Smart Card or Not

3DAS the Dawn Of What Could Have Been A New Way

philip andreae and associates

Magnetic Stripe Limitations

Today's Magnetic Stripe is limited in data space

Chip Cards Vary In Capabilities

Simple Memory Cards

Secured Memory Cards

Processor Chips

Crypto Chips

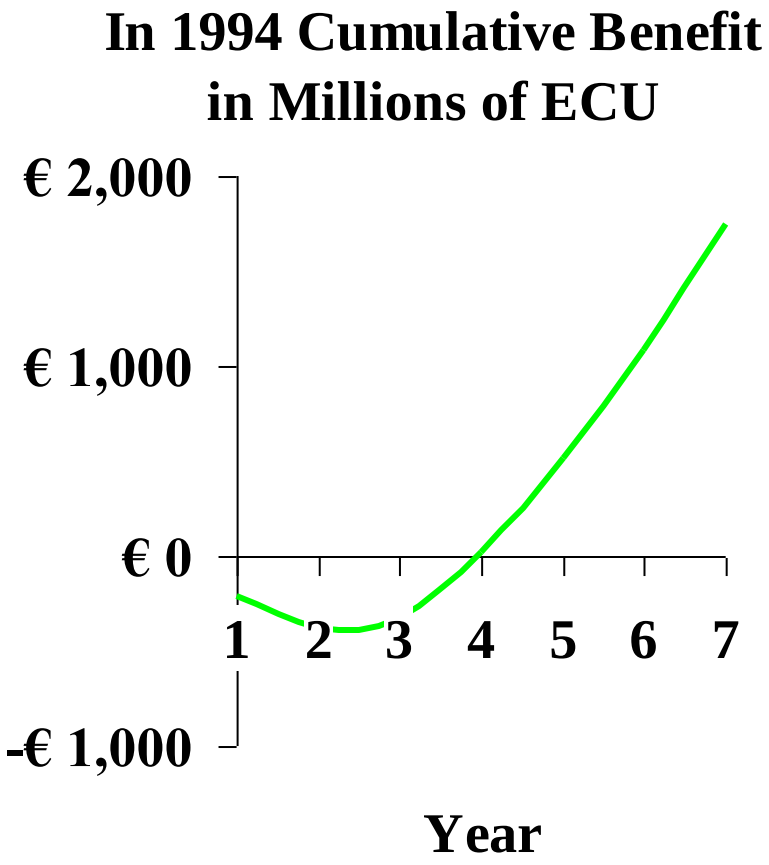
Multi-application Operating Systems

• Multos	Multos
• Java Card	Global Platform
• Host	Oberthur
• &	240 Others

Contact, Contactless or Combi

Europe Used a Business Case

To Justify Global Investment In Smart Cards



Based On

- **A CAM to stop counterfeit loses**
- **A CVM to reduce lost & stolen card fraud**
- **Off-line algorithms to reduce processing cost**
- **An infrastructure to support new profit opportunities**

CAM and CVM

EMV created a vocabulary

- CAM Card Authentication Method
- CVM Cardholder Verification Method

3DAS employs that vocabulary

Why The Banks Wanted Chip ?

