PIV for PACS or MR-PIV
Mutual Registration in PIV

Gilles Lisimaque

IDTP

GLisimaque@idtp.com

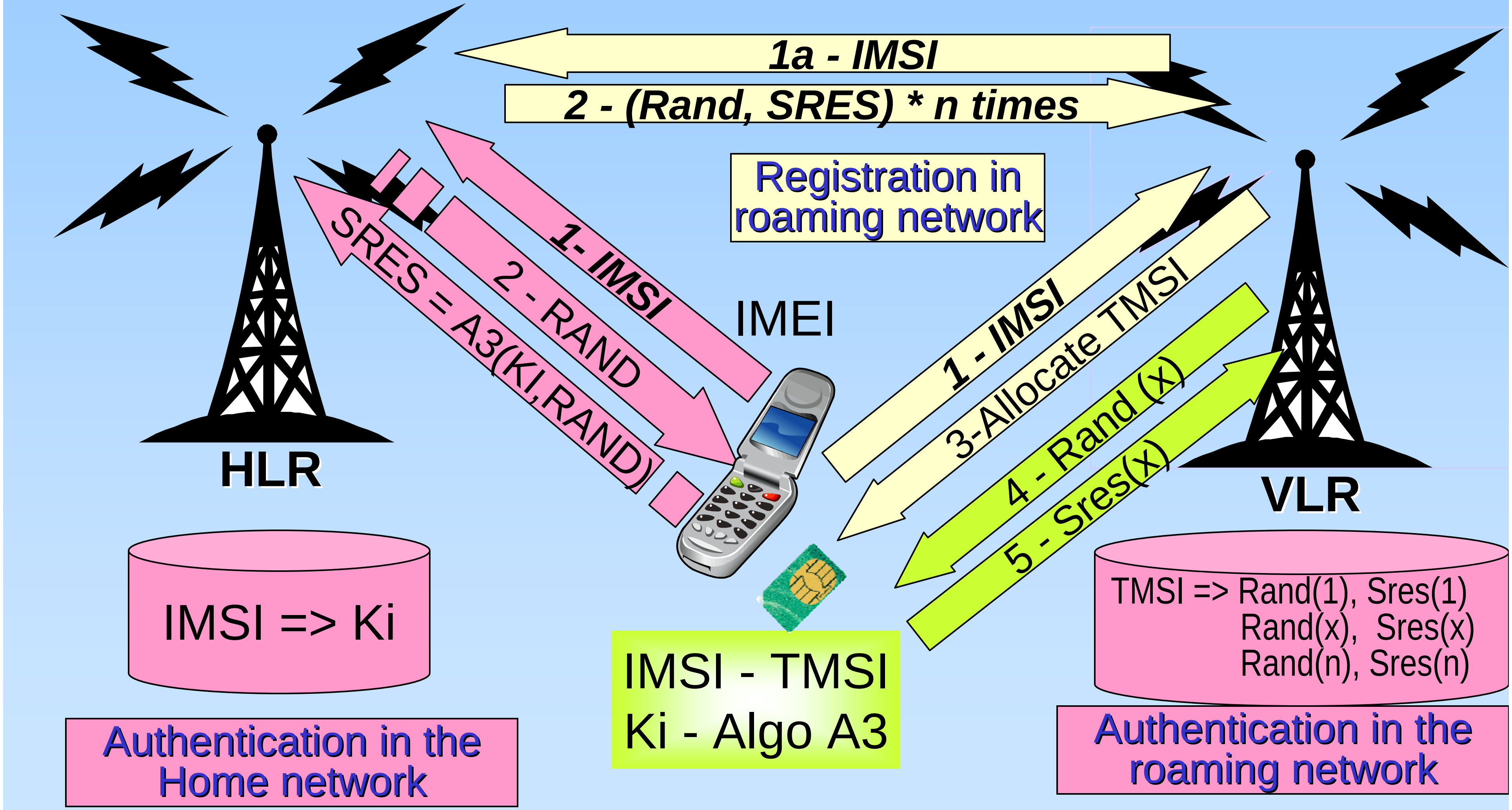
Roaming in GSM

- *One of the big success of GSM all around the world was it provided for* **authentication allowing roaming***.*
- *This allowed a cellular operator to provide service (and be paid for it) to a subscriber from another operator.*
- *The authentication mechanism was built to prevent sharing of any "operator secret" with any other operator.*

Roaming in GSM

- *The subscriber is allocated an* **IMSI (International Mobile Subscriber Identity)** *by its home network an*
- *A unique* **authentication key (Ki)** *is attached to each unique IMSI in the* **Home Location Register (HLR)** *data base*
- *When a user is roaming the* **Visitor Location Register (VLR)** *assigns a* **Temporary Mobile Subscriber Identity (TMSI)** *at registration, allocated & managed by the local system*
- *At* **registration***, the* **VLR** *uses the* **IMSI** *to get what it needs from the* **HLR**
- *A unique* **set of challenge responses** *are attached to the TMSI in the VLR and* **used for local authentication**

