Calypso

Networks Association

Calypso Open Tech Day

OpenSAM – Round Table

1

Recap

Calypso
Networks Association

The OpenSAM is…

- …truly ***open*** with a licence and certification policy based on the same principles as for the card
- …meant to ***firstly*** address ***new markets***
- …based on an entirely ***new specification*** that integrates more that 20 years of CNA's members shared experience to optimise and simplify operations
- …***free of archaisms*** inherited from the past
- …***agnostic*** of platform and form factor

Product Development Plan

- Phased Development for faster Go To Market
  - Phase 1:
    - Minimum set of SAM Management commands
    - Calypso Light/Basic Command Set
  - Phase 2:
    - Calypso Prime Regular mode Command Set
    - Complete SAM Management commands
  - Phase 3:
    - Calypso Prime Extended mode Command Set
    - Business Rules management

2

Status

Phase 1

Calypso
Networks Association

Calypso OpenSAM Status

Card Transaction

Draft of the Specification available since 31st July 2023.

Open for **feedback**!

Initialization & Management

Draft of the Specification coming early 2024

Certification

Definition of the certification scheme began in October 2023

3

Main Features

Calypso
Networks Association

Issuance Level

- The Open SAM ensures that the **ownership of the keys always belong to the network** regardless of the SAM supplier or Key Ceremony Supplier
- Use cases like adding other SAM providers or the generation of extra keys are covered from the start by the design of the OpenSAM
- Using a trust chain asymmetric model with CNA on top
- Taking inspiration of standards defined by Global Platform with an open certificate format better suited for the SAM reality

Management Level

- The OpenSAM is designed to be included in a multi-application platform bringing a greater level of flexibility
  - Allowing to have multiple OpenSAM instances allowing a greater isolation of functions and roles between OpenSAM Applications in the same secure element
  - Co-existence with other technologies
  - Supporting several form factors
- Supporting the capability for remote updates from the start ensuring that any product placed in the field has a bigger lifespan
- Conceived from the beginning to be flexible and evolvable bringing a new level of future proofing (e.g. Possibility to evolve the keys to bigger lengths)

Card Transaction Level

- **Keyple compatible and optimized from the start**
- Better operation traceability
  - Adds **greater control on counter manipulation** bringing Stored Value like security to Calypso Light and Basic
  - Allows to audit the entire data that was exchanged with the card
- Optimized transaction flow with the combination of multiple commands in a single command
  - **Optimized from the start for both local and remote transactions**
- Clearer key roles and less chance to make mistakes
  - **Improves and simplifies the design** and configuration of new SAM applications **reducing the dependency** on a small number of experts