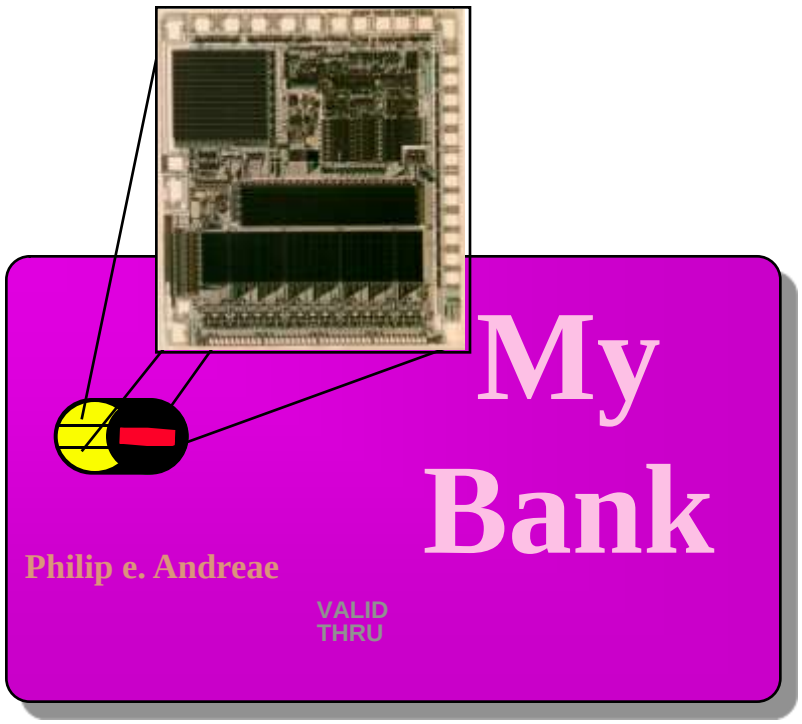
The Technology Was Proven

It Was Future Safe

The Banks Believed In the Integrity It Provided

Incremental Profit Opportunities Might Exist

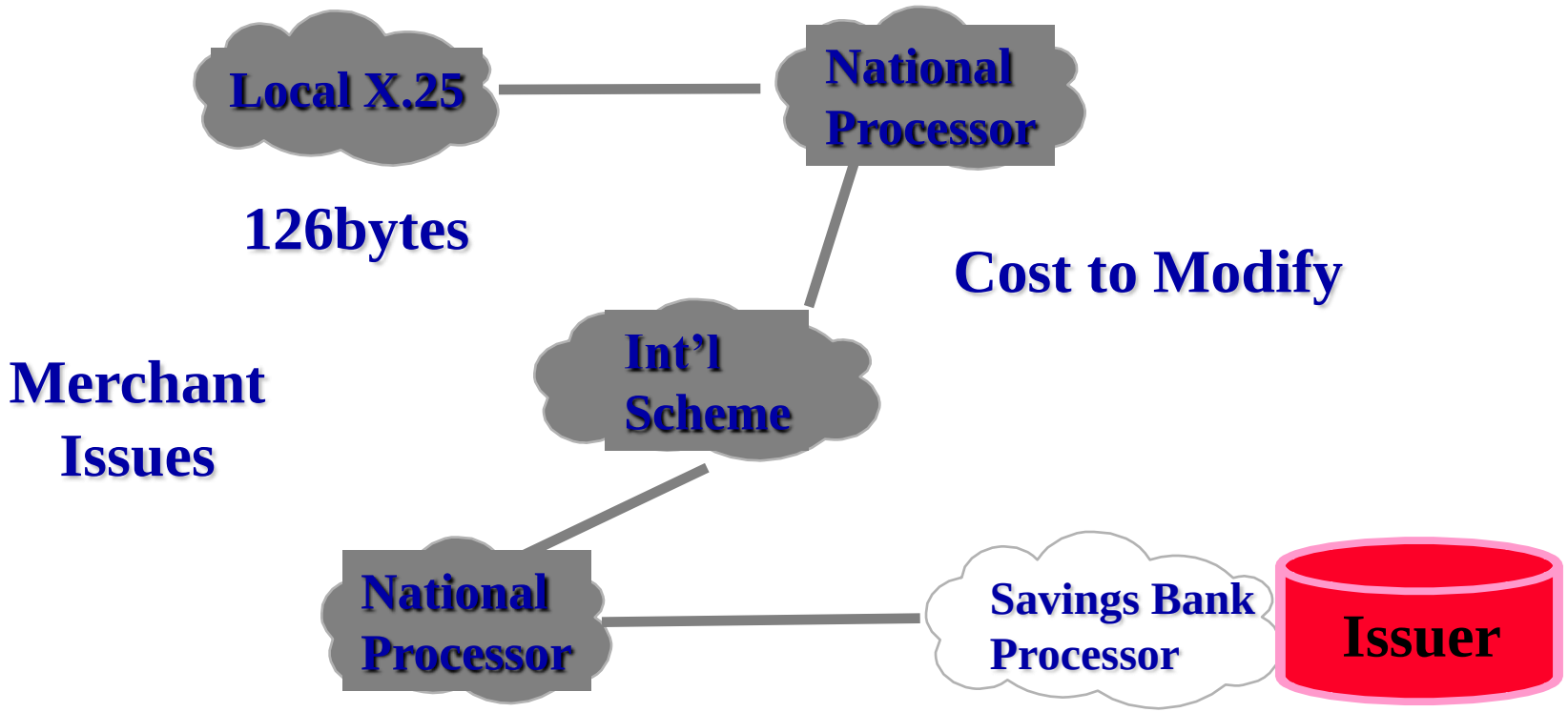
The Banks Wanted Control



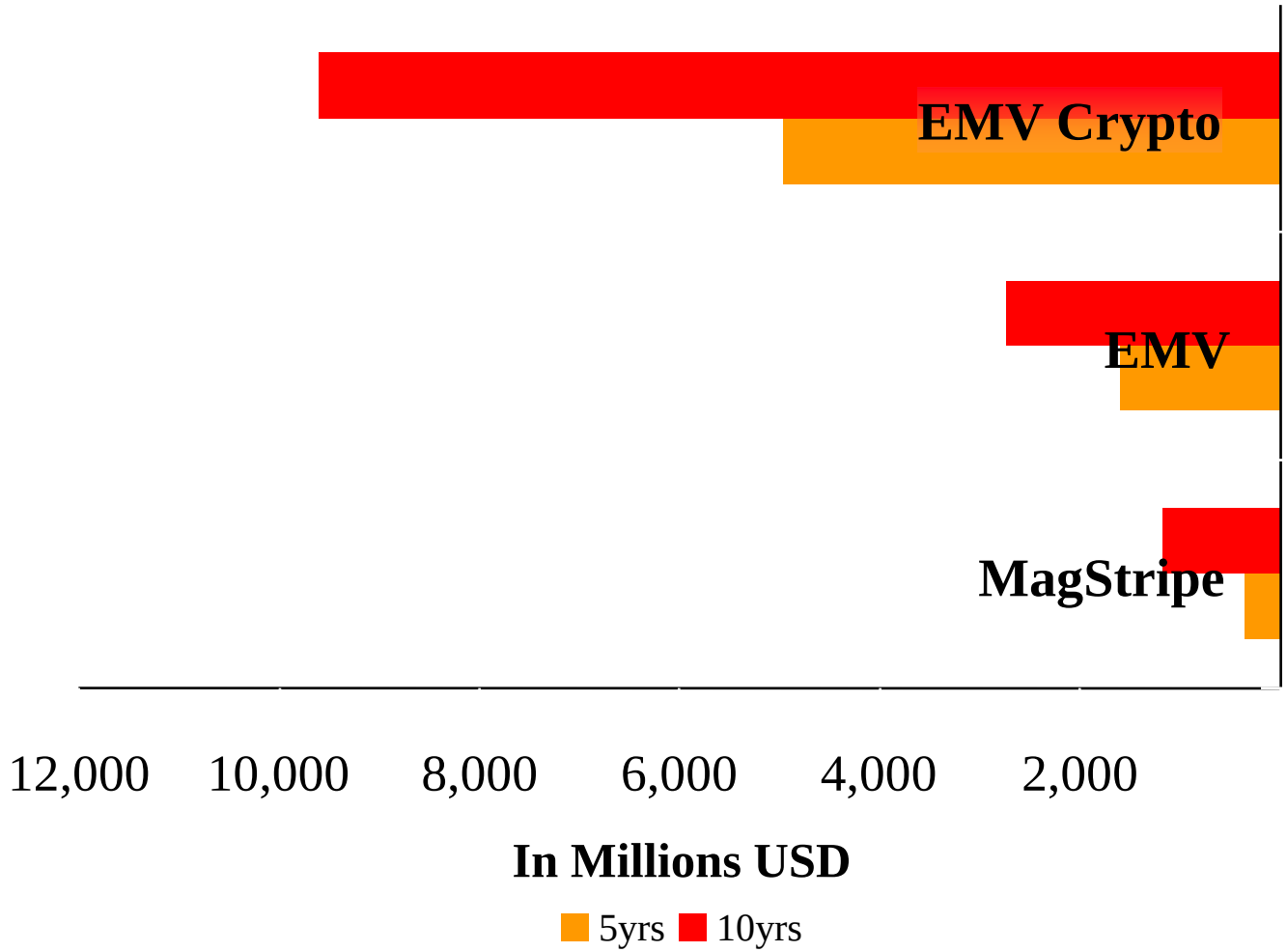
Network Nightmare

Legacy Systems Abounded

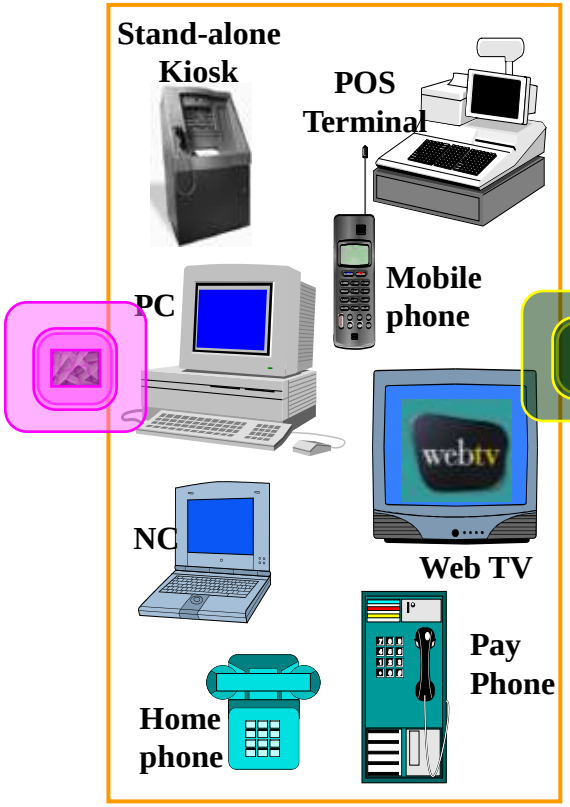
Aspects Implementing EMV Surfaced Network Issues



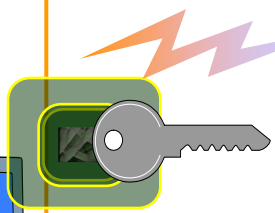
Fiscal Nightmare US Business Case Based on 1996 Data



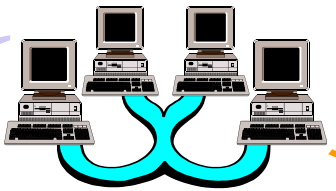
The User Requirements Are Simply
From Anywhere, Easy and Always the Same



Multiple Devices



The Insecure Internet



Tracking & Tracing

Inventory Control

Finance

Order Processing

Confidential Corporate Information Processing Services

Safe & Secure Virtual Commerce

Held Back by Complexity and a Lack of Global Standards

What are the economic drivers

- Improvements in Internal Process and Procedures
- Empowerment and the Need for Information
- Customer Service and Retention
- New Sales Channel
- Competition

