



Secure UHF Tags with Strong Cryptography

Development of ISO/IEC 18000-63 Compatible

Secure RFID Tags and Presentation of First Results

Walter Hinz, Klaus Finkenzeller, Martin Seysen

Barcelona, February 19th, 2013



Giesecke & Devrient

Creating Confidence.

Agenda

- Motivation for Secure UHF Tags
- The Rabin-Montgomery Cryptosystem
- Message Flow
- Protocol Extension with Mutual Authentication
- Proof-Of-Concept Implementation

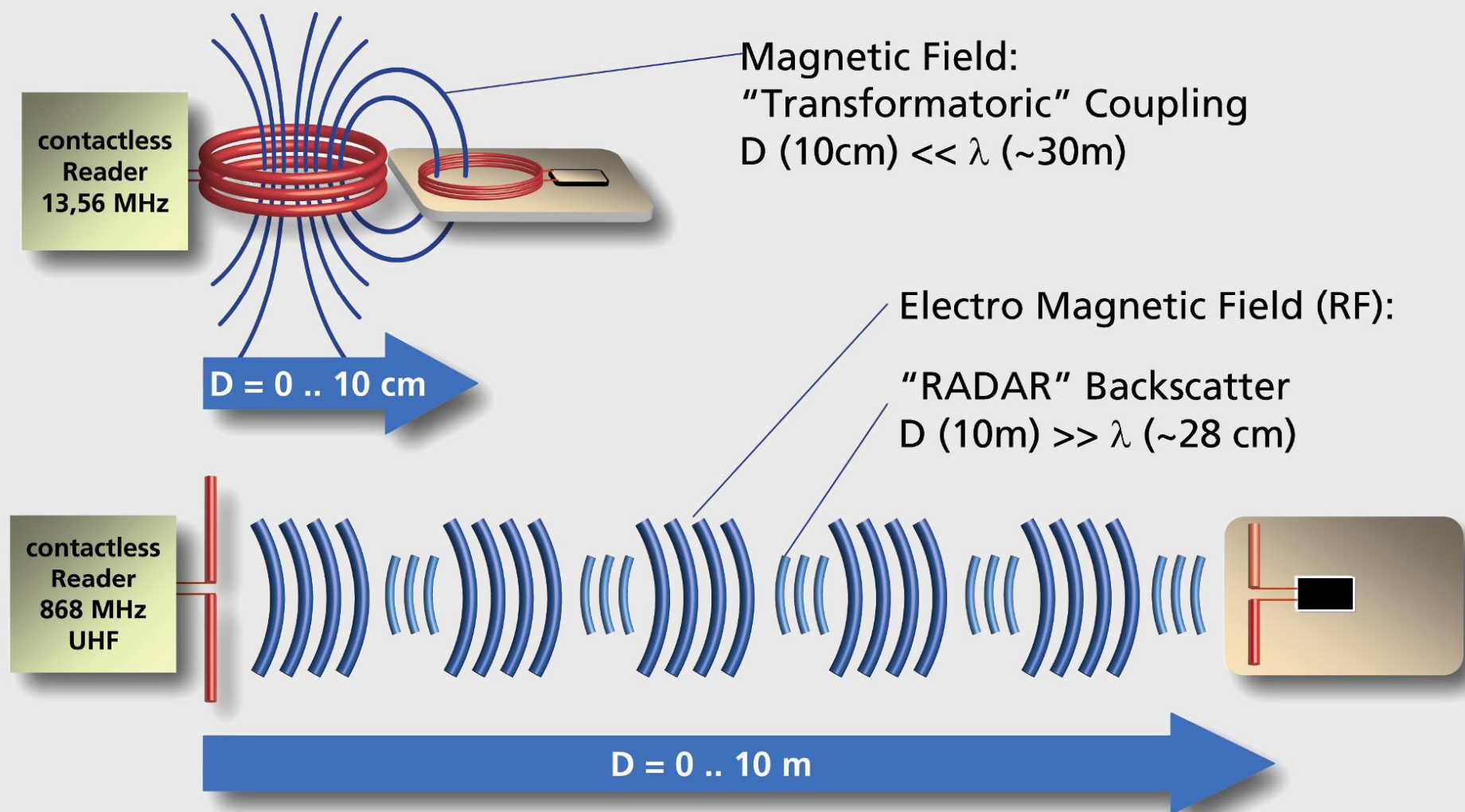


Agenda

- Motivation for Secure UHF Tags
- The Rabin-Montgomery Cryptosystem
- Message Flow
- Protocol Extension with Mutual Authentication
- Proof-Of-Concept Implementation



Inductive and radiative RFID Systems



Secure UHF RFID

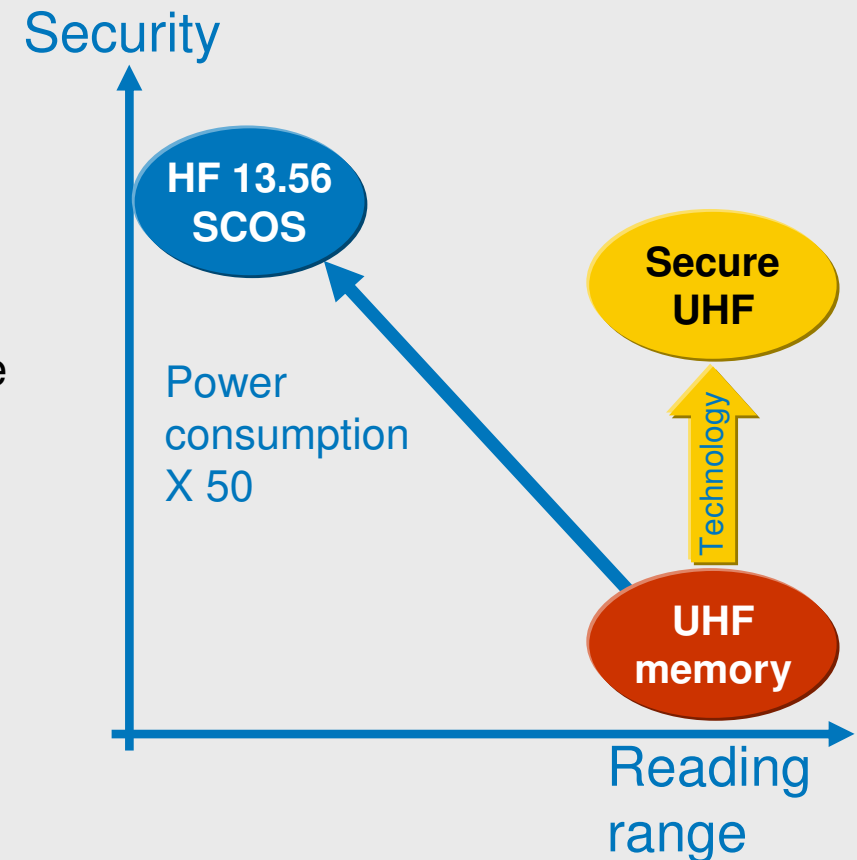
Cryptographic protection of UHF RFID systems facilitates novel applications thanks to its long operating range