GSM Authentication (very simplified)



1a - IMSI

2 - (Rand, SRES) * n times

Registration in roaming network

HLR

1- IMSI

2 - RAND

SRES = A3(KI,RAND)

IMEI

1 - IMSI

3-Allocate TMSI

4 - Rand (x)

5 - Sres(x)

VLR

IMSI => Ki

IMSI - TMSI
Ki - Algo A3

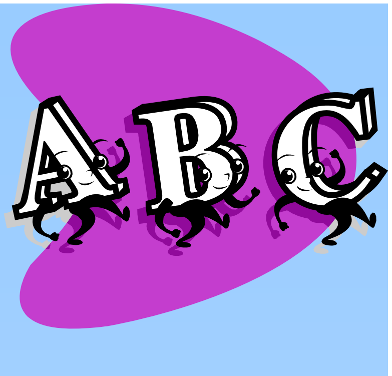
TMSI => Rand(1), Sres(1)
Rand(x), Sres(x)
Rand(n), Sres(n)

Authentication in the Home network

Authentication in the roaming network

ID TECHNOLOGY PARTNERS

GSM Acronyms



- IMSI International Mobile Subscriber Identity
(Permanent Global Subscription Identifier)
- TMSI Temporary Mobile Subscriber Identity
(Locally/Temporary Managed Identifier)
- HLR Home Location Register
(Subscriber Issuer and cellular service provider)
- VLR Visitor Location Register
(Cellular Service Access provider)
- Ki Secret Key used for active IMSI Authentication