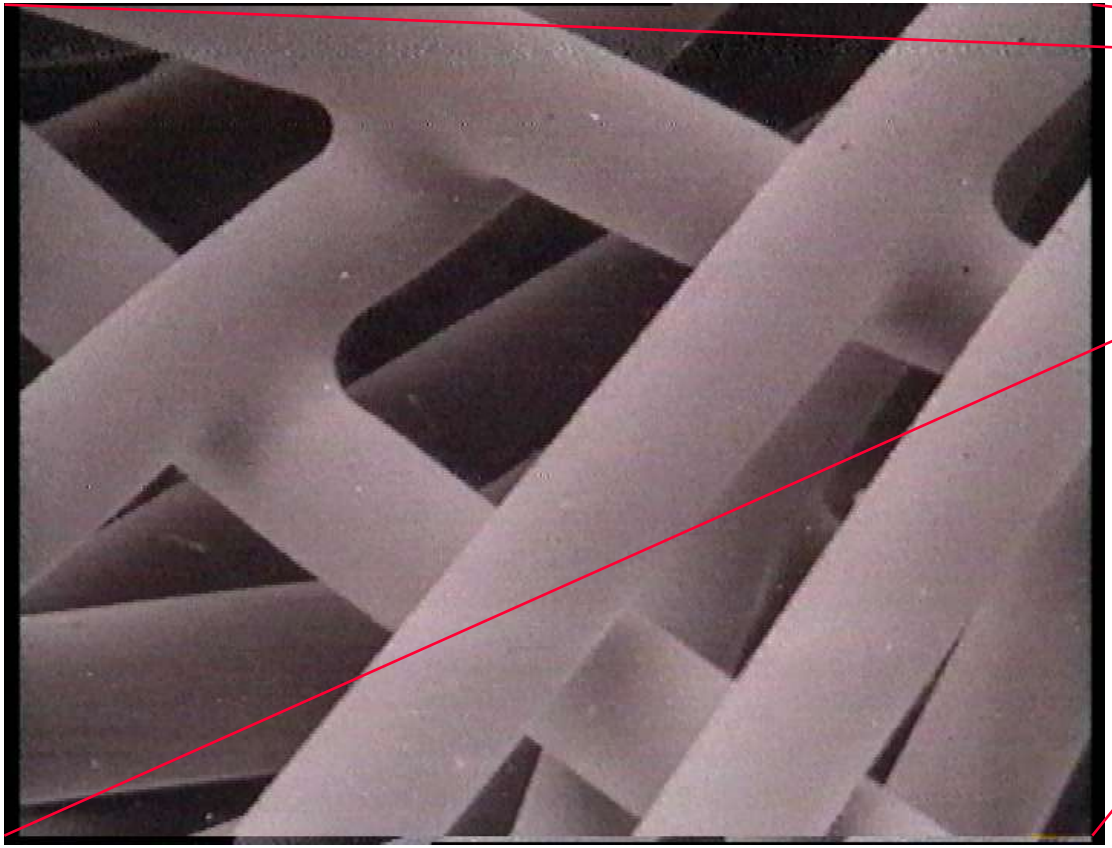
Who Should Drive Internet Solutions

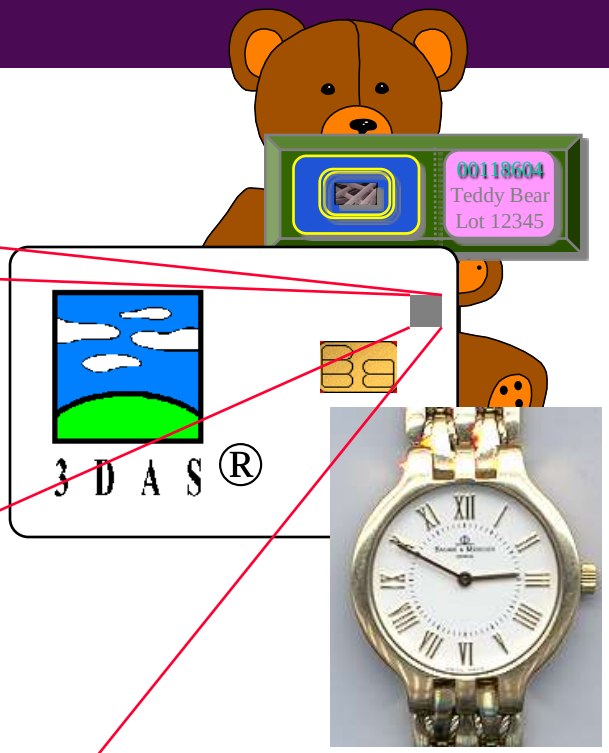
- Technology and Security Professionals?
- Marketing and Business Professionals?
- European Pride (Smart Cards are French)?
- Visa, MasterCard and the Banks?

Three Security Solutions

- Account Number & Password
  - Mobile
  - Cheap (somewhat secure)
  - Demands Your Memory
- Software Wallet
  - User Friendly
  - Secured Inside a PC?
  - Not Mobile
- Physical Token
  - Mobile
  - Easy To Use
  - Requires a Reader

1997 Unicate Introduced 3DAS





Authenticate
Your Product
Or Card

The 3DAS System
The 3DAS Marker Is Unique

The Production process can only generate random markers

A 3DAS Marker is unique in 10^{36}th Objects

The terminal must read the marker

To clone 3DAS requires replication in 3D

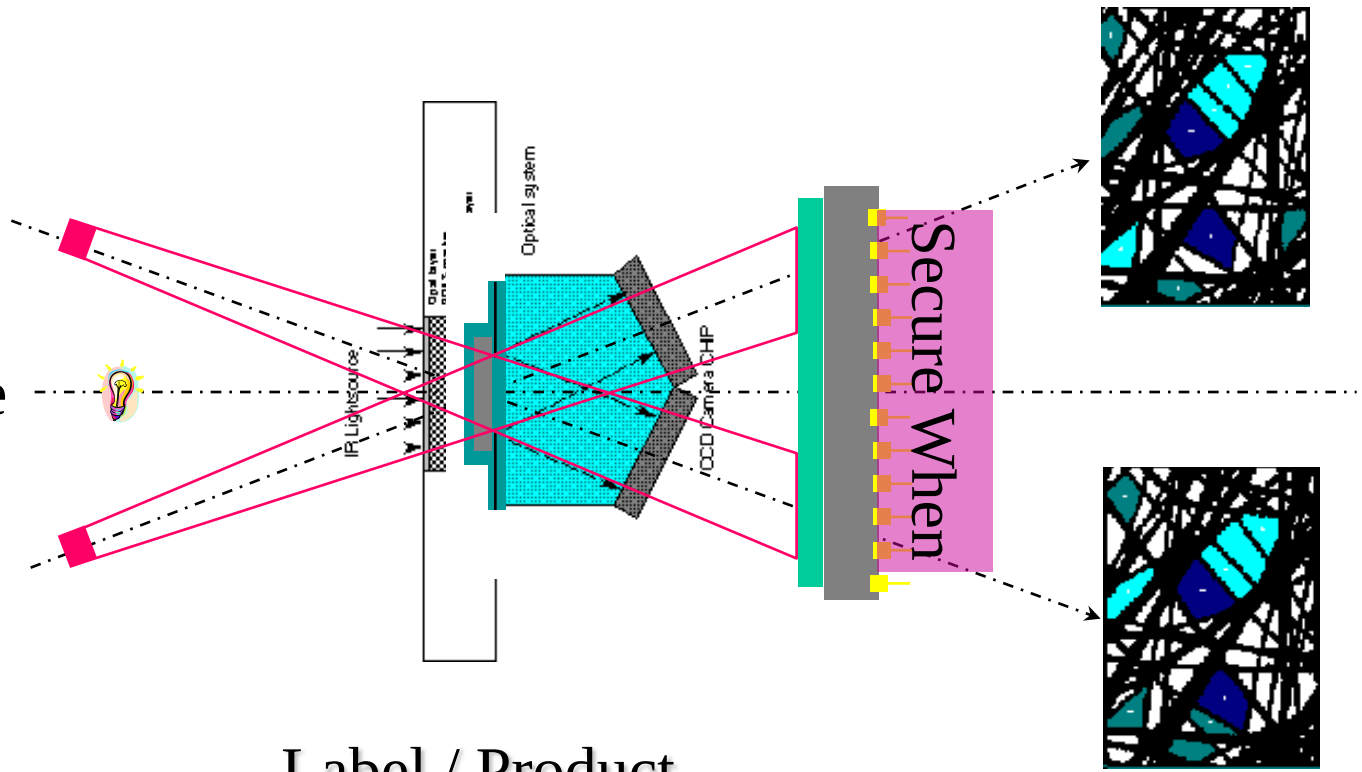
- The marker is in 3 dimensions 2 x 2.4 x 0.24 millimetres
- Filaments average 38 micron
- A 4 micron deviation in the its 3 dimensional geometry is a different marker