4

Specification

A brief glance

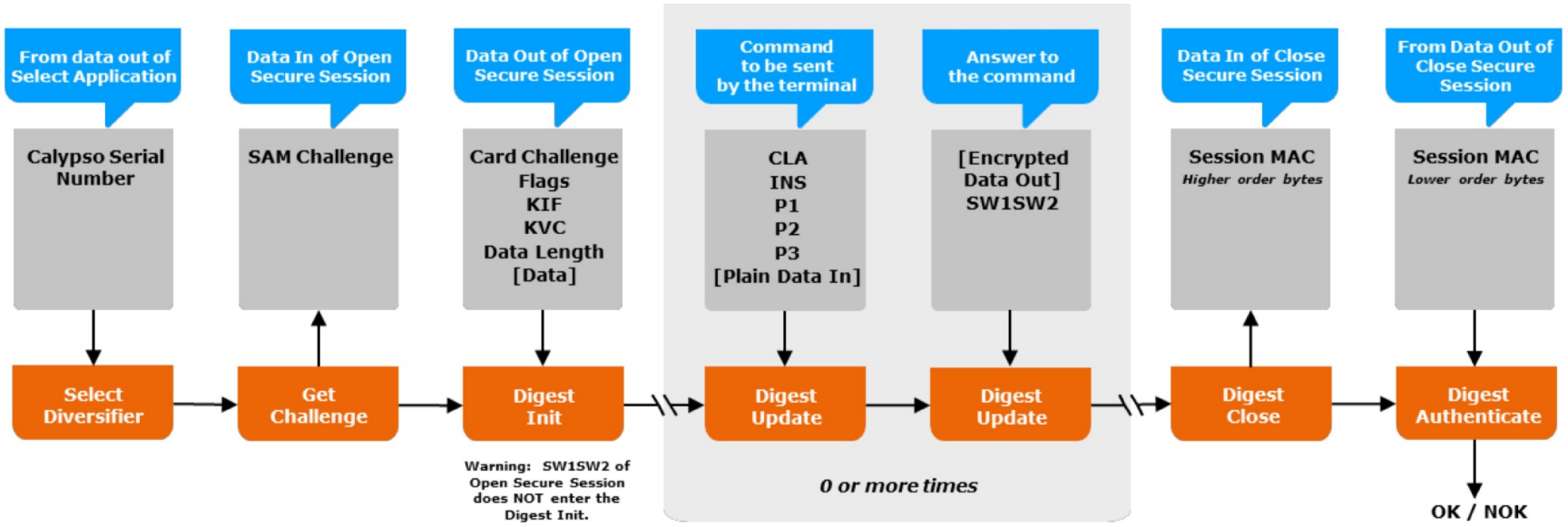
Calypso
Networks Association

SAM Application Typification

Category	*Value*	*Description*
SAM Management	01_H	Master: Can generate all other SAM Applications
	02_H	Key Loading: Can load keys into other SAM Applications
	03_H	Key Management: Can update max counter values, disable/delete keys, etc.
Card Management	10_H	SAM Applications for Card Transaction (e.g., Loading, Validation, etc.).
	11_H	SAM Applications for Card Pre-personalization (key loading).
Data Management	20_H	Data Validation: Can verify signatures, data objects, etc.

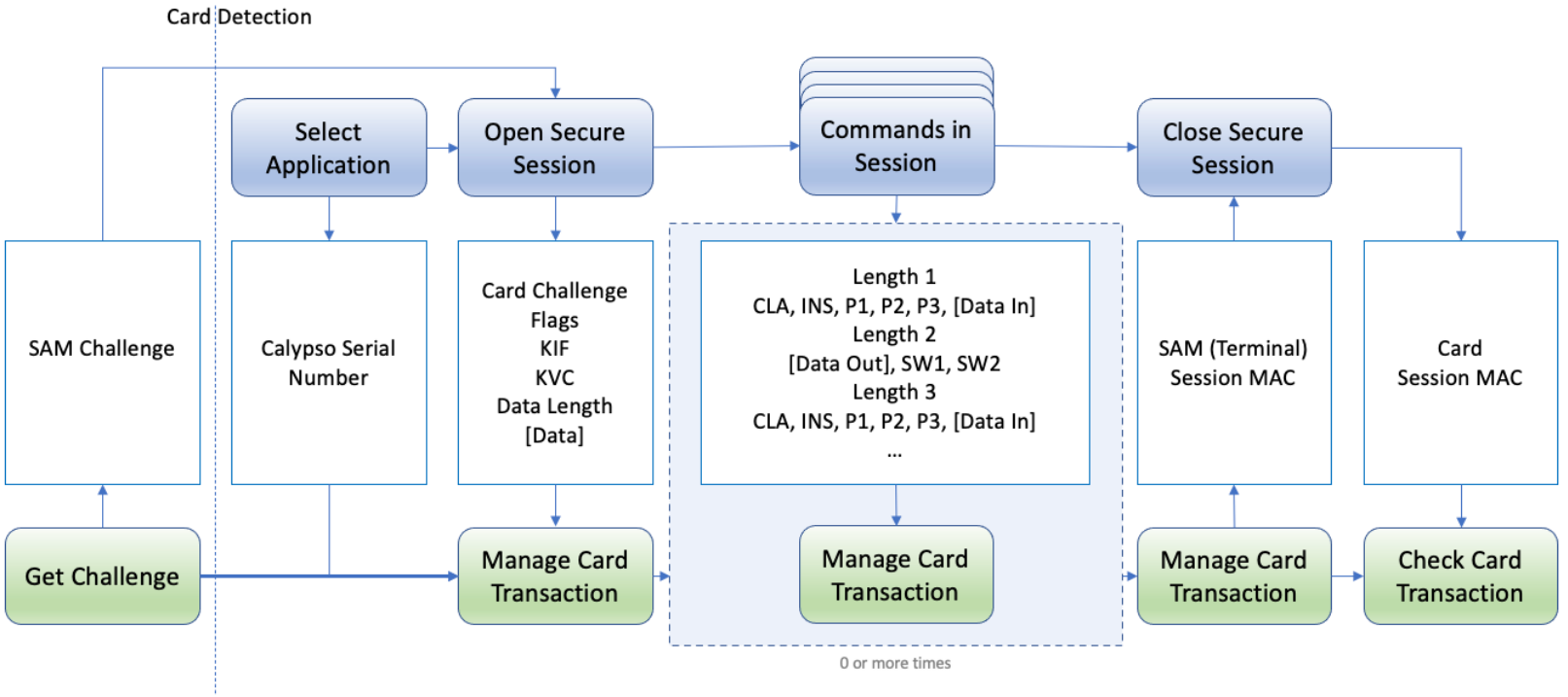
Command	*Usage Value*					
	01	*02*	*03*	*10*	*11*	*20*
Select Application	*	*	*	*	*	*
Get Response	*	*	*	*	*	*
Verify Application Password	*	*	*	*	*	*
Get Card Key Data					*	
Get Card Key Bundle					*	
Get Challenge				*		
Manage Card Transaction				*		
Check Card Transaction				*		
Prepare Card Transaction Audit				*		
Audit Card Transaction				*		*
PSO Compute Digital Signature				*		
PSO Verify Digital Signature				*		*