Today:

- RF 13,56 MHz: Smart Card OS / 10 cm
- UHF 868 MHz: Non-secure memory / 10 m

Secure UHF RFID:

- Cryptographic security with same operating range
→ technological leap
- μ Controller with SCOS → full flexibility in the choice of authentication protocols
- AES efficiently implemented in hardware



Agenda

- Motivation for Secure UHF Tags
- The Rabin-Montgomery Cryptosystem
- Message Flow
- Protocol Extension with Mutual Authentication
- Proof-Of-Concept Implementation



The Rabin-Montgomery Crypto Suite

- Based on the asymmetric cryptosystem by Michael O. Rabin (1979)
- Augmented by a method from Peter Montgomery (1985) to avoid the division of long numbers in modular arithmetic
- Allows cost and energy efficient implementation by combining the Rabin and Montgomery algorithms
- Allows non-traceable and confidential identification and authentication
- Does not require a private (secret) key to be stored in a tag
→ the tag performs only efficient public key operations
- Time consuming private key operations need only be performed by the interrogator
- Can be combined with symmetric mutual authentication, based on AES



How the RAMON Tag Authentication Works

RAMON is a public key protocol, using four different keys:



A public key K_E , used for encryption.

➔ This is the only key stored on the tag



A private key(-set) K_D , used for decryption

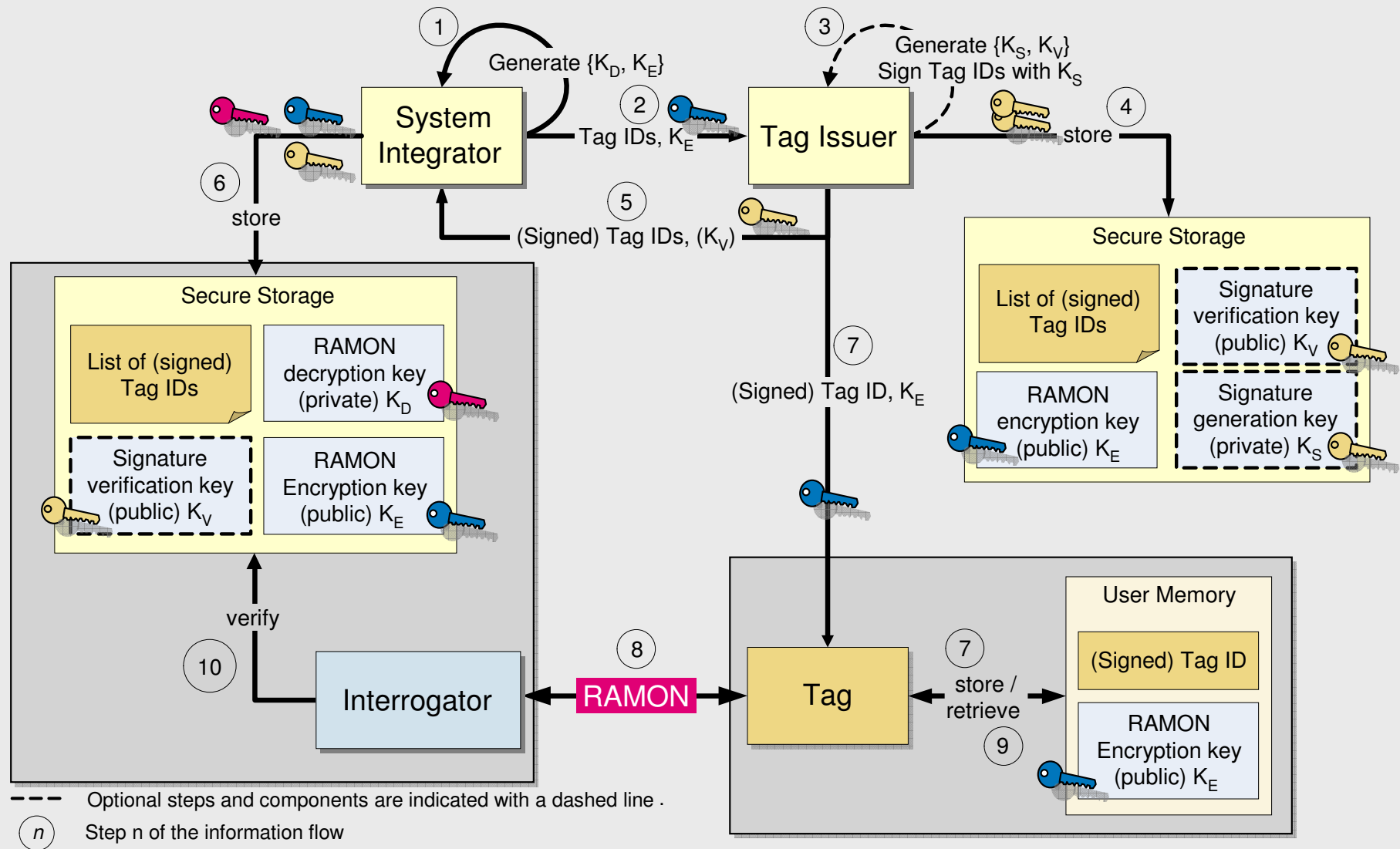
➔ This key is only stored in a secure memory in the interrogator