A Simple Optic Read

+20°

infrared Source

-20°



Label / Product

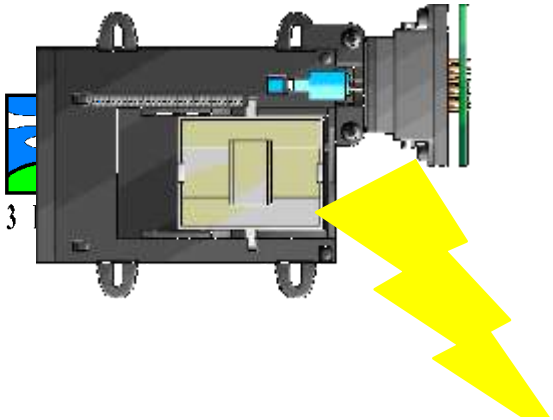
The 3DAS Reading Process
A Simple Use of Parallax

6 milliseconds infrared flash

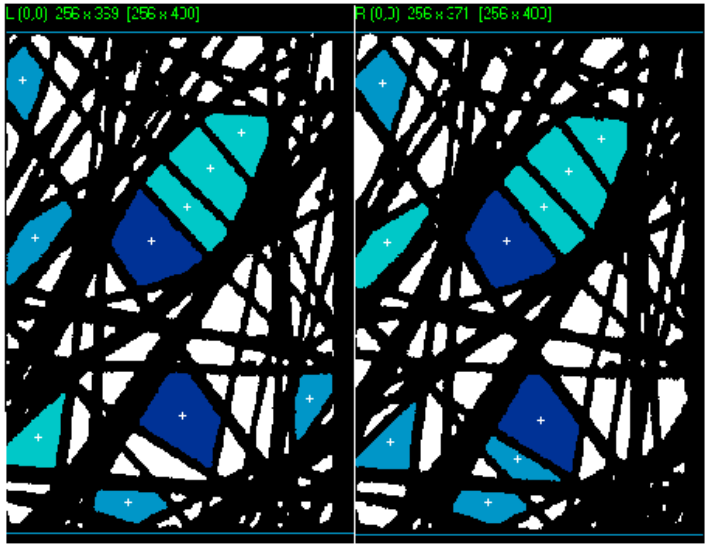
40 milliseconds photo image

100 milliseconds table generation

Total read 150 milliseconds



#	A area	X pos	Y pos	#	A area	X pos	Y pos
0	1891	112	106	0	1963	115	107
1	1820	136	195	1	1758	142	198
2	1369	156	70	2	1439	163	71
3	1027	138	88	3	1060	144	89
4	963	24	206	4	1033	24	107
5	908	181	52	5	896	188	55
6	876	23	104	6	855	21	26
7	698	94	239	7	821	27	208
8	637	233	186	8	687	101	240
9	637	13	24	9	534	123	218



3DAS Guarantees Irrefutability

#	A area	X pos	Y pos
0		112	106
1		136	195
2			
3			
4			
5			
6			104
7			
8		233	
9			

#	A area	X pos	Y pos
0		115	
1			
2			
3			
4			107
5			
6			
7			
8			
9			

Using the 8 Byte Hash Of the Transaction As The Pointer

(In this case Hash = 00118604)

Strong Security with The 3DAS Signature

Physical Tokens

3DAS

- Cost Effective <$.30 per card
- Each one is Unique in 10^{36}
- Each Cloning is Unique
- Not Subject to Replay
- Supports any Data Carrier
  - Blank Token
  - Magnetic Stripe Card
  - Inexpensive Memory Chip
  - Bar Code
  - Diskette
  - EMV
  - . . .

Smart Cards

- Data Limited by Chip
- Requires Programming
- Speed Limited to Chip I/O
- Costly >$1.00 Per Card
- Replaying Certificates is Easy
- Clone One Clone Millions

