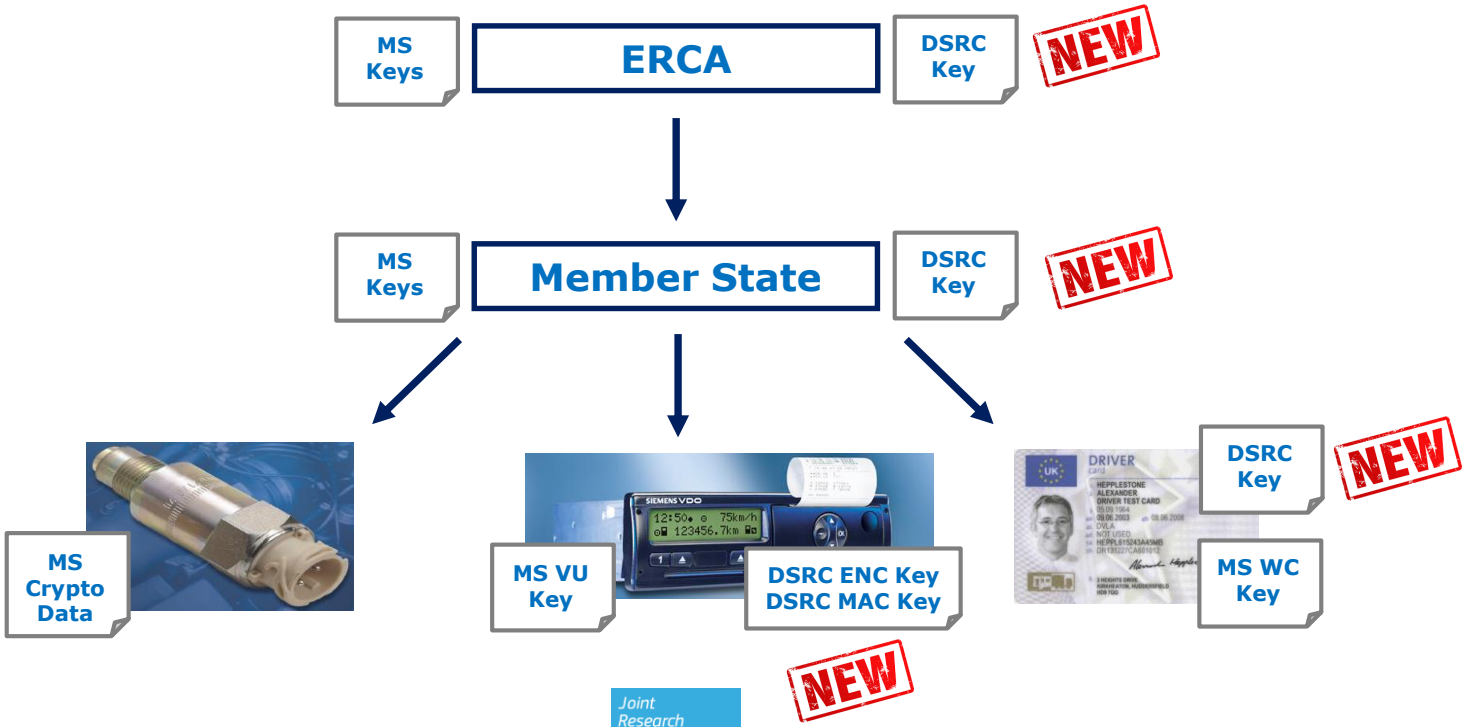
Cryptographic Infrastructure: PKI

- Now MSCAs issue two certificates for VUs and Cards
  - One for authentication and one for digital signatures
  - (signature certificate in VUs and Driver and Workshop card only)
- Now MSCAs issue certificates for the external GNSS facility as well



Cryptographic Infrastructure: Secret Keys Distribution

- Now also the secret keys to secure the DSRC channels are distributed
- MSCAs receives the DSRC master key providing it for Control and Worlshop cards
- MSCAs generates specific DSRC keys for each VU



Thank you for your attention!

Joint Research Centre (JRC)
Web: www.jrc.ec.europa.eu