An optional key set K_S , K_V , used to validate a signed UID

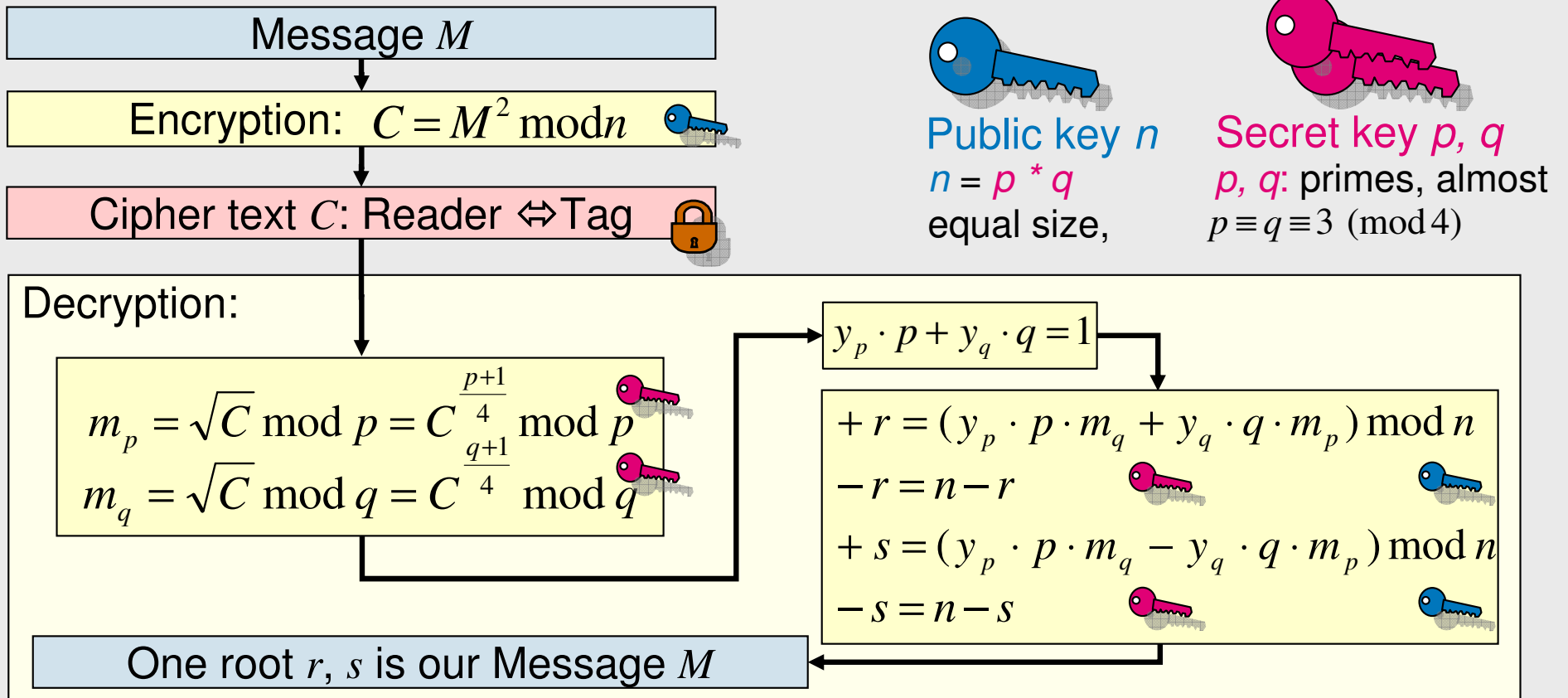
- As the data length might exceed the buffer capacity of tag or interrogator, response messages are chained
- First response chunk is delivered while ongoing encryption produces more data consecutively
 - ➔ Optimised transaction time

Information Flow with RAMON Tag Authentication



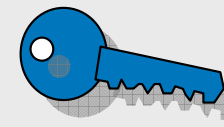
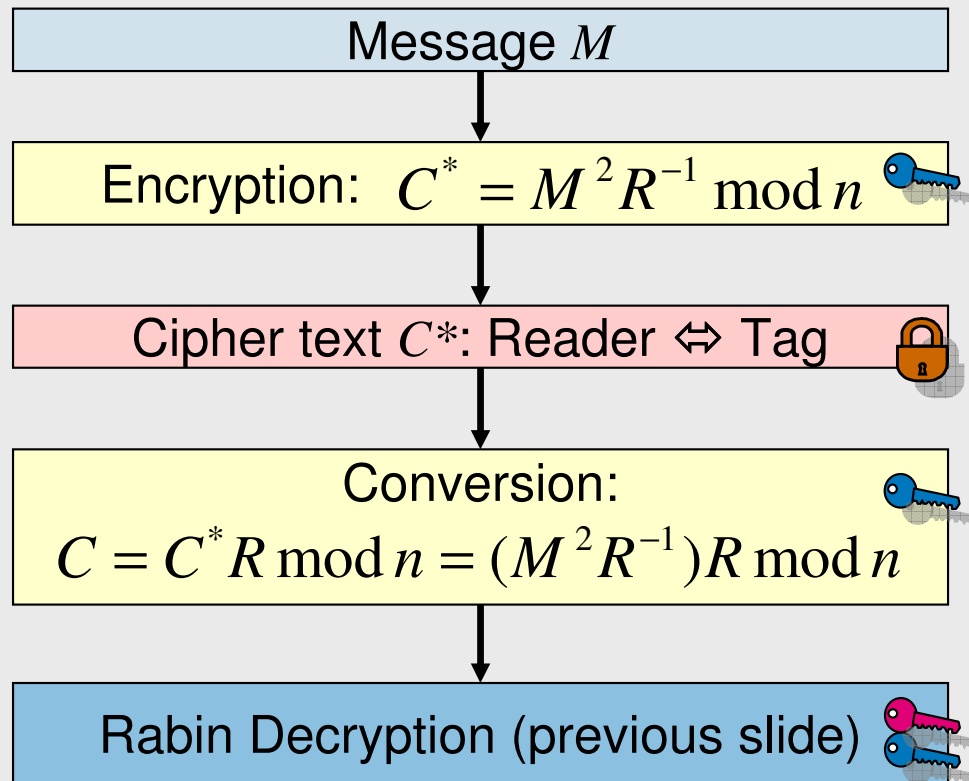
Basics: Rabin Cryptosystem

The Rabin cryptosystem is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the factorization problem.

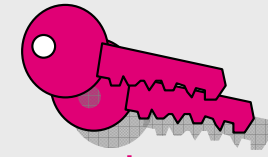


Basics: Montgomery Modular Multiplication

The Montgomery approach allows a much more efficient calculation of the cipher text C in the tag.



