



## WORKPACKAGE 6 Disposable media

Draft

In use

Obsolete

Sum up

## Foreword

### Author



### Editor



## Revision list

Version	Date	Author	Modifications
1.0	09/06/23		Reference, version number, table of contents
1.1	09/06/26		Revision list, reference, spelling

## References

Title	Version	Storage location / Url link

## Table of contents

1	Introduction.....	4
2	Objectives.....	5
3	Presentation of products manufacturers .....	6
3.1	NXP .....	6
3.2	INFINEON.....	6
3.3	ST MICROELECTRONICS .....	6
3.4	ATMEL.....	6
3.5	ASK .....	6
4	Calypso Memory Chips.....	6
4.1	New functionalities .....	6
4.2	Security and memory chips .....	6
5	Protection features.....	6
6	Security management on CTM512B .....	6
6.1	Anti-clone function .....	6
6.2	Certificate.....	6
6.3	Security features .....	6
	CTM512B security features are against:.....	6
7	SAM architecture implementation .....	6
8	Security in Memory Chips .....	6
9	Second part of WP6.....	6

# 1 Introduction

ASK, leader in manufacturing and supply of contactless tickets has brought its product experiences to help public transport companies in short-term tickets deployment. This kind of product provides an effective solution for occasional travellers.

All existing products use different command sets which are not completely ISO-compliant. This involves constraints on readers and it implies integration of each product (chip).

This work package has for objectives to evaluate constraints which lead to the creation of several specific command sets and to ponder how to realise a shared command sets to all memory chips.

ASK has invited silicon manufacturers to join the working group as they are at the origin of the chip technical specifications. Their involvements were essential to credible conclusions of this study and the implementation of those conclusions

## 2 Objectives

This work package is the only one with prospective view. All features of existing products will be brought together to define one unique, or into identical characteristics. This would avoid the set of command multiplicity and the different SAMs.

This product should answer to occasional or immediate usage needs and bring all necessary security features to prevent ticket's cloning.

At least two manufacturers should agree to specify this product.



### 3 Presentation of products manufacturers

#### 3.1 NXP

A family of product low cost type A: Mifare UL and Mifare UL II

FUNCTIONALITIES/CHIP NAME	Mifare Ultralight	Mifare Ultralight II
RF interface, Compatibility, EEPROM	ISO 14443-A  512 bits	ISO 14443-A to Mifare Ultralight  1500 bits
<b>Security:</b>		
Unique S/N	7 byte UID	7 byte UID
OTP area	32 bits	32 bits
Memory Write protection	Yes	Yes
Authentication	No	Yes
Key length	n/a	112 bit
SAM	n/a	available
Other features		Counter
<b>Miscellaneous:</b>		
Anti-collision	Yes	Yes
Typical transaction time	35 ms	35 ms
Typical communication distance	10 cm	10 cm
Write endurance	5 years/10 000	5 years/10 000



### 3.2 INFINEON

- MIFARE 1K memory type A
- A family owner My-d proximity. A light-memory of 1K will be available.

FUNCTIONALITIES/CHIP NAME		
	Infineon Mifare	my-d® proximity
RF interface,	13,56 MHz	13,56 MHz
Compatibility,	ISO14443-3	ISO14443-3
EEPROM	1KByte	5120 Byte
<b>Security:</b>		
Unique S/N	yes	yes
OTP area	no	no
Memory Write protection	each block of 16 bytes	each block of 8 bytes
Authentication	3 pass mutual Authentication	4 path mutual Authentication
Key length	48 bit	64 bit
SAM	no (Reader IP)	yes
Other features		ECC correction
		flexible memory concept
		supports multiapplication
<b>Miscellaneous:</b>		
Anti-collision	yes	yes
Typical transaction time	100 ms	100ms
Typical communication distance	up to 10 cm	up to 10 cm
Write endurance	100000 erase/write cycles at 25°Cel	100000 erase/write cycles at 25°Cel



