



CEN TC224 WG15

European Citizen Card Standard

Lorenzo Gaston

Porvoo Group, Brussels October 14th 2005





The ECC standard

- **Complete smart card specification covering the physical, electrical and logical features**
- **In two-steps: Experimental standard first, then EN**
- **Split into three parts:**
 - **Part 1: Physical, Electrical and Transport Protocol**
 - **Part 2: Logical Data Structure and Security Services**
 - **Part 3: Management of the card and services**



European Citizen Card TS progress

- **ECC-1 and ECC-2 draft comments distributed**
- **159 comments (Austria, Sweden, German, UK, France, ANEC,**
- **Next week 19-21th meeting in AFNOR for Resolution of Comments**
- **Target Publication: / Q1 2006**
- **ECC-3 New Work Item submitted: Start of the work December 05 after stabilization of CD 24727-3**



European Citizen Card moving to EN

- **CEN TC224 waiting for « political decision »**
- **Technically it will involve**
 - ✓ **Alignment with ISO 24727 (if any)**
 - ✓ **Alignment with ISO 7816-13 (if any)**
 - ✓ **Alignment with WG16 (if any) and WG17**
 - ✓ **Alignment with ISO JTC1 WG1 (if required)**
 - ✓ **Possible impact of Match on Card WG11 (?)**



Political environment

G5 : Looking for IOP ID cards

- G5 agreed that the new electronic identity cards issued by the five partner countries be technically compatible and interoperable
- On last July 5th the European Council instructed the Council and Commission to prepare the development of minimum standards for national identity cards, covering:
 - IAS
 - Access to e-administration
 - To extend the use of biometrics to all identity documents including driving licences



Main physical/electrical choices for ECC-1

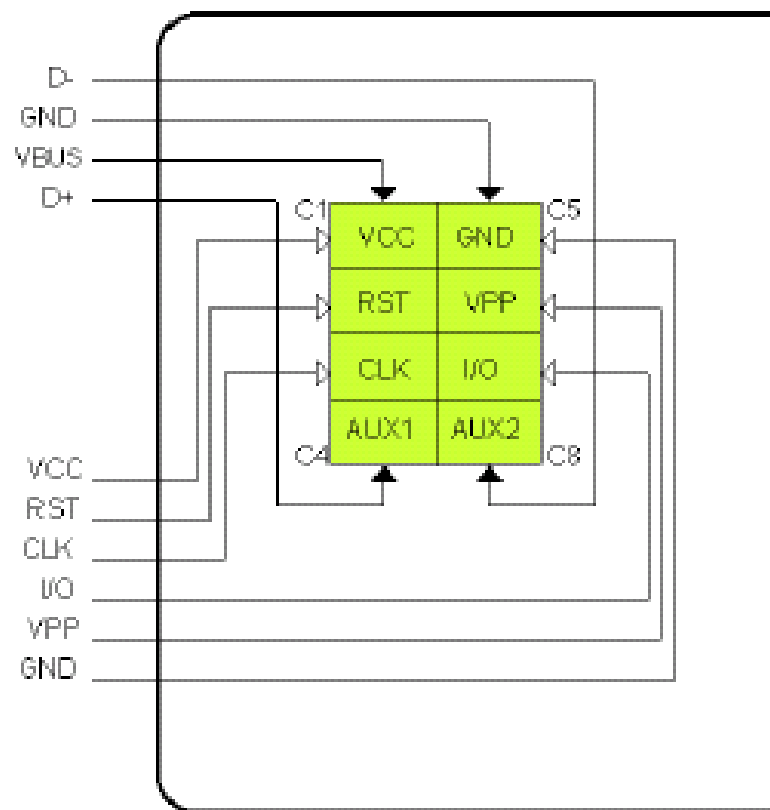
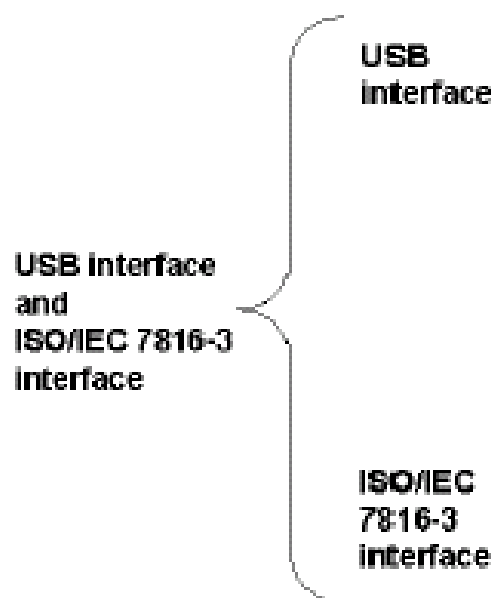
- **ISO 7810 (bank card) format**
- **Only contact interface mandatory**
- **ISO Contactless interface conditional**
- **USB interface optional compliant with 7816-12**
- **Methodology for card Durability and specific Testing applicable only to personalized cards**
- **Security Evaluation according to CWA 14169**
- **Physical Securities depending on the ECC**