Public key n
 $n = p * q$
equal size,



Secret key p, q
 p, q : primes, almost
 $p \equiv q \equiv 3 \pmod{4}$

Residue R is a power of 2 and
 $R \geq 2^k > n$
In other words, R is at least
the next power of 2 which is
larger than n .

$$n = 1 \bmod 2^{bl \cdot nd}; 1 \leq nd < d; nd \approx \frac{d}{2}$$



Agenda

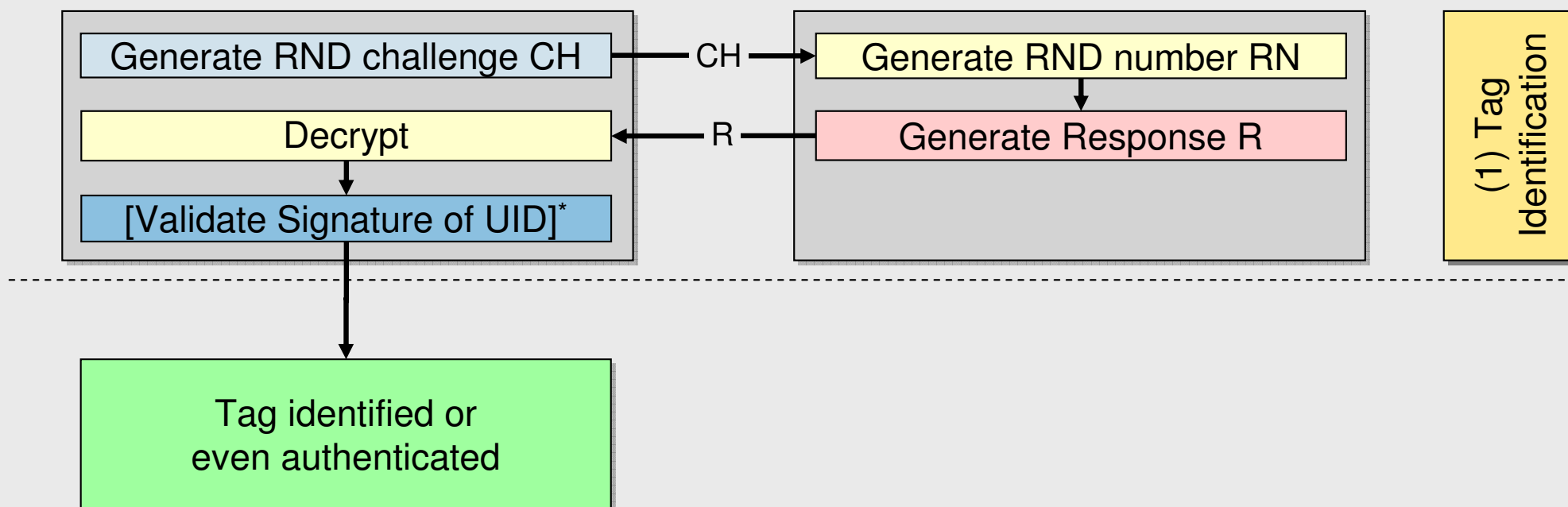
- Motivation for Secure UHF Tags
- The Rabin-Montgomery Cryptosystem
- **Message Flow**
- Protocol Extension with Mutual Authentication
- Proof-Of-Concept Implementation



