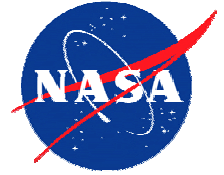


# **Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems Version 2.2**

Tim W. Baldrige  
October 7, 2004

# Purpose



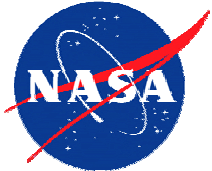
- Define specifications and standards for physical access control systems (PACS), such that these systems will:
  - Operate with the Federal Agency Smart Credential (FASC).
  - Facilitate cross-agency, federal enterprise interoperability.
  - Allow existing legacy PACS to operate with FASC compatible card readers until the time comes for its upgrade

# CHUID Data Model



(Card Holder Unique Identifier) CHUID File / Buffer		EF 3000	Always Read
Data Element	Tag	Type	Max. Bytes
Buffer Length	EE	Fixed	2
FASC-N (SEIWG-012)	30	Fixed	25
Agency Code	31	Fixed	4
Organization Identifier	32	Fixed	4
DUNS	33	Fixed	9
GUID	34	Fixed	16
RFU	35-3C		
Authentication Key Map	3D	Variable	TBD
Asymmetric signature	3E	Variable	TBD
Error Detection Code	FE	LRC	1

# Federal Agency Smart Credential – Number (FASC-N)



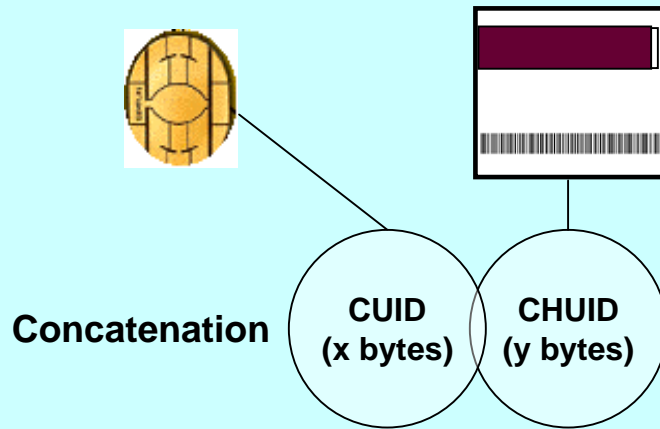
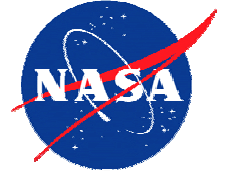
SS	AGENCY CODE	FS	SYSTEM CODE	FS	CREDENTIAL NUMBER	FS	CS	FS	ICI	FS	PI	OC	OI	POA	ES	LRC
1	4	1	4	1	6	1	1	1	1	1	10	1	4	1	1	1

# Assurance Profiles

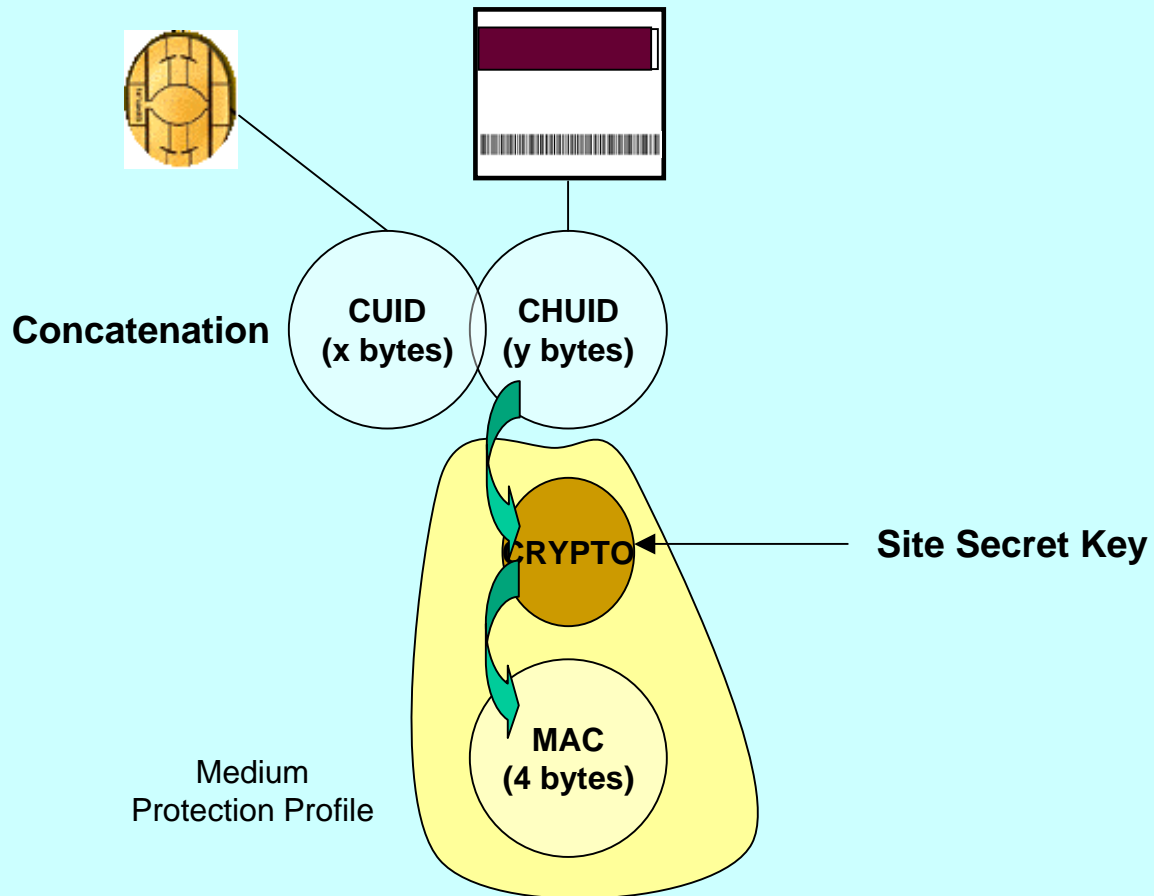
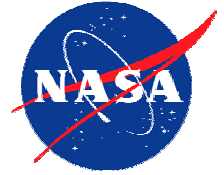