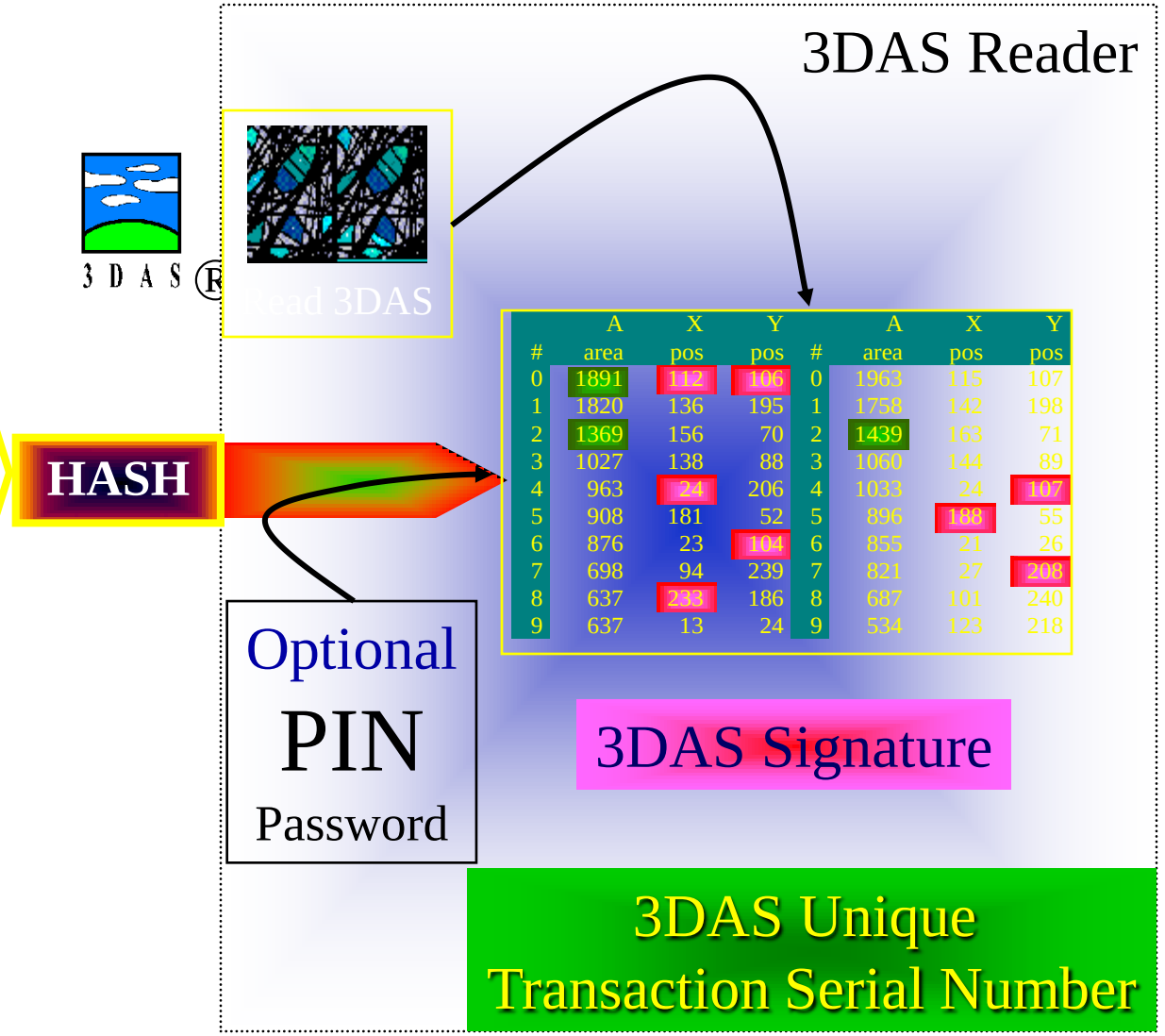
Crypto Smart Cards

- Expensive >$3.00 per Card
- Clone One Clone Millions
- Still Uses a One Way Function

Primer in 3DAS Mathematics

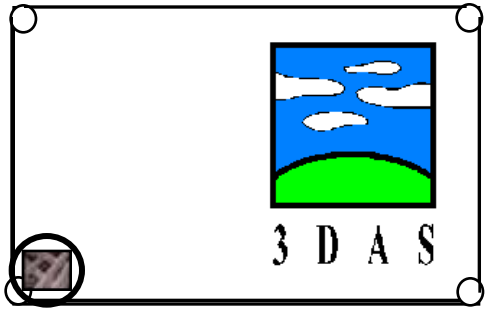
A Hash Is a Means of Assuring the Integrity of Data

- Transaction Description
- Date and Time
- Consumer Id
- Merchant Id
- Amount

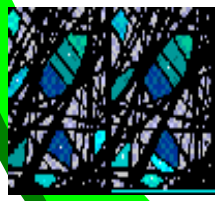


#	A area	X pos	Y pos	#	A area	X pos	Y pos
0	1891	112	106	0	1963	115	107
1	1820	136	195	1	1758	142	198
2	1369	156	70	2	1439	163	71
3	1027	138	88	3	1060	144	89
4	963	24	206	4	1033	24	107
5	908	181	52	5	896	188	55
6	876	23	104	6	855	21	26
7	698	94	239	7	821	27	208
8	637	233	186	8	687	101	240
9	637	13	24	9	534	123	218

3DAS Is the Ultimate In Identification



Optically Read
3DAS Marker



1

Transmit 3DAS Code
To the Card Issuer
(7x4 bit - 80bytes)
Use The Unique Number as Identification and a key to any Database

2

Card Issuer's Database

Yes
The Card
Is Present
& Genuine

3DAS Supports On-line PIN

Without any network security

1

2

3

4

5

Request the Pin

PIN

Add the PIN to the Hash
to Point and create 3DAS Signature

Issuer Database

Yes

The Card is Genuine
The Person is Verified
The Transaction is Unique
and it is Irrefutable

The Business Case for 3DAS Technology

Was Compared With the US Chip Card Business Case

- Developed PC-based model to evaluate impact of 3DAS
- Used current Visa and MasterCard industry data
- Incorporated incremental costs to upgrade cards, POS terminals and ATMs to 3DAS technology
- Estimated cardholder and retailer education costs and Issuer, Acquirer and retailer infrastructure migration costs
- Used a five year evaluation period