ECC with USB Interface

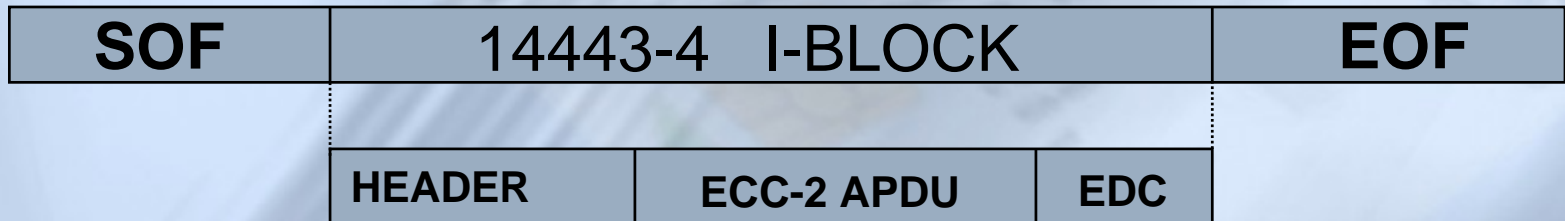
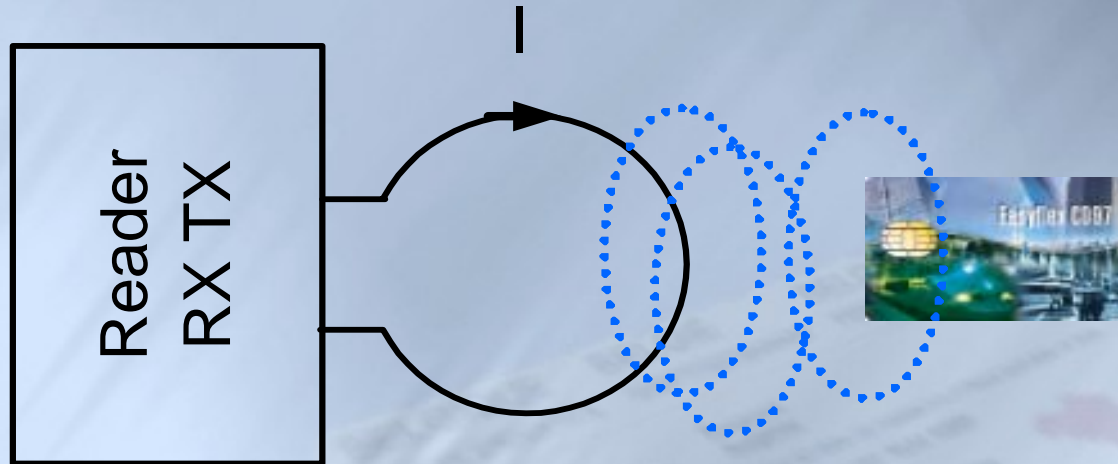
Interface Devices