RAMON Protocol Steps – Tag Identification Only

Interrogator

Tag



Stop here, if only tag identification is required

*: signature validation is an optional step

Detailed data flow for tag only authentication

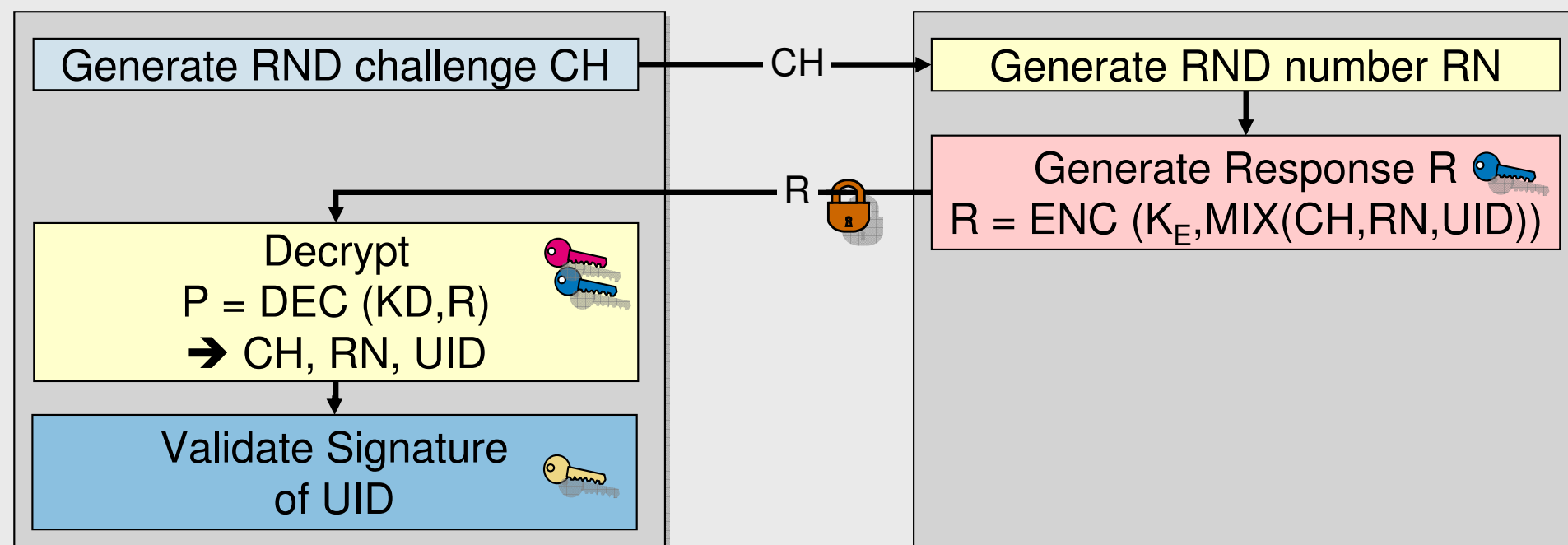
Interrogator

{Database, K_D , K_V }



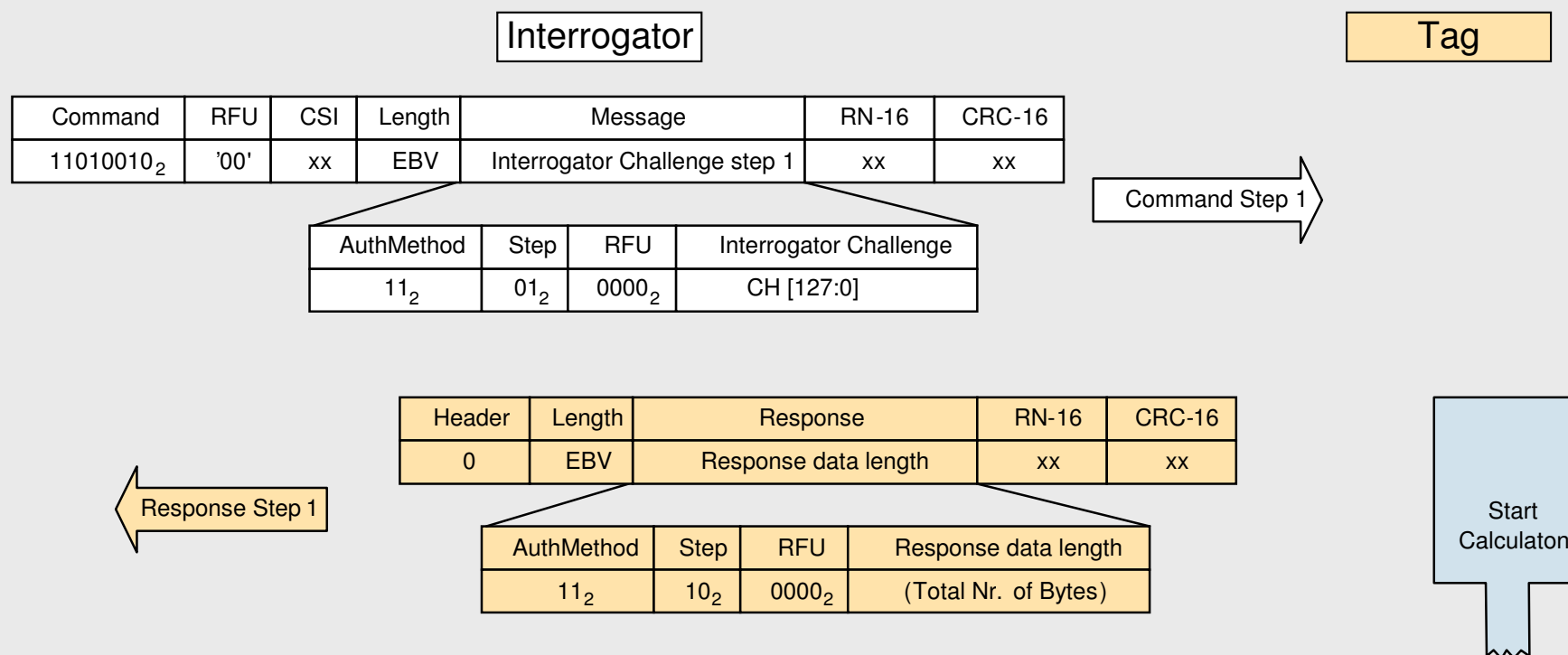
Tag

{(signed)UID, K_E }



Detailed Protocol Step 1: Interrogator send challenge

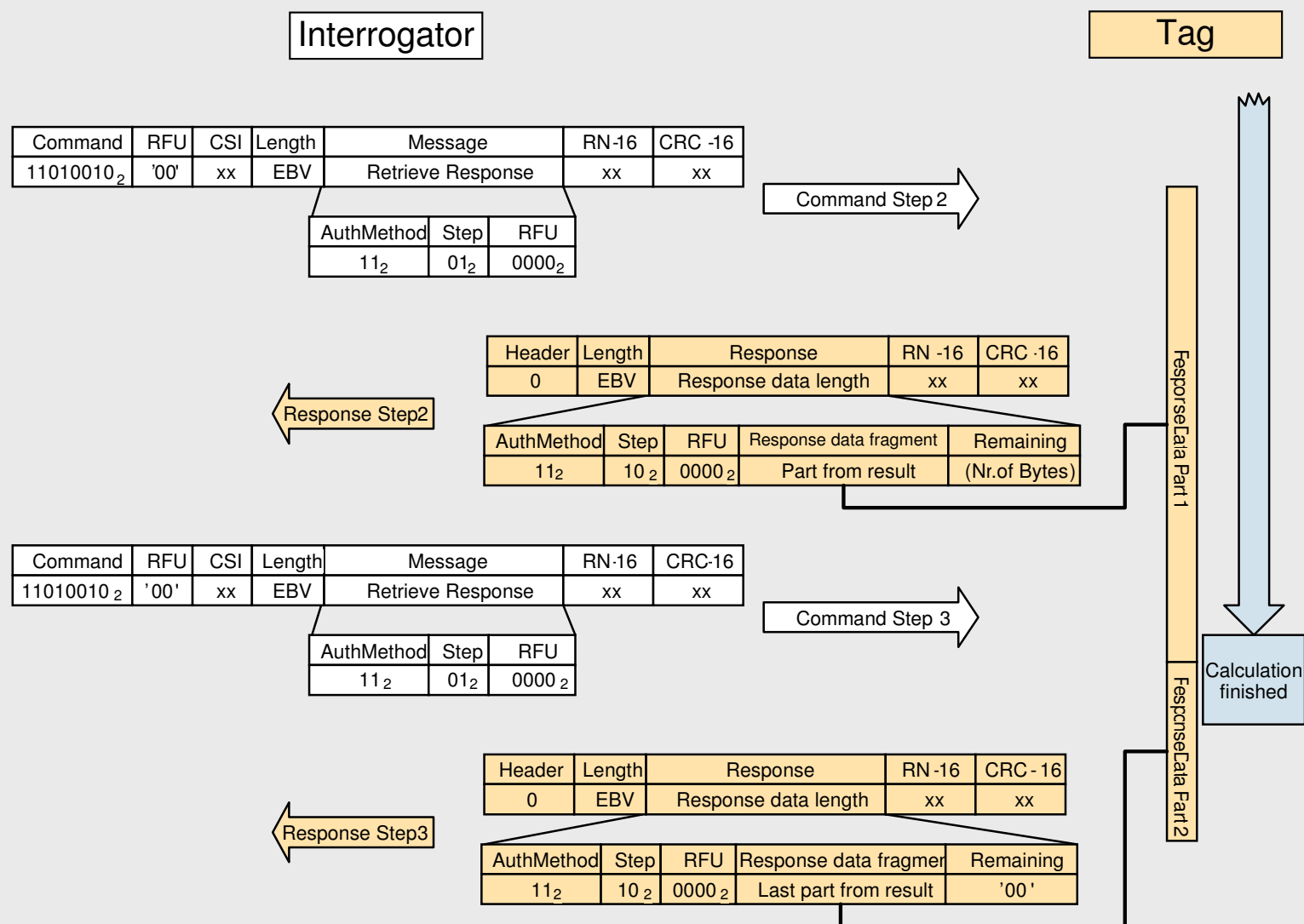
- Step 1: The interrogator challenge is delivered to the tag.
- The tag immediately starts with the cryptographic calculation and answers with the length of the response data which will be calculated.