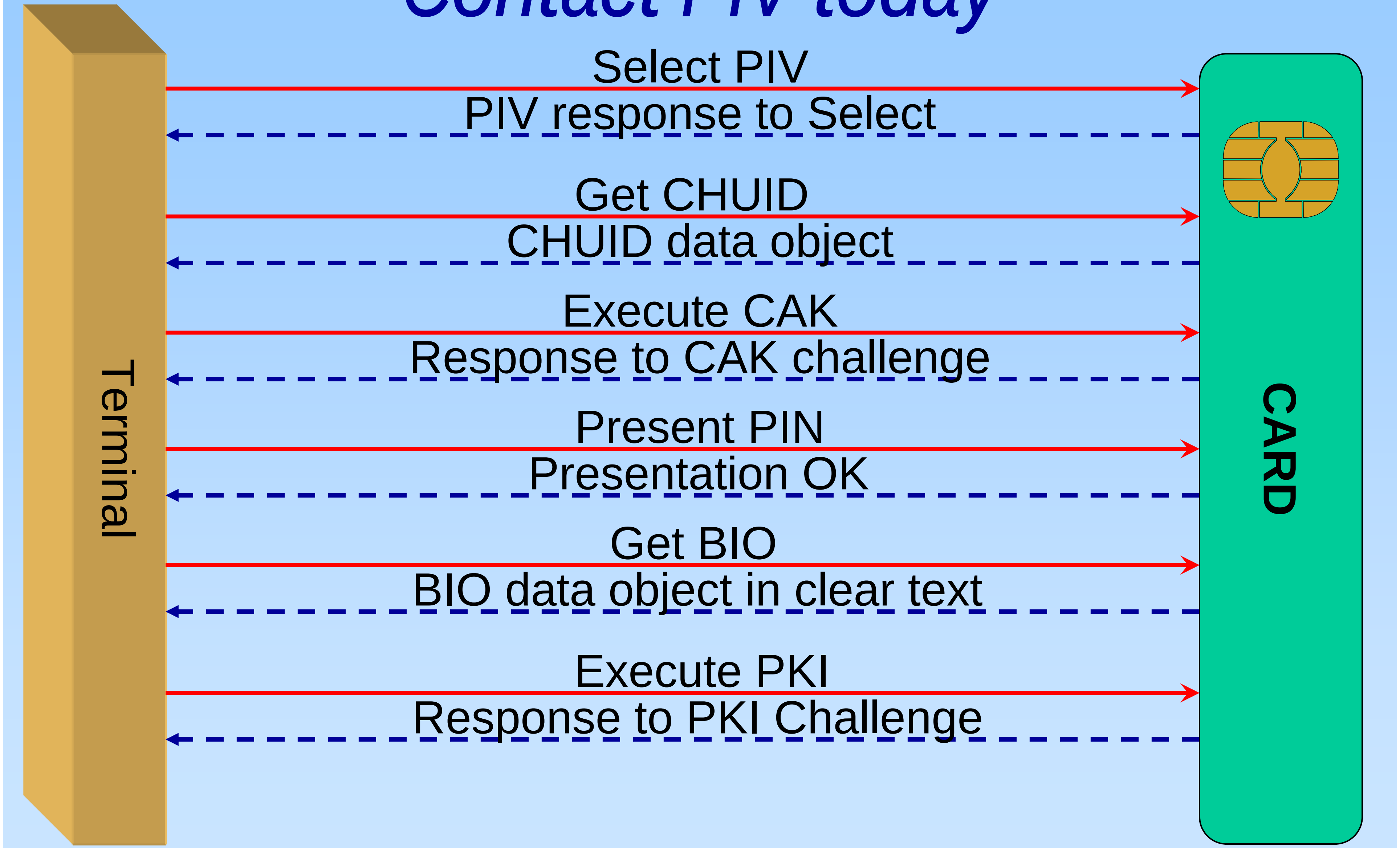
ID TECHNOLOGY PARTNERS

PIV and GSM similarities

- CHUID (Global unique identifier, similar to IMSI)
- Local identifier - No TMSI equivalent in PIV
- CAK Authentication of card (contact & contactless) (similar to Ki used for card authentication)
- PKI Authentication of user & card (contact only) (similar to Ki when PIN presentation is required)
- BIO Authentication of user (contact only) (no equivalent in basic GSM functions)

Note: In GSM the PIN presentation to the SIM by the user is optional and depends on the issuer security choices