- Low – Basic Interoperability
  - Free read CHUID (Card Holder Unique Identifier)
  - Transmit {56bit:CHUID}
- Medium – Validated Data
  - Free read CUID + CHUID
  - Reader computes MAC
  - Transmit {56bit:CHUID, 32bit:MAC}
- High – Authenticated Token (Contact Only)
  - Free read CUID + CHUID
  - Reader computes MAC and KEY
  - Reader authenticates card with KEY
  - Transmit {56bit:CHUID, 32bit:MAC, z:Status}

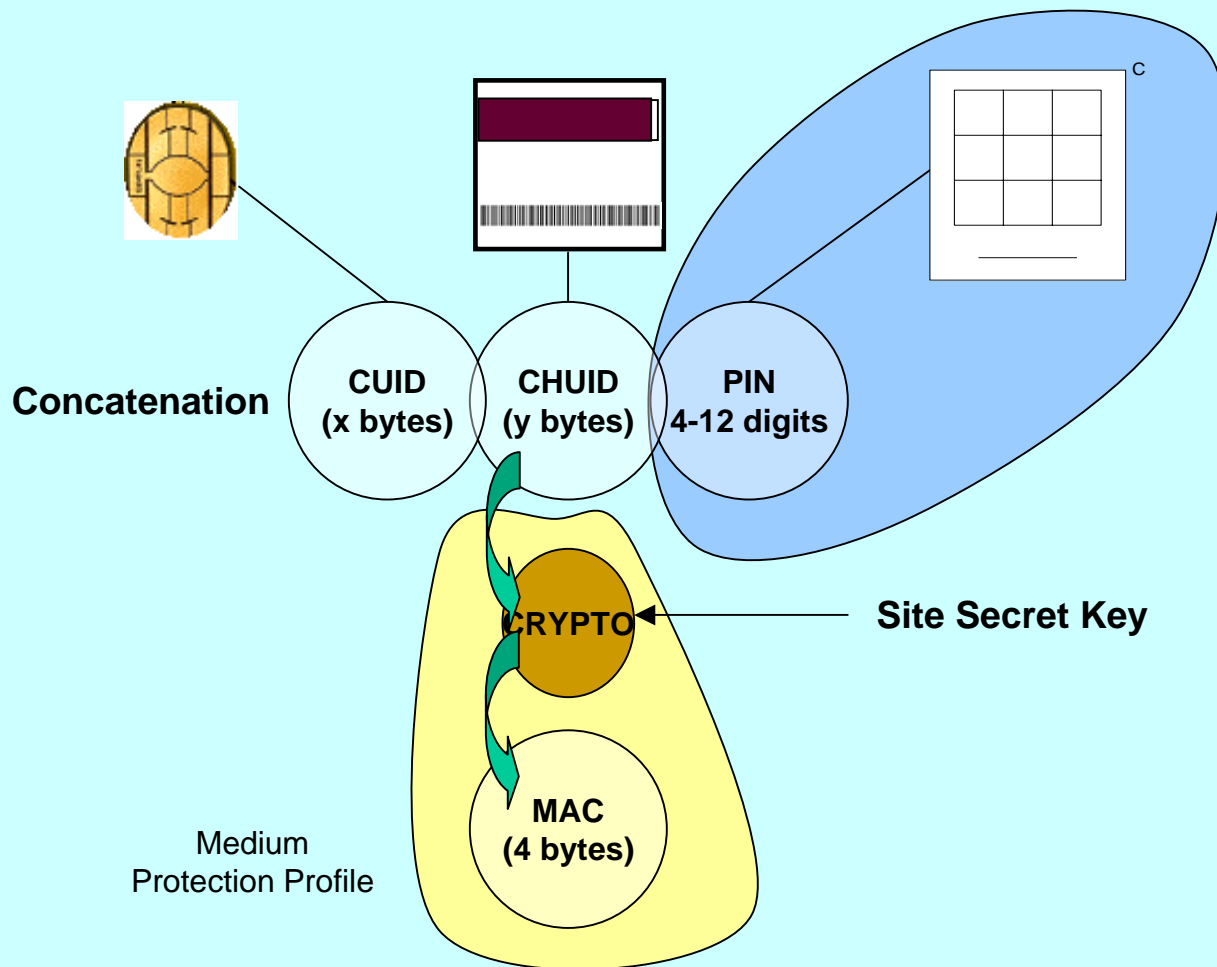
# Low Assurance Profile



# Medium Assurance Profile



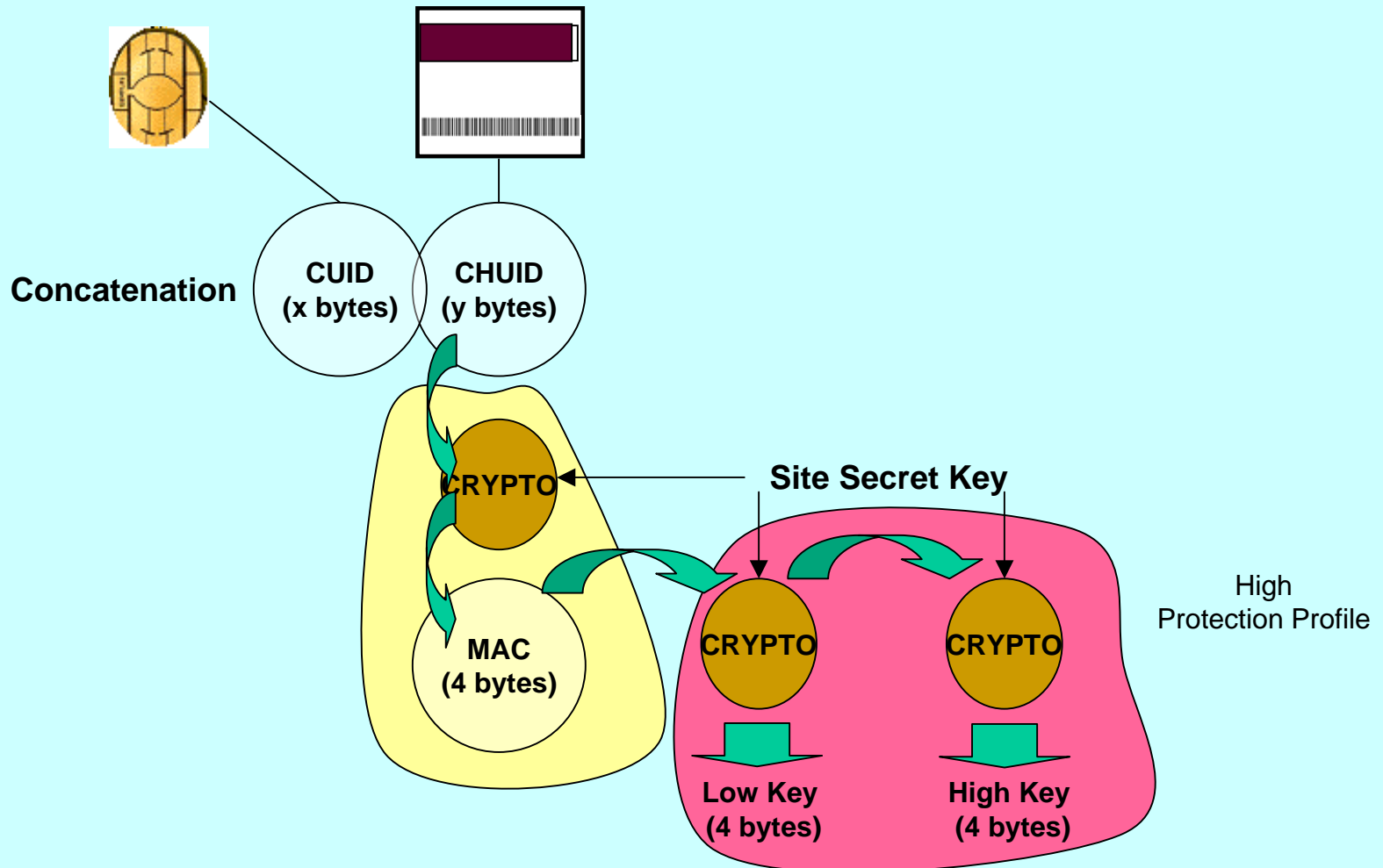
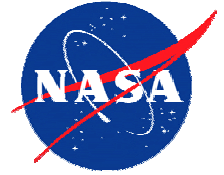
# Medium Assurance Profile w/PIN