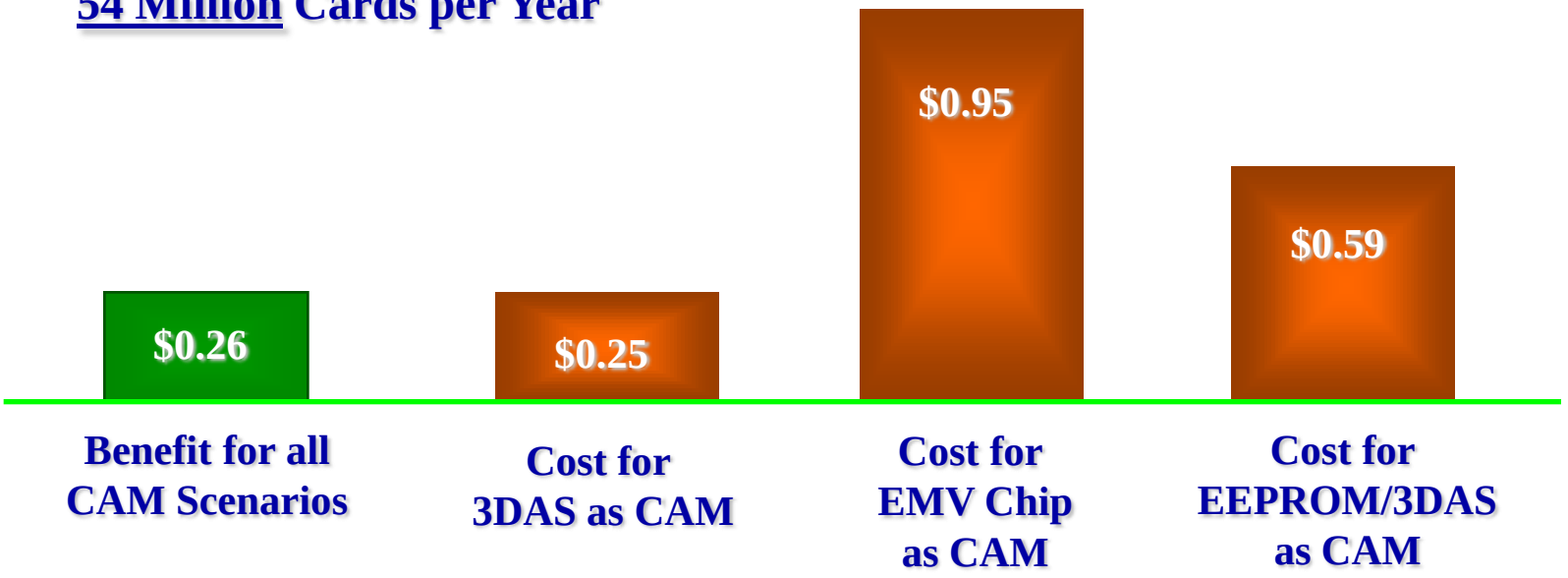
Methodology was same as used for chip / PIN business cases developed for MasterCard and Europay

The total cost and benefit can also be expressed on a per card basis

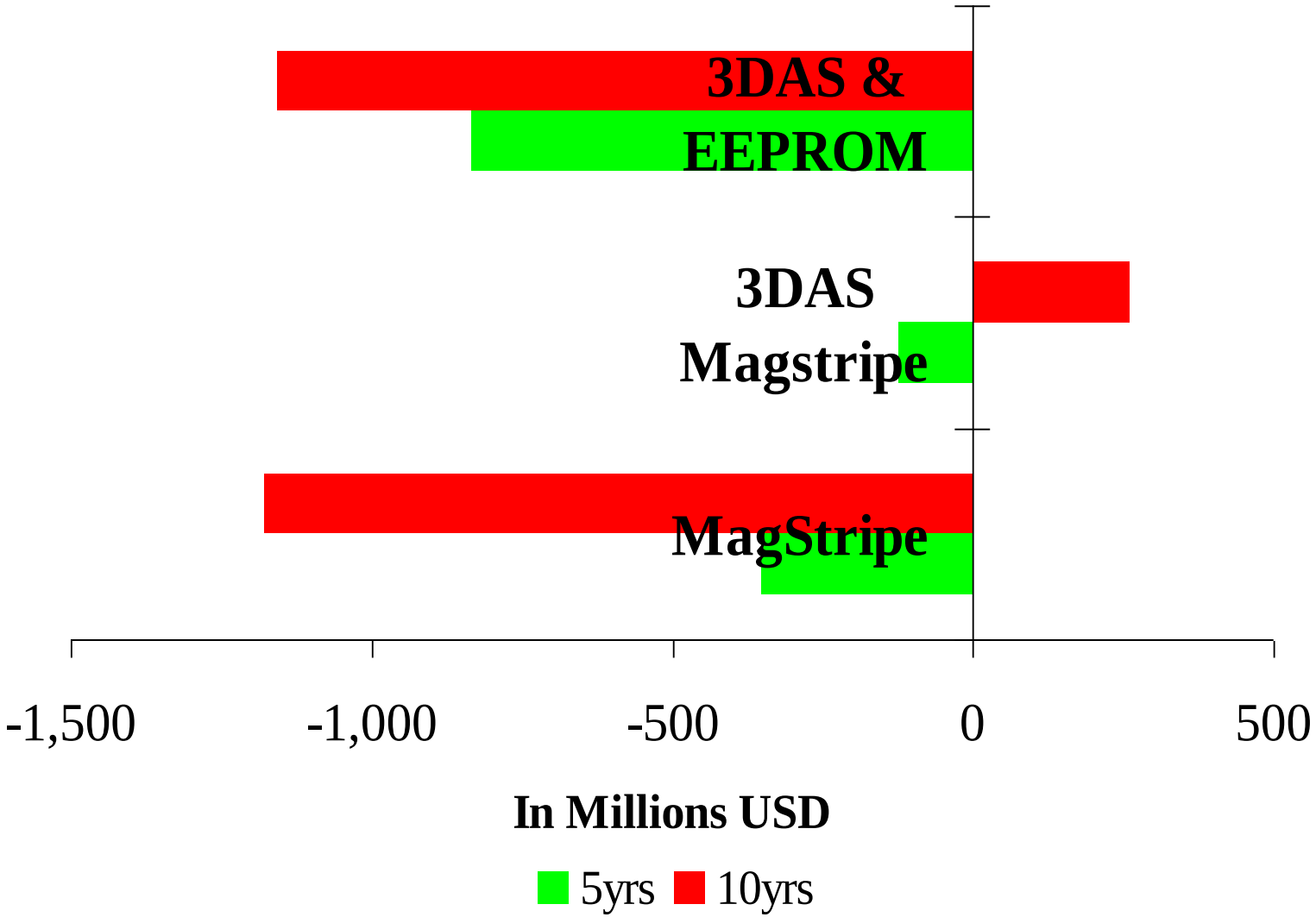
A/P Market ($US)