Contact PIV today



Terminal

Select PIV

PIV response to Select

Get CHUID

CHUID data object

Execute CAK

Response to CAK challenge

Present PIN

Presentation OK

Get BIO

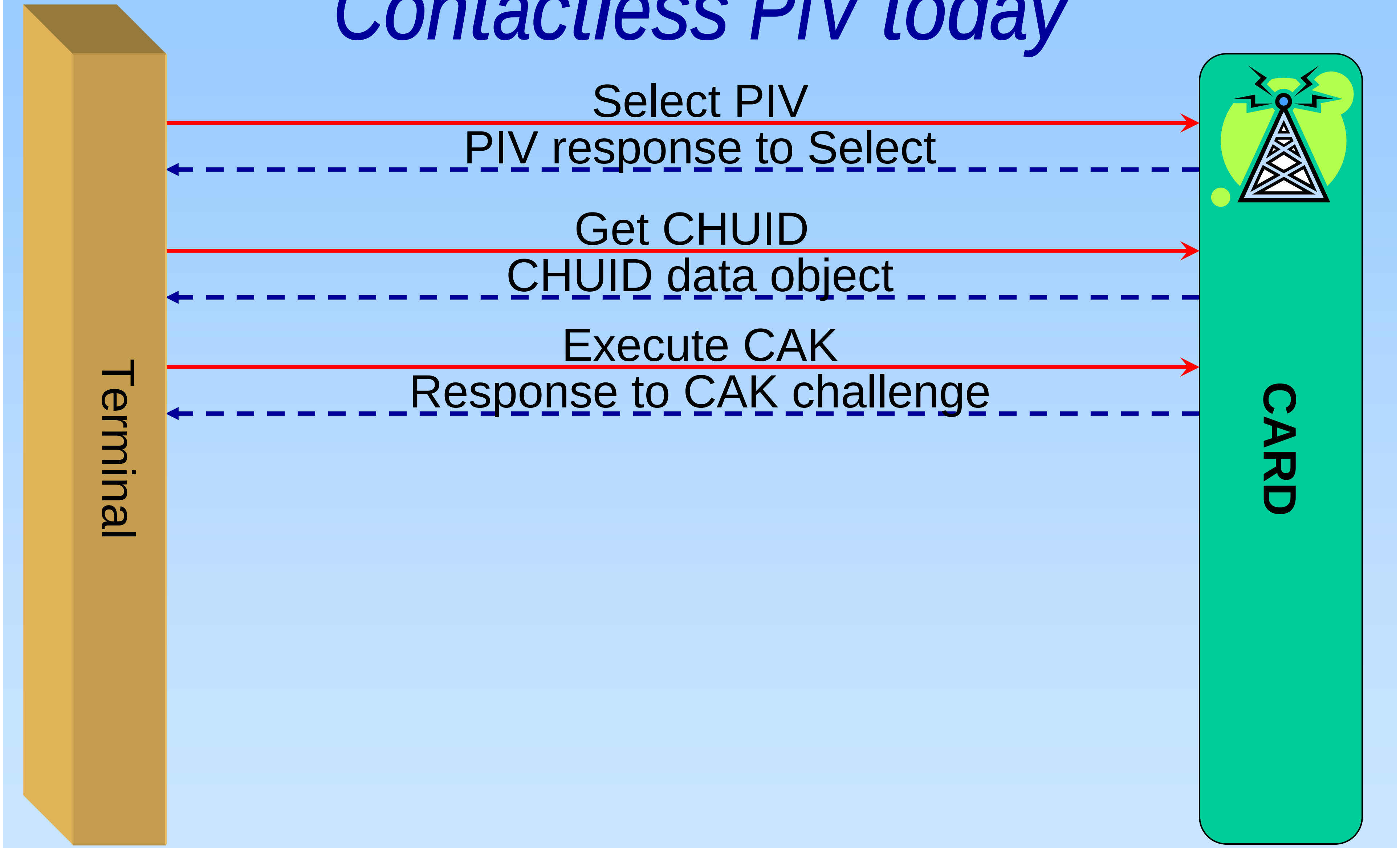
BIO data object in clear text

Execute PKI

Response to PKI Challenge

CARD

Contactless PIV today



Terminal

Select PIV

PIV response to Select

Get CHUID

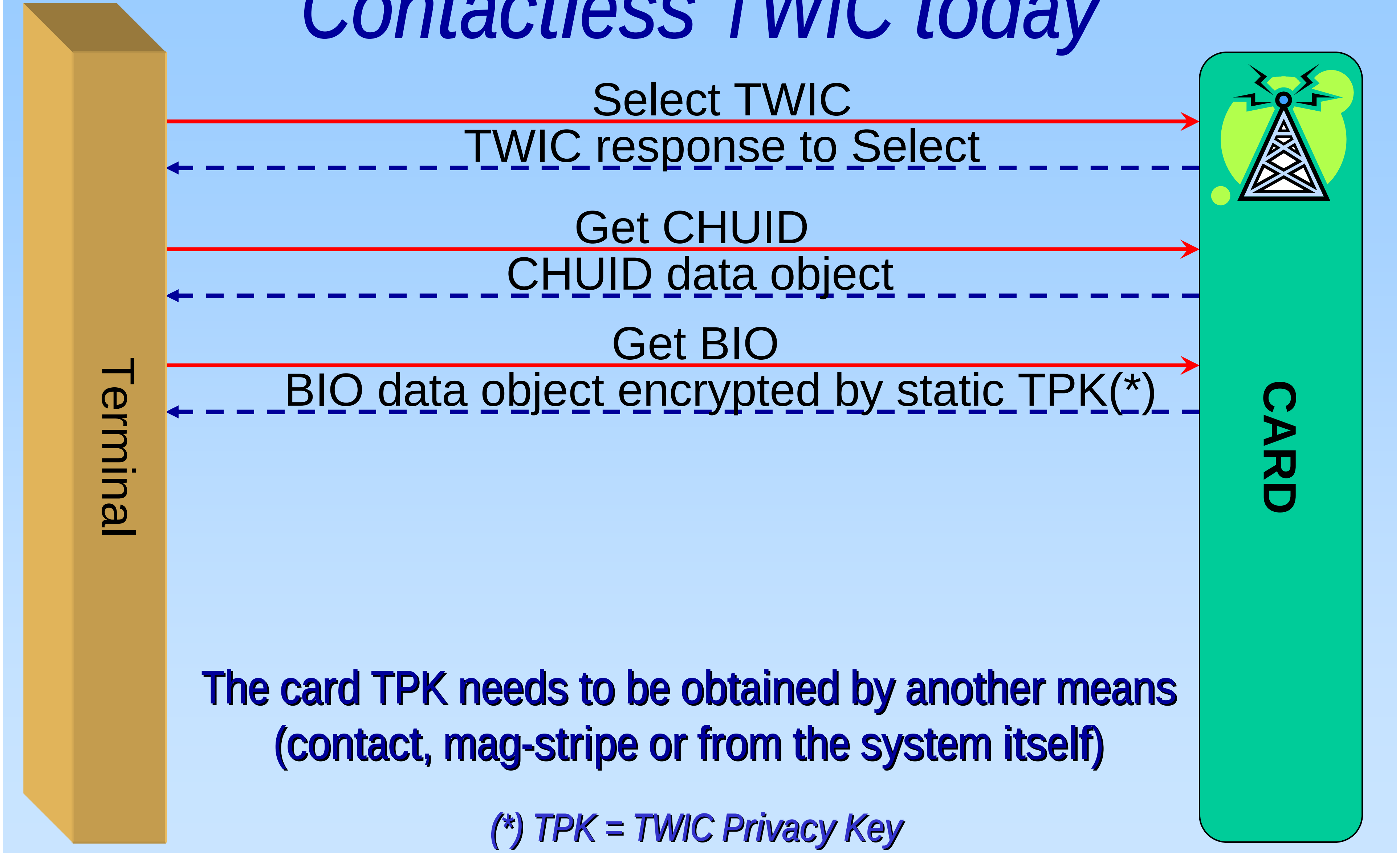
CHUID data object

Execute CAK

Response to CAK challenge

CARD

Contactless TWIC today



The card TPK needs to be obtained by another means (contact, mag-stripe or from the system itself)