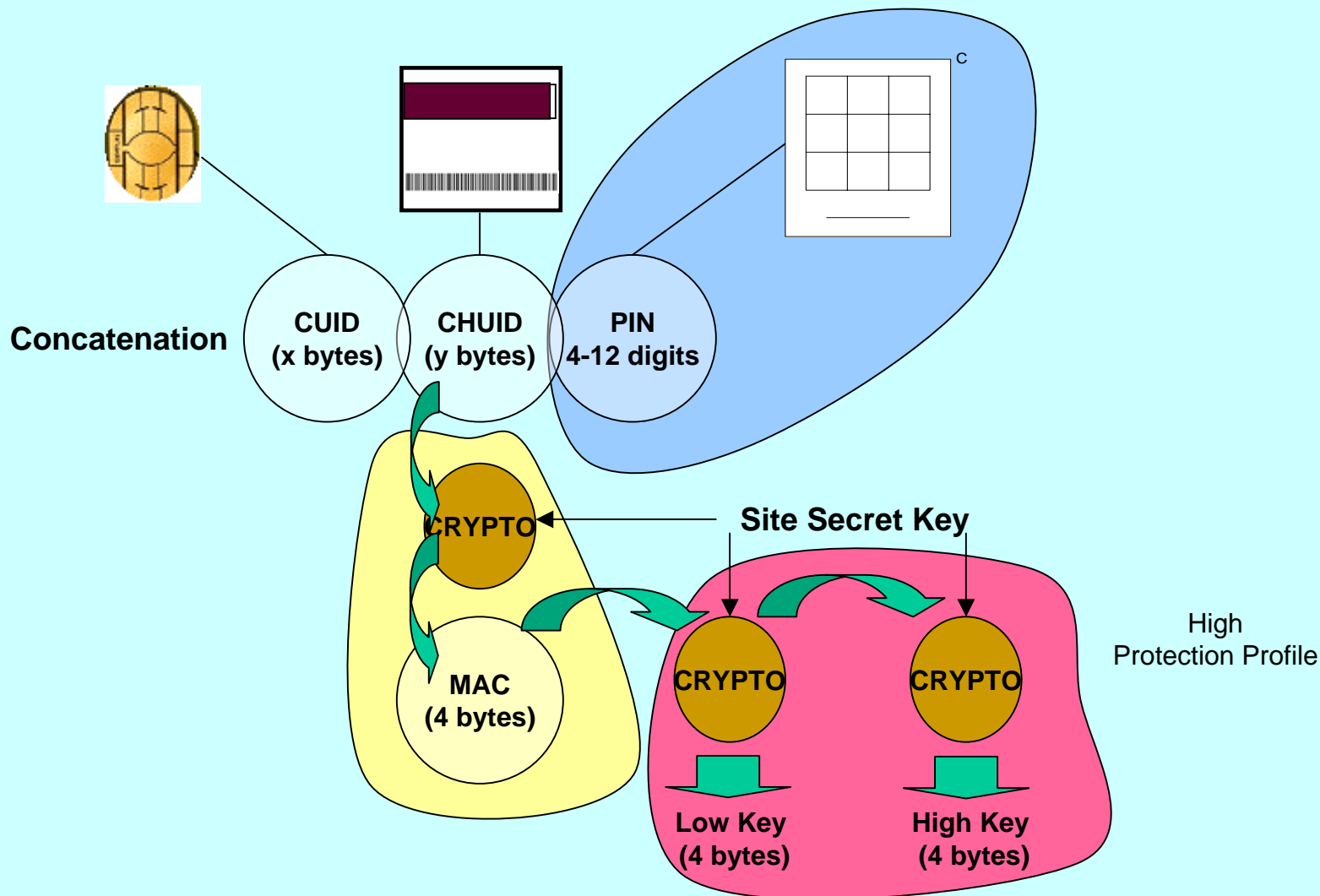
# High Assurance Profile

(Contact Card Only)



# High Protection Profile w/PIN

(Contact Card Only)



# Possible Reference Standards for Physical Access PIN Management



- ANS X9.8 / ISO 9564
  - Banking – PIN Management and Security
- ISO 11568
  - Banking – Key Management