Detailed Protocol Step 2: Retrieve calculation results

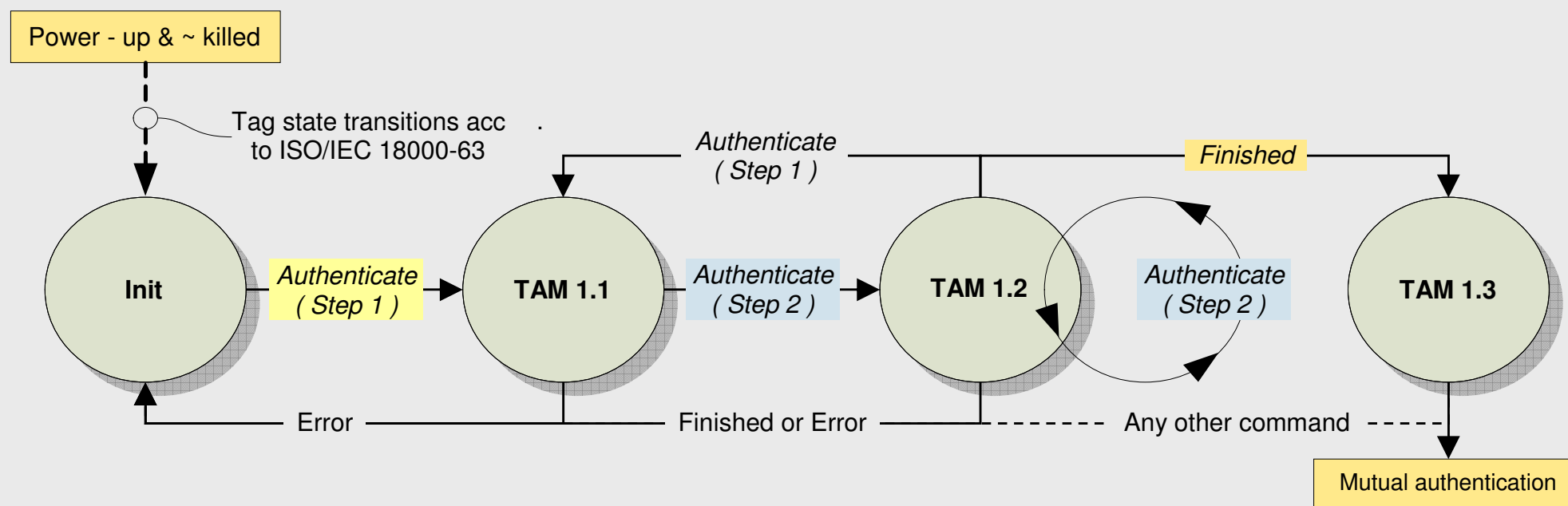
- Step 2: The interrogator retrieves the remaining fragments by chaining.

- Once the interrogator has retrieved the entire record, it is able to authenticate the tag.



Detailed Protocol steps for tag only authentication

- In **Step 1**, the interrogator challenge is delivered to the tag. This message is used to request the tag to perform authentication.
- In **Step 2**, the interrogator retrieves the remaining fragments by chaining further Authenticate commands and responses. Once the interrogator has fetched the entire authentication record it is able to authenticate the tag.



Agenda

- Motivation for Secure UHF Tags
- The Rabin-Montgomery Cryptosystem
- Message Flow
- Protocol Extension with Mutual Authentication
- Proof-Of-Concept Implementation



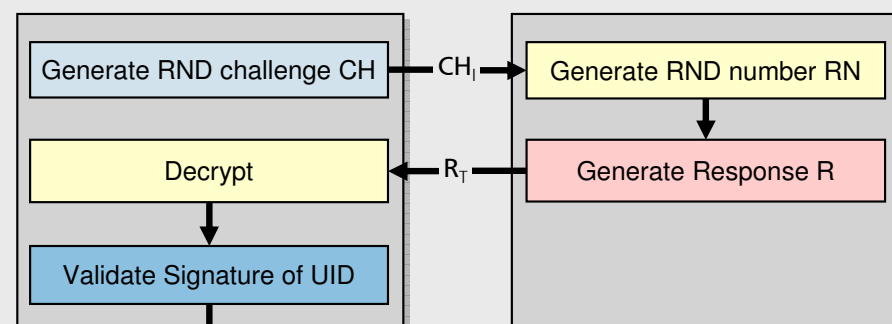
RAMON protocol steps – Algorithms Used

Interrogator

Tag

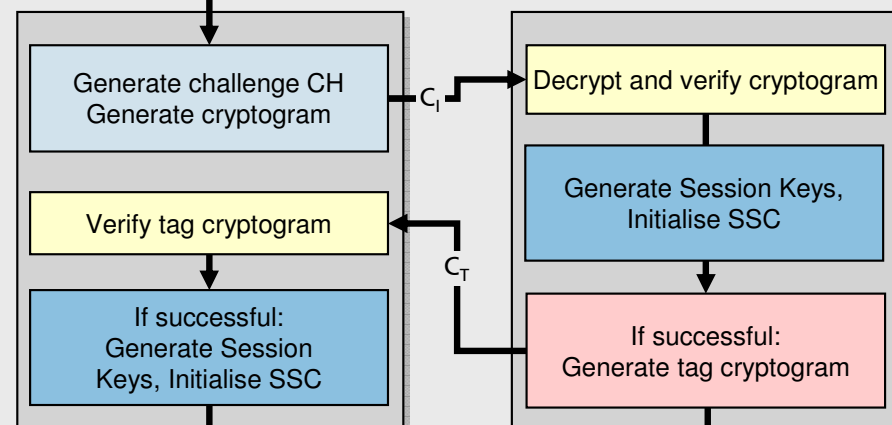
Algorithm

State



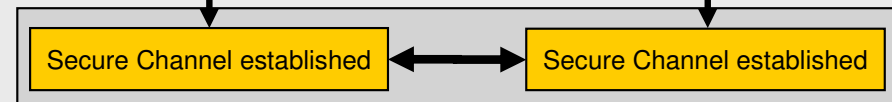
■ Rabin Montgomery (RAMON)

(1) Tag Identification



- AES (FIPS197)
- AES CBC-Mode (SP800-38A)
- CMAC (SP800-38B)
- KDF (SP800-108)