Average Cost and Benefit per Card per Year Over the Five Year Period

Based on an Average of 54 Million Cards per Year



3DAS in the United States
A Sound Insurance Policy

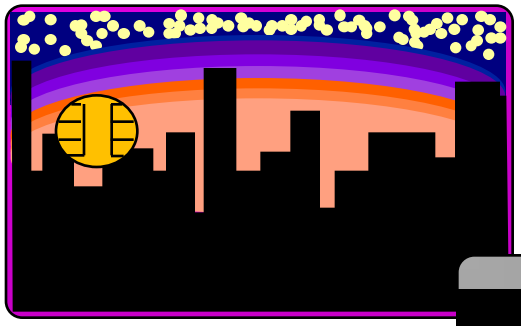


3DAS is Designed to Grow With Your Business

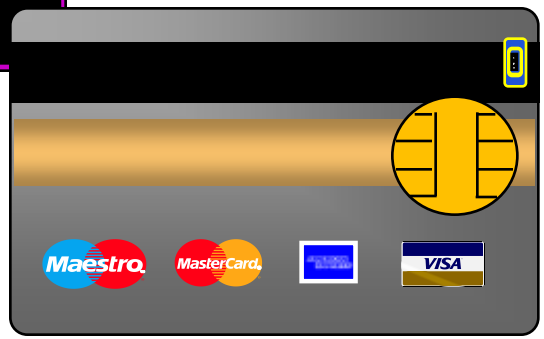
Mag-stripe → **EEPROM** → **EMV Chip**

Mag-stripe	EEPROM	EMV Chip
Access	Stored Value = Data	E-Purse
Identification	Rewards	? ? ? ?
Payment Card	Certificates	
Loyalty	Profile (Health care)	

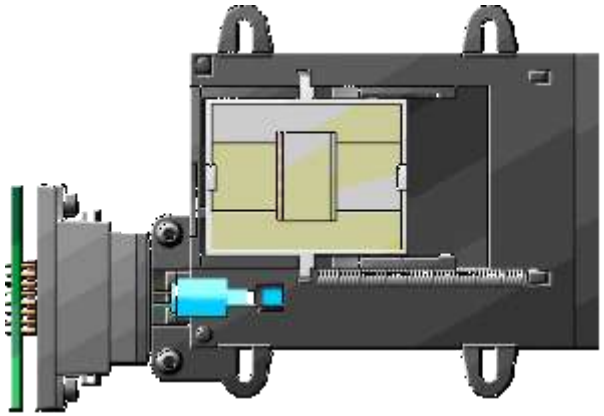
Random

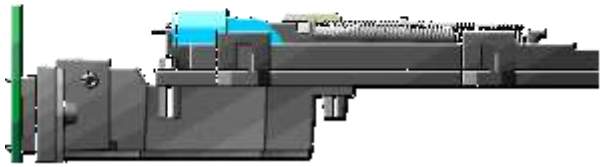


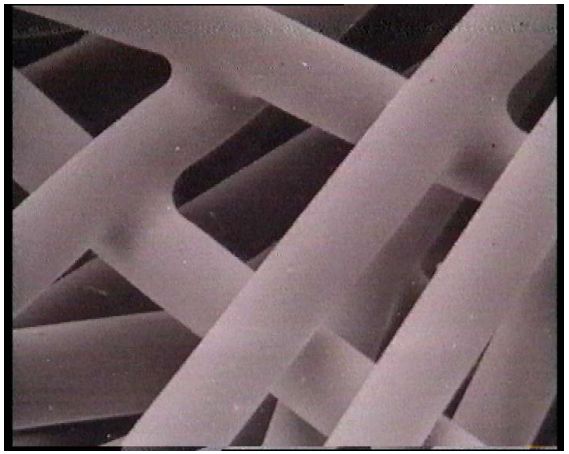
Chaos



10^{36}







The 3DAS Algorithms

- ✓The 3DAS FastKey
- ✓Cost Effective On-Line PIN CVM
- ✓Secret Data = *f* {3DAS + Your Secret Key}
- ✓The Hash = *f*{Irrefutable Transaction Data}
- ✓Off-Line PIN Verification & the 3DAS Internet Tunnel
- ✓On/Off-Line Product & Data Authentication
- ✓Off/On-line *CAM* for *Existing* Bank Cards
- ✓3DAS Signature = *f*{Hash + PIN}
- ✓Unique 3DAS Transaction Ref#

3DAS

a Physical Token Offers the Ultimate In Security

Authenticity	The **Token** Is Present
Verification	The User Is Present
Integrity	The Transaction is Correct
Confidentiality	The Details are Secure
Irrefutability	The Person/Token Executed It

$.30 a Token, $30 per Terminal

without legacy system changes

Why is 3DAS better / different

3DAS is Cost Effective

- $.30 Per Card & $30 per reader (in volume)
- Seamless integration to today's systems

The 3DAS Reader Fits Anywhere

3DAS Is Bullet proof

3DAS Is Unique

- 10^{36} today. Tomorrow is the same
- No Secrets Required

Connects You to Your Authentic Customer

3DAS Is Business and User Centric

3DAS Offering Irrefutability

"The small and simple tactic wins the day, when generals themselves choose it over the grandiose and costly."

- Sun Yat Sen, "Notes of a revolutionary", 1927