### 3.3 ST MICROELECTRONICS

Type B family: SRI 512/ SRT 512

FUNCTIONALITIES/CHIP NAME					
	ST19 platform - 8 bit			ST23 platform - 8/16 bit	
	ST19WR02	ST19WR08	ST19NR66	ST23YR16	ST23YR80
RF interface,	ISO 14443/B	ISO 14443/B	ISO 14443/B	ISO 14443 A/B	ISO 14443 A/B
Compatibility,	ISO 7816	ISO 7816	ISO 7816	ISO 7816	ISO 7816
EEPROM	2 KBytes	8 KBytes	66 KBytes	16 KBytes	80 KBytes
<b>Security:</b>					
Unique S/N	Yes	Yes	Yes	Yes	Yes
OTP area	Yes	Yes	Yes	Yes	Yes
Memory Write protection	EEPROM ctrl register	EEPROM ctrl register	EEPROM ctrl register	EEPROM ctrl register	EEPROM ctrl register
Authentication	Yes	Yes	Yes	Yes	Yes
Key length	DES : 2 * 64 bits	eDES : 2 * 64 bits	eDES : 2 * 64 bits	eDES : 2 * 64 bits	eDES : 2 * 64 bits
SAM					
Other features					
<b>Miscellaneous:</b>					
Anti-collision	Yes	Yes	Yes	Yes	Yes
Typical transaction time					
Typical communication distance	0-10 cm	0-10 cm	0-7 cm	0-10 cm	0-10 cm
Write endurance	500kcycles	500kcycles	500kcycles	500kcycles	500kcycles



### 3.4 ATMEL

Family AT88 : From 1kbits to 64 kbits.

Algorithm develop and licencing by ELVA. It could be integrated in a SAM.

Memory is divided by area. Mutual authentication, 64 bits key, data encryption possible.

FUNCTIONALITIES/CHIP NAME		AT88SC0104CRF	AT88SC0204CRF	AT88SC0404CRF	AT88SC0808
RF interface,		ISO 14443-B	ISO 14443-B	ISO 14443-B	ISO 14443-B
Compatibility,		Type B	Type B	Type B	Type B
EEPROM		1K bit	2 Kbit	4 Kbit	8 Kbit
<b>Security:</b>					
Unique S/N		YES	YES	YES	YES
OTP area		YES	YES	YES	YES
Memory Write protection		YES	YES	YES	YES
Authentication		YES	YES	YES	YES
Key length		64 bit	64 bit	64 bit	64 bit
SAM		Software	Software	Software	Software
Other features		Encryption	Encryption	Encryption	Encryption
<b>Miscellaneous:</b>					
Anti-collision		YES	YES	YES	YES
Typical transaction time		106 kb/s	106 kb/s	106 kb/s	106 kb/s
Typical communication distance		5 cm	5 cm	5 cm	5 cm
Write endurance		100 K cycles/10 yrs	100 K cycles/10 yrs	100 K cycles/10 yrs	100 K cycles/10 yrs



### 3.5 ASK

Type B family: CTS512B and CTM512M

FUNCTIONALITIES/CHIP NAME	CTS-512-B	CTM-512-B
RF interface, Compatibility, EEPROM	ISO 14443 B Calypso 512 bits	ISO 14443 B Calypso 512 bits
<b>Security:</b>		
Unique S/N OTP area Memory Write protection Authentication Key length SAM Other features	64 bits 128 bits Yes per sector Simple static N/A Optional	64 bits Variable Yes per sector Simple dynamic 80 bits diversified YES One way counter
<b>Miscellaneous:</b>		
Anti-collision Typical transaction time Typical communication distance Write endurance	Yes <100ms 10 cm 100 000 cycles	Yes <200ms 10 cm 100 000 cycles

## 4 Calypso Memory Chips

### 4.1 New functionalities

Tickets are product dedicated for the occasional or immediate usage need.

The standard set of command is not mandatory, and a new memory organisation may be more useful than a harmonized set of commands. So, the solution to the occasional needs could be a ticket with little additional functionalities:

Security functions for ticket is an important topic, and first of all, authentication function might be useful to stop cloning issues.



## 4.2 Security and memory chips

As microprocessor prices will not decrease enough to be a solution for disposable media, the management of access rights in memory writing can prevent the copy of data. And, to prevent the ticket's cloning on a different media, it's maybe necessary to add cryptography (such as SRiX4K or CTM512B).