IC Card





ECC with Contactless Interface





Key target: Guarantee Durability

- **Existing standards: ISO 7810/10373, 7816, ... don't deal with durability.**
- **Isolated tests target specific performances**
- **Durability test should simulate the real operational conditions of the card**
- **A notion of Card mission profile is needed**
- **This Card Mission Profile is defined by Age and Usage parameters using the Durability Class Tool**

Step 1. Card Mission Profile

Durability Class definition tool

ENVIRONMENT	Usage	"Age"	STORAGE	Usage	"Age"	READER PROFILE	Usage	"Age"
Controlled clean room	0	0	hard plastic holder	0	1	Long range vicinity	0	0
Residential/office	0	2	hard plastic holder in pocket, purse...	0	1	Medium proximity	0	0
light factory	0	3	Tyvel sleeve	3	0	Barcode scanner	0	1
day to day temperate country	1	3	wallet in purse	1	0	short range C-less	1	0
chemical exposure	0	4	soft plastic holder	3	0	IC contact	4	1
extensive UV exposure	0	5	soft plastic holder in side pocket	5	1	Card imprinter	2	4
extreme cold	0	5	soft plastic holder in pant pocket	10	1	magstripe insertion	4	2
extreme T/H	0	5	wallet in pant pocket	9	2	Weigand	?	?
extreme T/H change	0	5	Loose in purse	9	4	barcode swipe	2	5
heavy factory	10	6	loose in pocket	10	4	magstripe swipe	2	8
Vehicle environment	6	3	Attached to key ring	10	6			
			Loose in schoolbag	9	7			
			loose in car or glove box	8	8			
Selected profile:	1	3		9	2		4	1

	Usage	"Age"
Resulting raw grade:	14	6
Usage Frequency	1	
Expected lifetime		5
Global Application Rating	14	30

FREQUENCY	Coefficien
0 to monthly(0-100/yr)	1
weekly(100-500/yr)	2
daily(501-2000/yr)	5
hourly(>2000/yr)	10

Usage frequency *weighting coefficient* influences application placement on the "Usage" axis.

EXPECTED LIFETIME	Coefficien
up to 2 years	1
up to 3 years	2
up to 5 years	5
up to 10 years	10

Expected lifetime *weighting coefficient* influences application placement on the "Age" axis

Formulas:
Global Rating(Usage axis) = [Environment(Usage) + Storage(Usage) + Reader(Usage)] x Frequency
Global Rating (Age axis) = [Environment(Age) + Storage(Age) + Reader(Age)] x Lifetime



Step 2: Selecting the card technology

- The « Age » Global Rating Value translates into number of Durability Cycles from 0 to 3 (Annex B.1)
- The « Usage » Global Rating Value translates into a Durability Class from A to B (Annex B.1)
- Durability Cycles and Durability Class are positioned in the Durability Test Sequence Table
- A card able to pass the Test Sequence Table is in principle right to host the application with such Card Mission Profile



ECC-1 proposal overview

DURABILITY TEST SEQUENCE TABLE

Number of cycles to perform (<u>not</u> years)		0	1	2	3
Durability Classes (~severity of mechanical aggressions)	A	ISO 7810	Sequence 1	Sequence 1	Sequence 1
	B	Tests	Sequence 2	Sequence 2	Sequence 2
	C	Tests	Sequence 3	Sequence 3	Sequence 3
	D	Tests	Sequence 4	Sequence 4	Sequence 4

“Age”