(*) TPK = TWIC Privacy Key

ID TECHNOLOGY PARTNERS

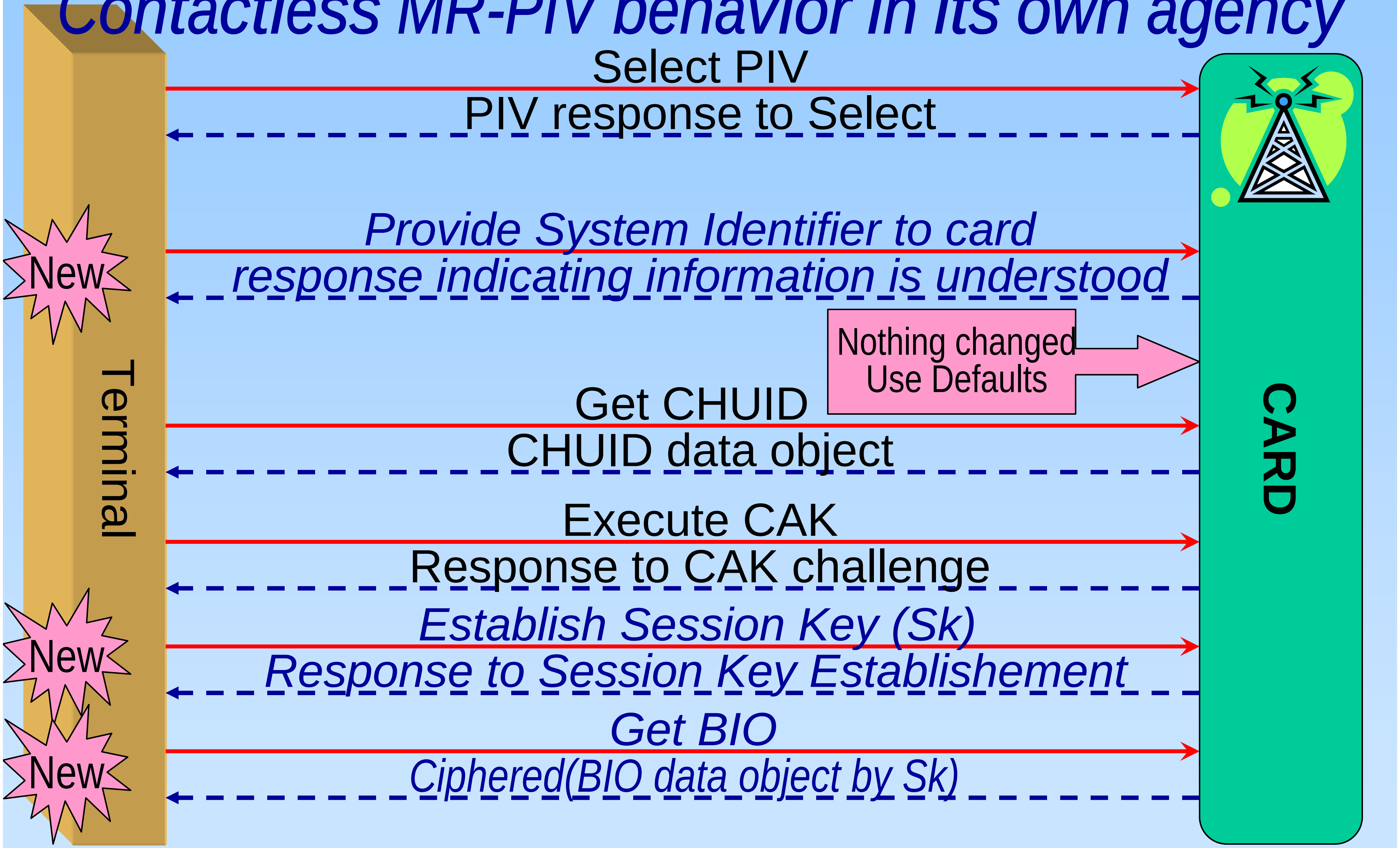
Proposed enhanced behavior

- The CAK key selected by the card could be variable depending on the system asking the question
  - Card key used for CAK is found by the card doing a lookup in a table based on the system identifier of the PACS asking to communicate
- The BIO information could be dynamically ciphered by a key depending on the system asking the question
  - Card key used to cipher the BIO is the result of a session key established from the key found in the look up table or resulting from a mutual authentication process (e.g. CAK is a symmetric diversified key)