(2) Mutual Authentication



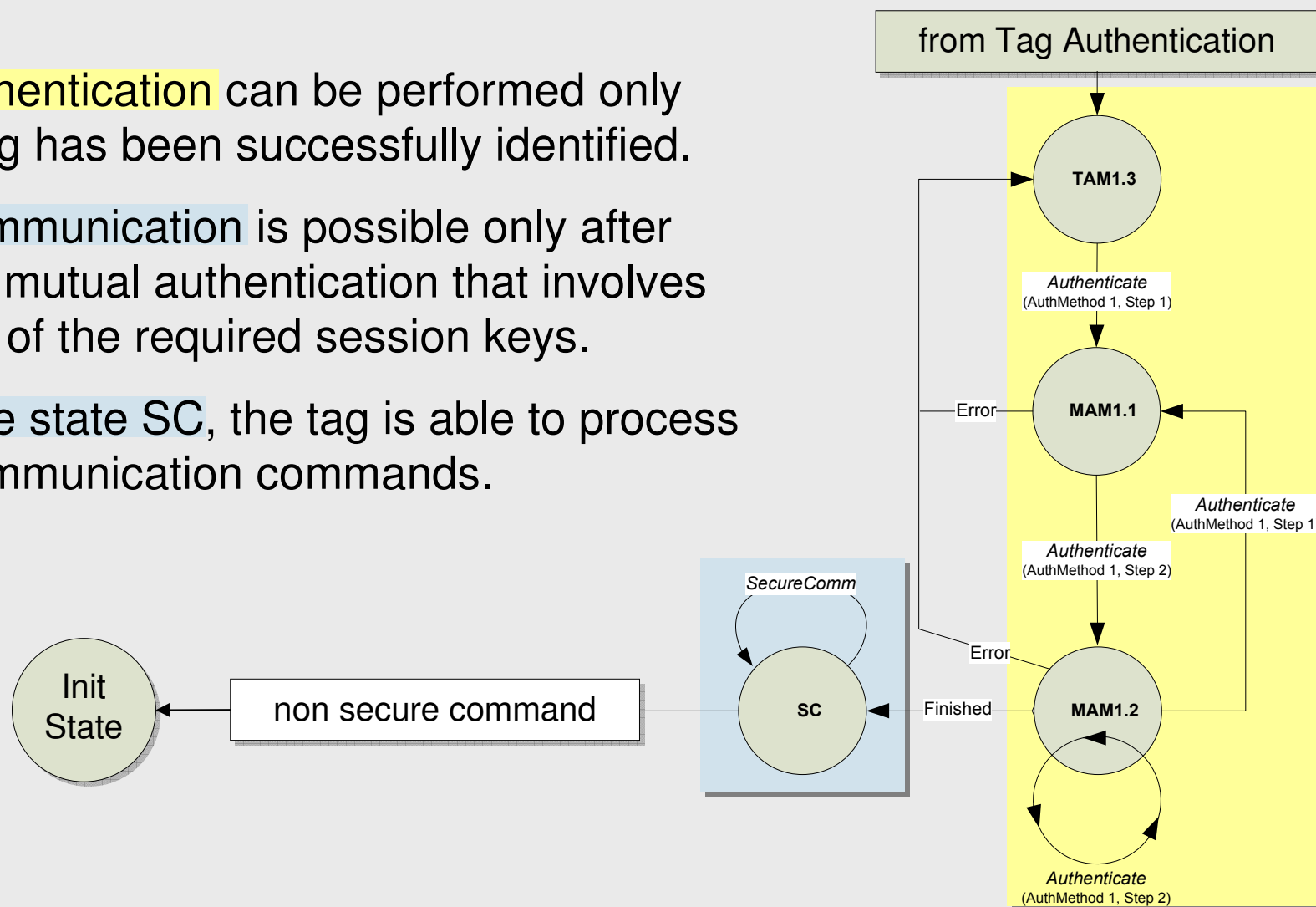
- AES (FIPS197)
- CMAC (SP800-38B)

(3) SC










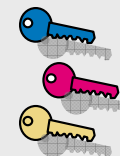
Detailed Protocol Steps for Mutual Authentication

- Mutual authentication can be performed only after the tag has been successfully identified.
- Secure communication is possible only after successful mutual authentication that involves generation of the required session keys.
- While in the state SC, the tag is able to process Secure communication commands.



RAMON – Keys Used

Key	Usage	Length in bits	Remark
K_{ENC} 	Shared secret encryption key	128	Optional
K_{MAC} 	Shared secret message authentication key	128	Optional
S_{ENC} 	Session encryption key	128	Dynamic
S_{MAC} 	Session message authentication key	128	Dynamic
K_E 	Public key for encryption stored on tag	$1024 \geq n $	Mandatory
K_D 	Private decryption key stored on interrogator	$1024 \geq n $	Mandatory
K_V 	Public signature (ECDSA) verification key stored on interrogator	$320 \geq n $	Optional



Session Keys

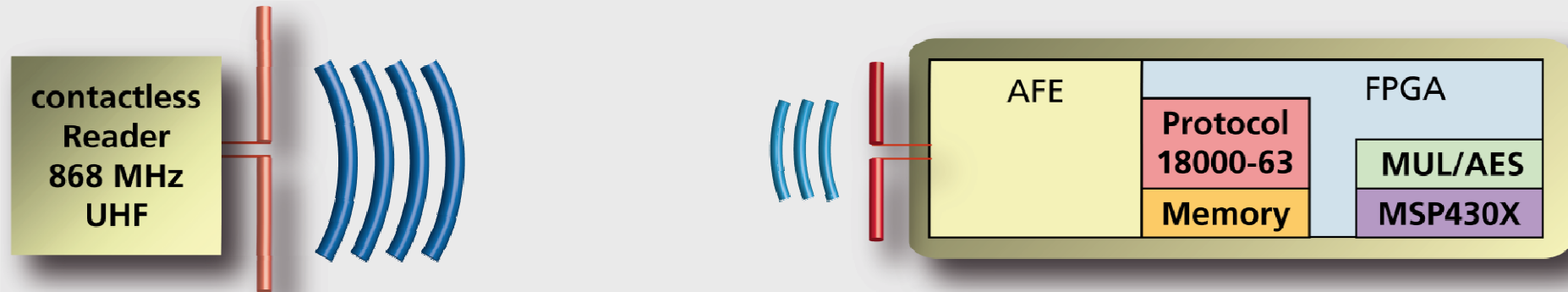
Tag Identification keys

Agenda

- Motivation for Secure UHF Tags
- The Rabin-Montgomery Cryptosystem
- Message Flow
- Protocol Extension with Mutual Authentication
- **Proof-Of-Concept Implementation**