Application

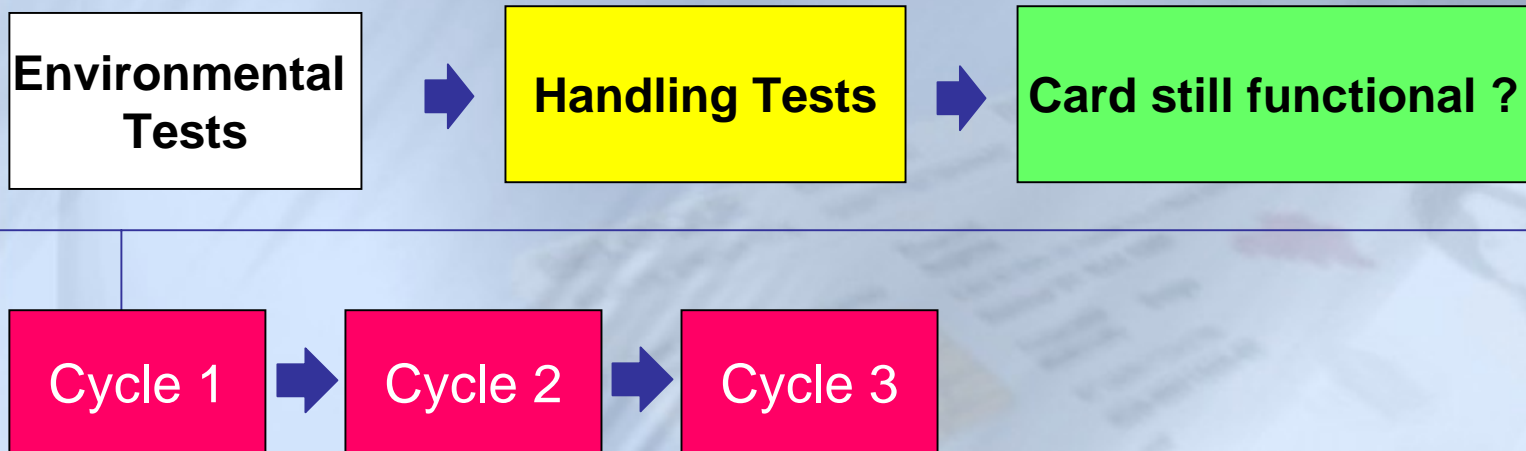
Usage





ECC Test sequence for Durability

- Test sequence architecture:





ECC Durability: Sequence table

Before

After

Sanctions

Dimensions/aspect

Layers adhesion
(peeling)

Module adhesion

Functionalities*

1 sequence X (X= 1-4): cumulated
usage aggression tests with

Mechanical aggressions (bendings ...)

Chemical aggressions

Climatic aggressions (heat, humidity)

Sanctions

Dimensions/aspect

Layers adhesion
(peeling)