Updated Transaction Flow



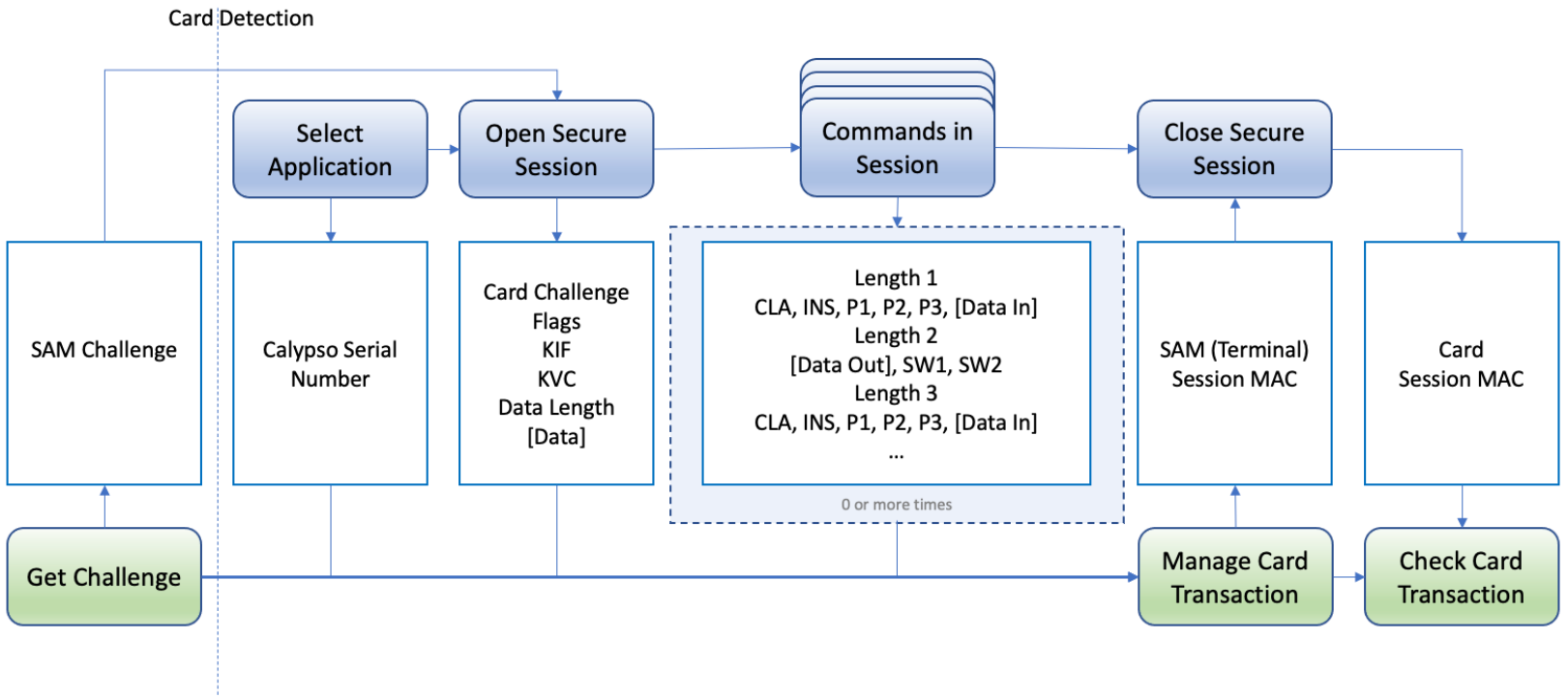
Calypso Networks Association

Updated Transaction Flow



Calypso Networks Association

Updated Transaction Flow



Calypso Networks Association

New Key Bundle Formats

OpenSAM signed/ciphered Key Bundle format

The signature is calculated using the LEN byte in clear and the rest of the Key Bundle ciphered.

Signature (16 bytes)	**Keys Global Data**		**Key #1**	
	Key LEN (1 byte)	ALG (2 bytes)	Identifier (2 bytes)	Key Value (LEN bytes)
			Key #2	
			Identifier (2 bytes)	Key Value (LEN bytes)
			Key #3	
			Identifier (2 bytes)	Key Value (LEN bytes)

Ciphered

OpenSAM plain Key Bundle format

The plain format is derived from the signed and ciphered format.

Keys Global Data		**Key #1**	
Key LEN (1 byte)	ALG (2 bytes)	Identifier (2 bytes)	Key Value (LEN bytes)
		Key #2	
		Identifier (2 bytes)	Key Value (LEN bytes)
		Key #3	
		Identifier (2 bytes)	Key Value (LEN bytes)

Traceability & Counters

- Operations Counter
- Value Counter
  - Linked to Calypso Stored Value Keys
  - Linked to Calypso Session Keys
- Traceability Control
  - Linked to Calypso Session Keys
  - Linked to Value Counter Restrictions