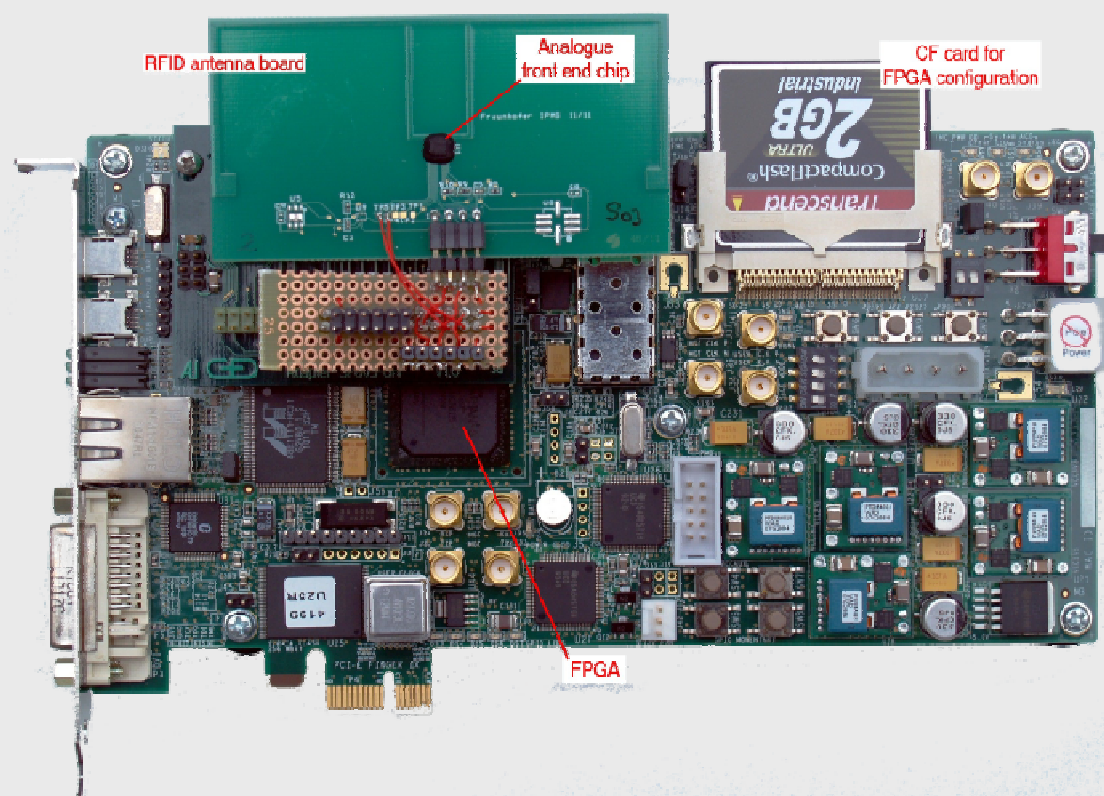
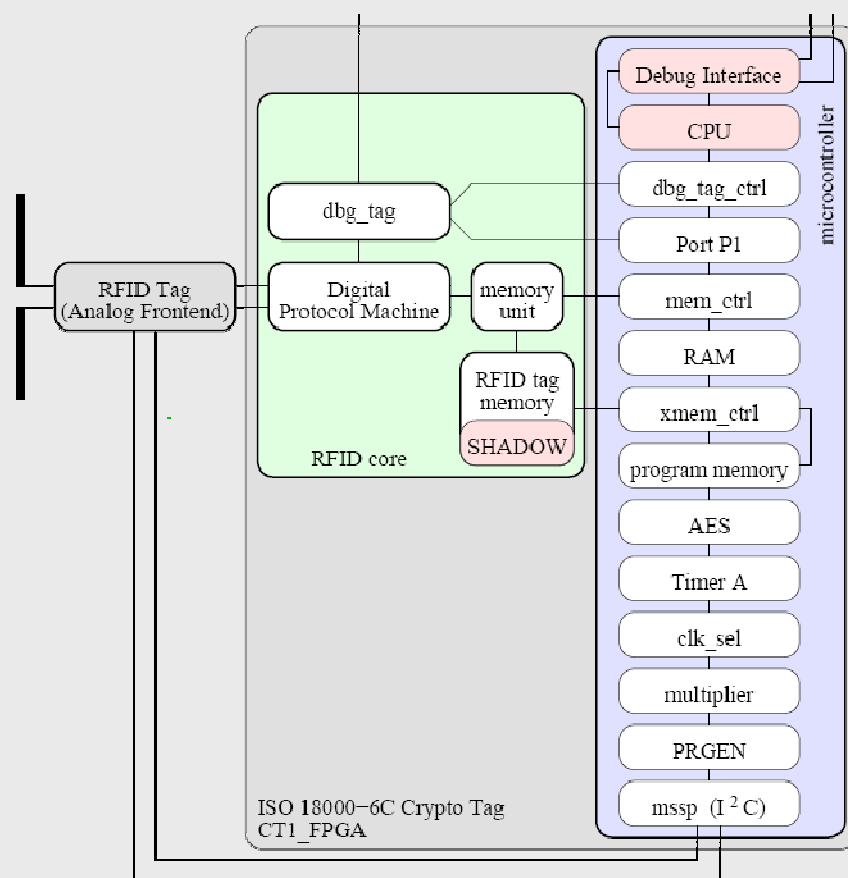
FPGA Layout for a Proof-of-Concept



- Commercial RFID reader connected to PC
- Externally powered FPGA Evaluation Board
- Existing non-secure tag as (analogue-only) radio front end, AFE
- Re-implemented ISO 18000-63 state machine and tag memory
- Soft-core microcontroller, MSP430X-compatible
- Hardware multiplier and AES coprocessor

A Closer Look to the Actual Demonstrator

The available UHF tag evaluation board facilitated the design of the demonstrator by providing digital baseband access to the modulator / demodulator:



Some Results

- MSP430 clock rate 1.25 MHz corresponds well to 1.28 MHz subcarrier
- RAMON calculation only: 134 ms
- RAMON including transmission: 330 ms
 - Improve messaging concept
 - ISO/IEC 29167 will define standard command set



Thank You for Your Attention

Walter Hinz
Giesecke & Devrient GmbH
Prinzregentenstrasse 159
D-81677 München

email: Walter.Hinz@gi-de.com