In the following we will call such a card a MR-PIV (for Mutual Registration - PIV)

ID TECHNOLOGY PARTNERS

Contactless MR-PIV behavior in its own agency



Terminal

CARD

Select PIV

PIV response to Select

New

Provide System Identifier to card

response indicating information is understood

Nothing changed
Use Defaults

Get CHUID

CHUID data object

Execute CAK

Response to CAK challenge

New

Establish Session Key (Sk)

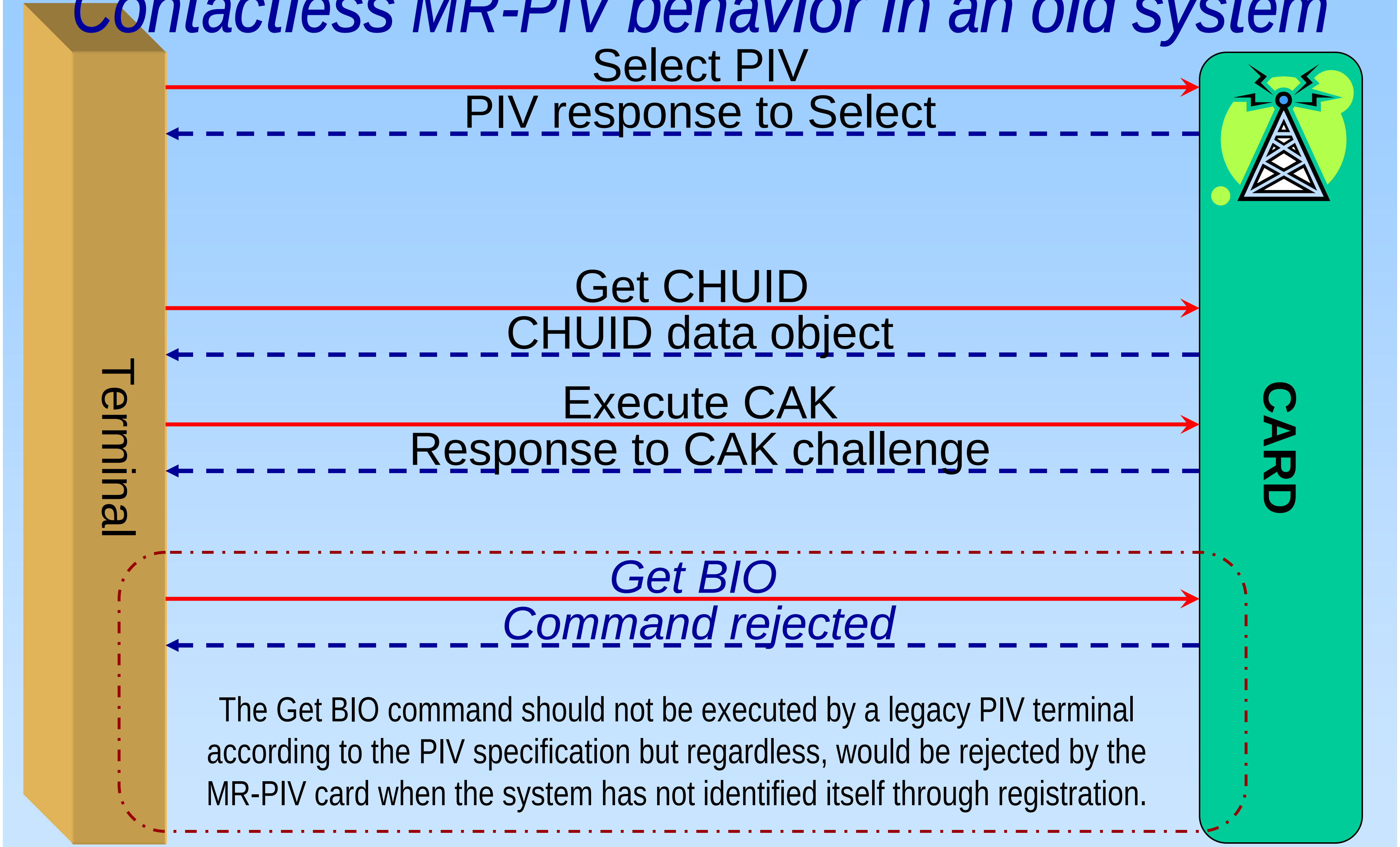
Response to Session Key Establishement

New

Get BIO

Ciphered(BIO data object by Sk)