WP6 recommends that those methods of protection and tools such as integration with SAM or API should be integrated in Calypso.

Some products are already available, such as:

### ST Products

Without security : SRi512, SRT512, SRi4K

With security : SRiX4K

### NXP products

Ultra Light

Ultra Light 2: With mutual authentication

### Atmel products

Famille AT88 : From 1kbits to 64 kbits.

Algorithm develop and licencing by ELVA. It could be integrated in a SAM.

Memory is divided by area. Mutual authentication, 64 bits key, data encryption possible.

### ASK products

CTM512B

One way counter as anti-replay attack.

Anti-clone function for dynamic data authentication (DDA).

Certificate generation and control for static data authentication (SDA). Encipher and decipher block function for read/write protection

Security features for memory chips exist and protect against:

- Re-issuing tickets
- Generation of counterfeit tickets
- Generation of cloned tickets
- Unauthorised memory read
- Unauthorised memory write



## 5 Protection features

### Memory areas :

By default a memory can be read in content. In an "access" point of view, several bytes are read and written each time.

In a "memory and features" point of view:

Several memory behaviors can be provided to fit with different functions:

- ✚ EEPROM memory: Free read and write area
- ✚ Lockable EEPROM: a part of the memory can be locked
- ✚ Read-only data: ROM
- ✚ More complex functionalities: OTP or counters. Those security functions are easy to implement.

Using those functionalities, we can add protection features on disposable media products.

### OTP area:

During writing operations, with a counter, it's possible hacking by remaining in an intermediate value. With an OTP bit, there are no intermediate values.

It allows to have protected systems. And the content of the product is not destroyed.

### Binary counter area :

You cannot provide modifications unless the value is smaller than the previous value.

It is a secured system (anti-tearing). If there is a problem, the previous value is preserved. At the computing system level, in case of problem we know where we are.

The idea is to have enough of logic to guarantee a transaction without increasing the complexity (using crypto).

### User EEPROM Area

There is an operation of deleting/overwriting. If we stop after deleting, there is nothing left in the zone. As soon as we stop, there might be an erroneous value. Advantage against magnetic technology: the area can be locked and it's not reversible.

An example with simple features ticket (counter for 10 tickets):

SRT512, and life cycle (annexe1).

An interesting point: the information can be locked once for all. These features are embedded in the chip.



## 6 Security management on CTM512B

CTM512B with this SAM (secure application module) could contain 4 main security features such as:

- One way counter as anti-replay attack
- Anti-clone function<sup>1</sup> for dynamic data authentication (DDA)
- Certificate generation and control for static data authentication (SDA)
- Encipher and decipher block function for read/write protection

Using applicative level functions, application could choose from zero up to three security levels.

### 6.1 Anti-clone function

After personalization, scheme of CTM512B authentication during user phase is as follow. This algorithm provides a one-way authentication: The terminal authenticates the card. After a successful execution of this algorithm, the secret Key and 64 bits data block are authenticated.