Module adhesion

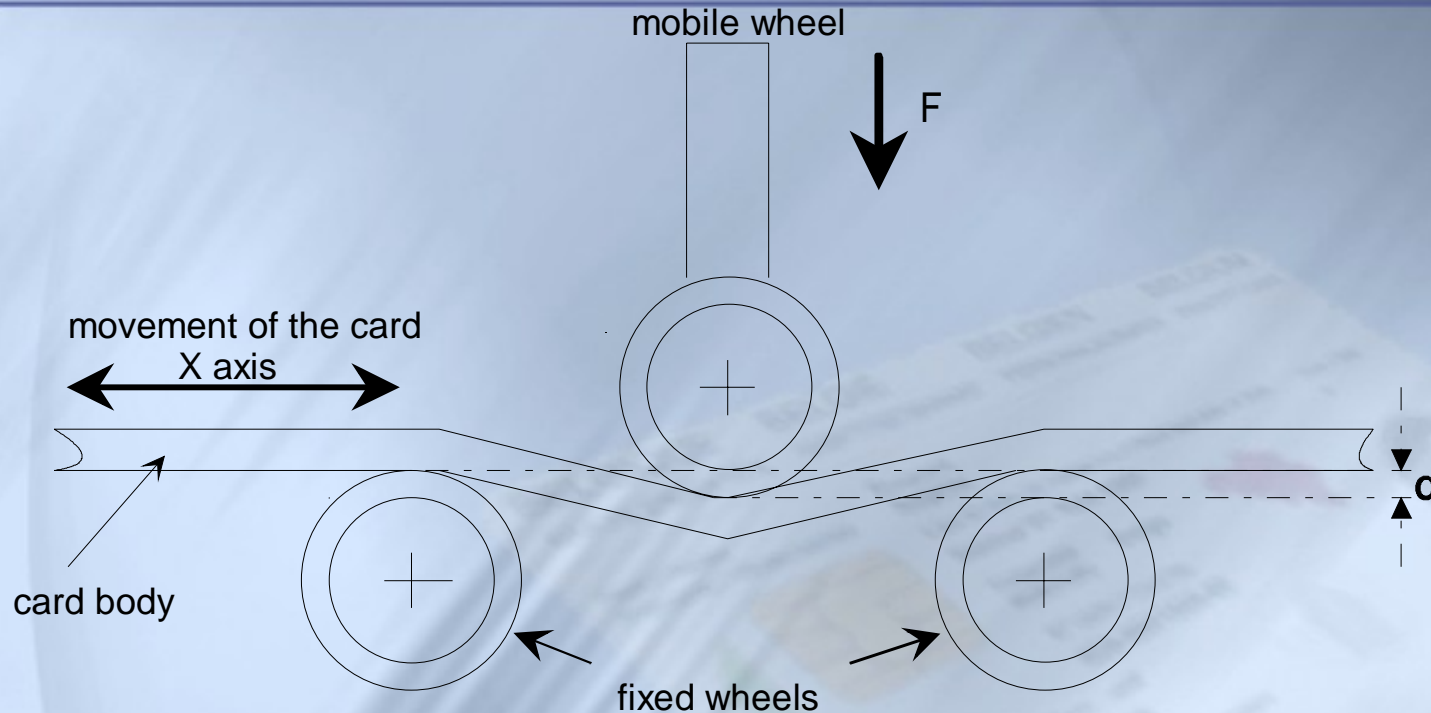
Functionalities*

- **Age axis : number of sequences (cycles)**
- **Usage axis : type of sequence/test tuned to the required « usage mission » (ex : harder aggression tests and/or more severe sanctions if class D than class C , B, A)**

* **Functionalities : RF and contact + all the functionalities of the secure features**



3 wheels test >> simulates insertion in the reader



3 F: 8 N, Max amplitude d: 0.5 mm (Ref. ISO std 10373-3)

Sanction : Minimum 160 insertion cycles (axalto proposal) for each of the 10 cards tested



ECC Card elements

Module: No technology mandated but specific tests

Card Body compliant with durability class

Microcontroller

Antenna (Optional) : ID1 according ISO 14443-1

**Background
printing**



Two-Tone guilloches

Rainbow colouring

UV-flourescent overprinting

Effective anti-counterfeiting

(optional microprinting)



Main logical & security choices for ECC-2

- **Electronic signature mandatory**
- **Both Java Card and File-Oriented cards supported**
- **APDU: Cryptographic, File and AID selection**
- **Authentication mechanisms with Privacy**
- **Common Data Structures**
- **Biometrics and ICAO application optional**



ECC-3 New Work Item content

- **Application life cycle management**
 - **Personalisation Aspects: ISO/IEC 7816-13**
- **ECC // 24727 Middleware Use Case**
 - **ISO / IEC 24727-1/2 at CD ballot (Nov WG4)**
 - **ISO / IEC 24727- 3 still at WD (Nov WG4/ TF9)**
- **Services to be supported by the ECC (info)**
- **Business models for the ECC (info)**
- **ECC operation and issuance procedures (info)**

CEN / ISSS

CWA eAuth

CEN TC224

CWA 14169

TS ECC 1

CWA 14890

TS ECC 2

WG17

WG16

WG15

EN PP IAS

EN 14890 1&2

EN ECC



What's new with ECC standard

- First standard methodology to proof smart card durability
- ECC **USB card interface compliant with 7816-12**
- First standard taking into account European regulations
- First standard to solve the problem of interoperability of IAS implementations by using ISO/IEC 7816-15 mechanisms
- First standard referencing Match-on-Card Biometrics
- First standard for interoperability with ISO/IEC 24727 middleware



More information

- **email: lgaston@axalto.com**

Thanks You!