Contactless MR-PIV behavior in an old system



Terminal

CARD

Select PIV

PIV response to Select

Get CHUID

CHUID data object

Execute CAK

Response to CAK challenge

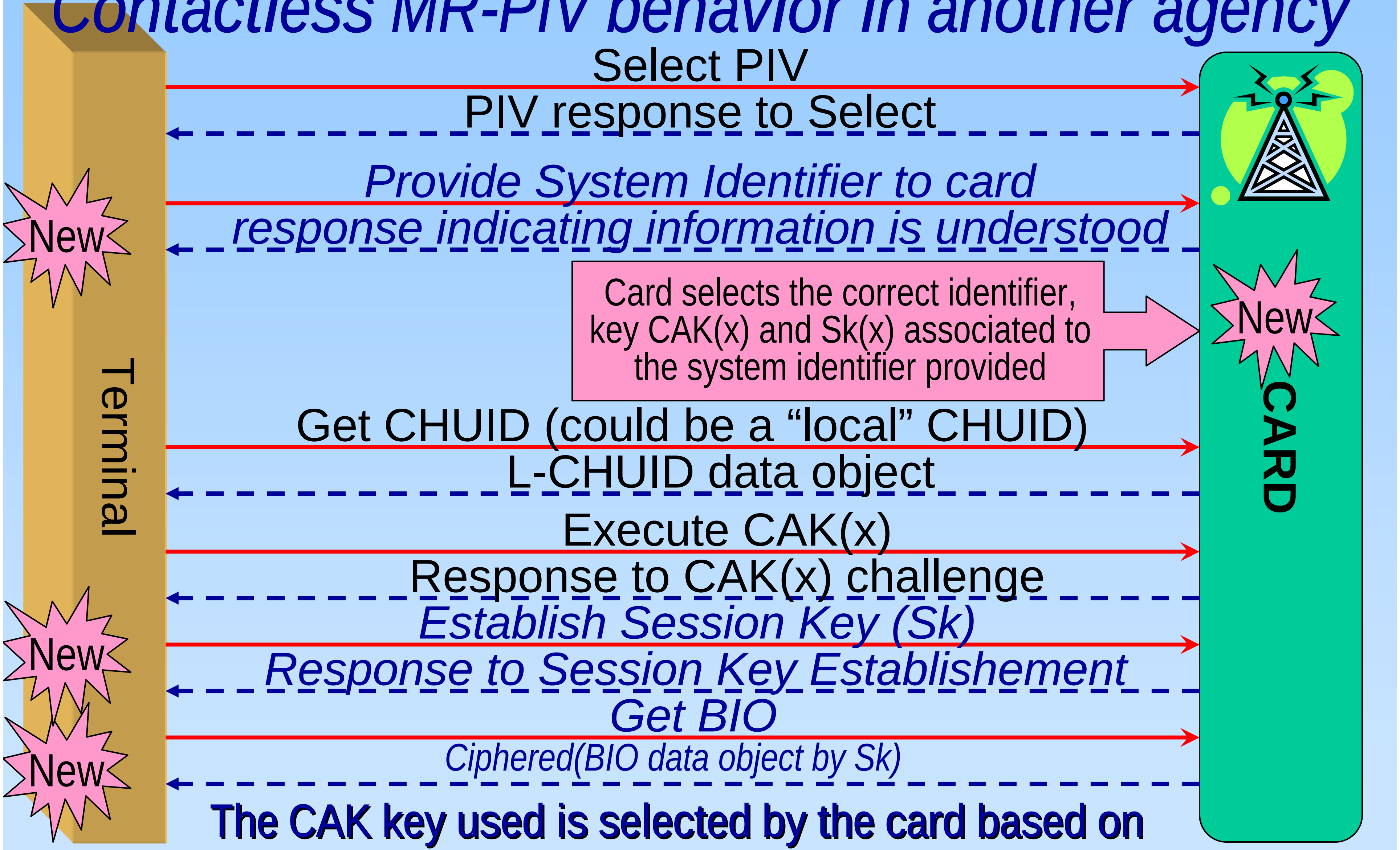
Get BIO

Command rejected

The Get BIO command should not be executed by a legacy PIV terminal according to the PIV specification but regardless, would be rejected by the MR-PIV card when the system has not identified itself through registration.

ID TECHNOLOGY PARTNERS

Contactless MR-PIV behavior in another agency



Select PIV

PIV response to Select

Provide System Identifier to card

response indicating information is understood

Card selects the correct identifier, key CAK(x) and Sk(x) associated to the system identifier provided

Get CHUID (could be a “local” CHUID)

L-CHUID data object

Execute CAK(x)

Response to CAK(x) challenge

Establish Session Key (Sk)

Response to Session Key Establishement

Get BIO

Ciphered(BIO data object by Sk)

The CAK key used is selected by the card based on the PACS System Identifier provided

Mutual Registration is required

- When a new PACS is registered in a MR-PIV card, an entry is created in the card PACS look up table:
  - PACS Identifier
    - Credential identifier to use for that PACS (Local-CHUID)*
    - CAK and Algorithm to use for this PACS
    - Session Key and mechanism to use for this PACS
- The "load new PACS" message is presented to the card ciphered by a random number chosen by the PACS.
- The random number is itself presented to the card ciphered by a public key related to the card (e.g. public key corresponding to the signing card key)

**** Same concept as a DHCP mechanism in network management***

NEW!