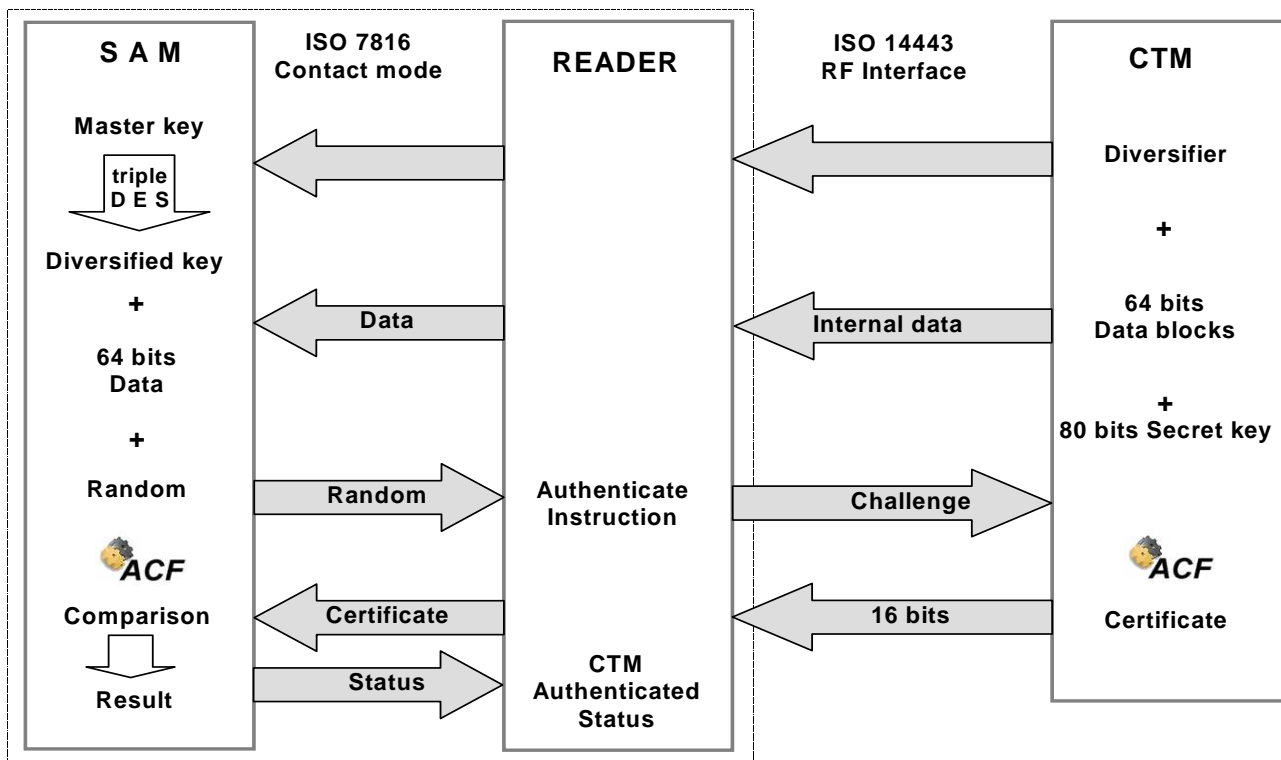


Figure 1 Authenticate transaction

<sup>1</sup> France Telecom proprietary AntiClone Function

Certificate is result of a cryptographic function from 80 bits secret key, 64 bits internal data and a challenge sent with instruction AUTHENTICATE.

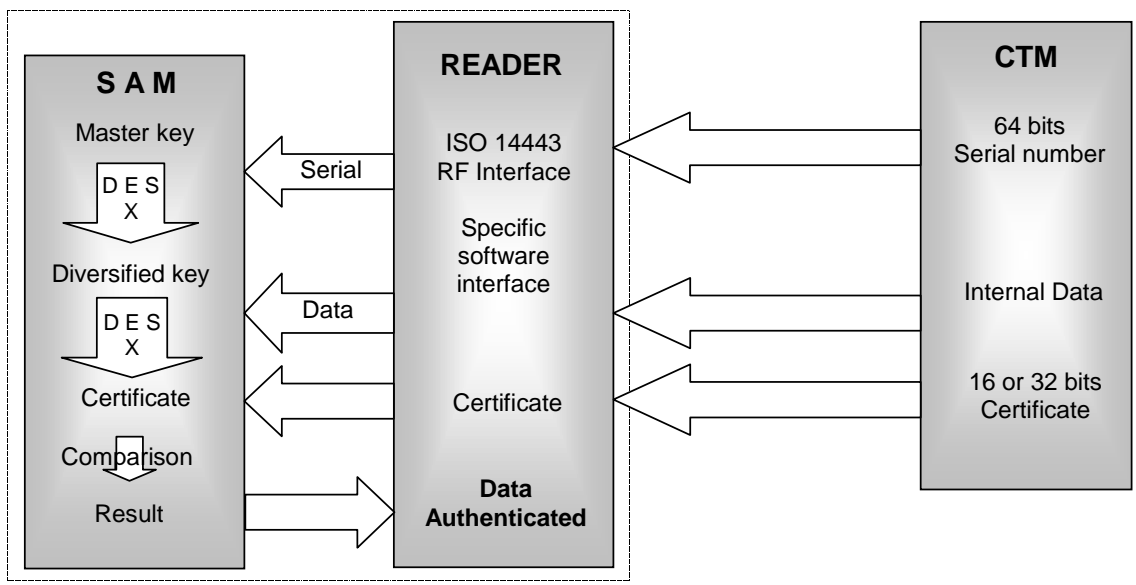
Verifying certificate, reader authenticate the chip and the data integrity written in CTM512B internal memory.