New commands in the MR-PIV card

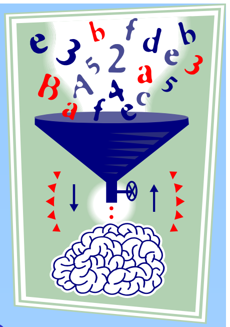
- At registration:
  - **Load PACS entry:** allows to load a new entry in the PACS look up table (ciphered message)
  - **Delete PACS entry:** When the PIN is presented the user is allowed to delete entries in the PACS look up table
- In use at PACS terminals
  - **Select PACS entry:** Sent by the PACS terminal, the PACS identifier allows the card to select the correct context

Note: When the PACS identifier is not found in the lookup table the card picks up a random value for CAK and Session Key and provides correctly formatted responses preventing a rogue system from finding which PACS is registered in the card.

New or Modified Commands in MR-PIV

- Establishment of Session Key
  - If a Symmetric key is available for CAK, it is possible to use standard mechanisms for session key establishment
- Get BIO
  - Can now return dynamically ciphered information using the session key established with the PACS
- Allows Match on Card to use the session key

All this works on the contact as well as the contactless interface and supports Match on Card privacy requirements



New Data Objects in MR-PIV

- No apparent change in the CAK at the interface
  - The value and algorithm used may change depending on the PACS selected but as only one instance if ever “seen at the interface” at any time, it becomes a value which depends on the context.
- L-CHUID
  - Identifier possibly allocated by a given PACS when a card is registered. This number is a PACS local identifier which could be different from the CHUID.

Based on the PACS system identifier the card presents a logical VIEW

Example of a look up table in the card

Site ID	Local- CHUID	Divers.	Algo CAK	CAK	Algo SK	Mutual A. Key
Issuing Agency	A1234	none	RSA 2048	a9b8e6	AES	caeb123
SDRT	95647	95647	3DES	prty142	== CAK	== CAK
....	....	....	......	....	.....	....
Other Agency	69679	69679	AES	6c548f	3DES	65ae34c

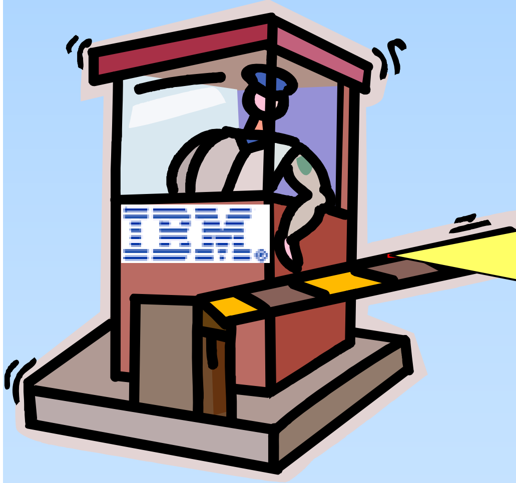
MR-PIV

No need for a common standardized unified privilege number used in PACS

The site has to actively identify itself to the MR-PIV card in order to set the context for the access privilege it is looking for.

PACS Identifier

PACS id	Authentication	Privilege #
DoD	Algo(x)+Key(z)	#13725#
IBM	*Algo(3)+Key(4)*	*AbC45&9*
IDTP	Algo($)+Key(&)	UFO666



Authentication Mechanism (Algorithm + Key)

Privilege Number

Basic ID data for interoperability & User authentication

The MR-PIV credential contains (and protects) a lookup table for the multiple privileges obtained by the legitimate bearer of the ID credential

Improved flexibility Backward compatibility

- Mutual authentication and session key establishment are proposed in this presentation but may create issues in strict backward compatibility with existing PIV or TWIC systems (e.g. not all existing systems support two algorithms for CAK keys)
- As the new modified MR-PIV relies on the new command by which the requesting system identifies itself to the card, backward compatibility can be preserved as the card without the requesting system identifying itself will behave as “before” in a default environment.

Conclusion:
The work just begins!

- This presentation proposes a working direction and does not pretend to be, in any way, a complete technical description.
- The concepts presented are taken from GSM implementations combined with Pay-TV and e-purse management functions which have both been used in numerous smart card systems for many years