This scheme secures transport, stock, issuing, and long life ticket cycle. It avoids counterfeit or cloning risk.

16 bits certificate = ACF(serial number, secret key, challenge, internal data)  
With secret key = DES<sup>3</sup>(serial number, master key)

## 6.2 Certificate

Certificate is used as static data authentication.



Certificate is the result of a cryptographic function from a serial number, an application code and internal data.

Certificate is assumed to be also a Message Authentication Code (MAC).

Application is free to add any certificate in any ticket memory areas.

Verifying certificate, reader authenticates the internal data: an authentic reader has written data.

This scheme secures write operation, issuing data for example.

Certificate could be managed by 16 or 32 bits depend on security level.

$$\text{Certificate} = \text{DESx or DES}^3 (\text{secret key, internal data})$$

$$\text{With secret key} = \text{DESx or DES}^3 (\text{serial number, master key})$$



## 6.3 Security features

CTM512B security features are against:

- Re-issuing of tickets
  - Thanks to the otp system bits, the application is irreversible
  - Embedded counter is one way only, counter value change every new issuing phase
  - Anti-Clone function could be disabled by the application at the end of life cycle
  
- Generation of counterfeit tickets
  - 64 bits Serial number written at the production time. This number is guaranteed unique in fabrication.
  - The certificate is written at the valorisation phase and become read only. This certificate is unique for each ticket. This certificate authenticates data written in ticket.
  - A unique and diversified 80 bits secret key is written during personalisation phase.
  
- Generation of cloned tickets
  - Anti-clone function with dynamic secret algorithm with 80 bits secret key
  - Specific AUTHENTICATE instruction base on challenge – response
  - Anti-clone function authenticates either the secret key and the data written in chip memory
  - One-way counter avoids replay attack. Counter could change at each validation.
  - Specific SAM secures applicative secret master key
  
- Unauthorised memory read
  - Made by enciphered data block
  
- Unauthorised memory write
  - Made by data block enciphered
  - Authenticate by a good certificate

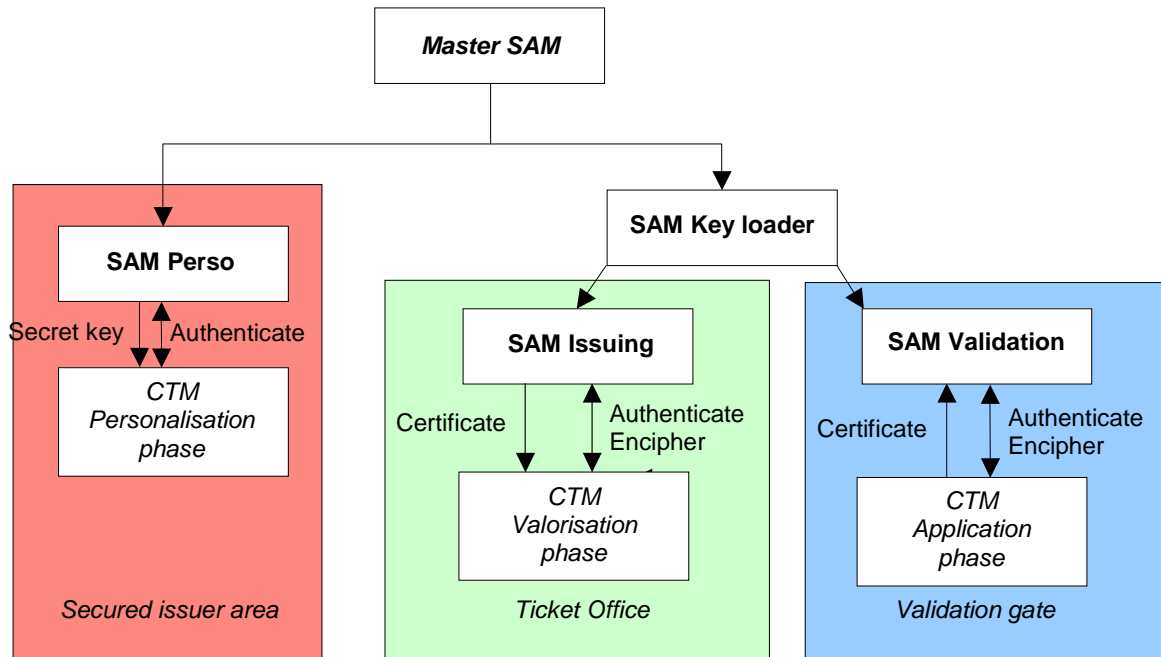
Additional SAM features:

- Different issuer and validation key set
- Issuing counter: possibility to set the maximum issuing count by SAM
- Counter event for each key
- Counter against brute force attack
- Mutual authentication before all encrypted load key set
- True random generation (FIPS 140-2)
- Hardware security (power consumption analysis, voltage sensor, frequency sensor, temperature sensor, micro probing detection, etc...)



## 7 SAM architecture implementation

Example of security using CALYPSO SAM:



**SAM Perso:** it reads the ticket serial number, diversifies key then write secret key in ticket specific area.

When Key area is protected, this SAM could check Authenticate instruction result. SAM contains unique serial number and counts each CTM512B personalisation. This SAM cannot generate the issuer area certificate.

**SAM Issuing:** It authenticates the ticket without output any information about the secret key. It generates the issuer area and the issuer area certificate. This certificate is written in clear during transmission. This SAM is able to authenticate the CTM512B ticket. This SAM is not able to output secret diversified key. This SAM is able to encipher / decipher blocks

**SAM Validation:** It authenticates the ticket and verifies issuer area certificate. This SAM never output any information about the secret key and the certificate. This SAM is not able to output certificate and secret diversified key. This SAM is able to encipher / decipher blocks

**SAM Key loader:** It is able to perform mutual authentication between SAM Emission or Validation. This SAM writes in secure mode a new set of keys stored in the SAM: a Master key for the authenticate algorithm and a master key for static certificate.

**Master SAM:** generates and stores all key sets. It is able to perform mutual authentication with all SAM. This SAM writes in secure mode a new set of key in SAM field.



## 8 Security in Memory Chips

To resume:

Critical data can be protected using the ROM data.

Coherence can be protected with a certificate.

Multiple voyages are activated with counters.

It's also possible to avoid emulation using UID, it means the black list.

Authentication can be added where it's interesting:

- ✚ Either a simple authentication which is not a condition to access the ticket (useless to read the content of the product, it avoids copies).
- ✚ Or an authentication to define the access, it means that the ticket is not accessible. It conditions the read/write operations. The ticket cannot be modified if the reading is not recognize (reading fraudulent = hacker who would like to modify the ticket).

This feature could be used for multiple voyages or durable tickets.

We must also remind that the first hacking protection is the visual aspect of the paper ticket. It must be similar with others.

If we except the SAM theft, there is only risk of clonage.

Depending of the memory impact, could we have a certificate for this type of support? It implies the cost augmentation to have anti-clonage system but memory size have to be optimized.

Who could define this authentication? Calypso? The manufacturer ?

Will Calypso generate its own authentication algorithm?

In case of a Calypso algorithm, will Calypso members have access to this algorithm? If not, what might be the extra cost to have this algorithm?

To conclude, the level of security requested should be listed depending on the kind of tickets.

## 9 Second part of WP6

During a second part of this work package, WP6 could define specifications on how to implement such a disposable support in a Calypso environment and which security functions Calypso should recommend in term of security to do transactions.

The following societies: ERG, ACS, LINK, PARKEON, THALES, SNCF, RATP, TRANSDEV, KEOLIS...could joined the WP6 and determined which level of protection is needed for current or new projects.

Disposable support with memory chips is a need, and WP6 highly recommand to preserve this support into CALYPSO.