



# Next Generation Hardware Security Concept: Protection For The Next Decade

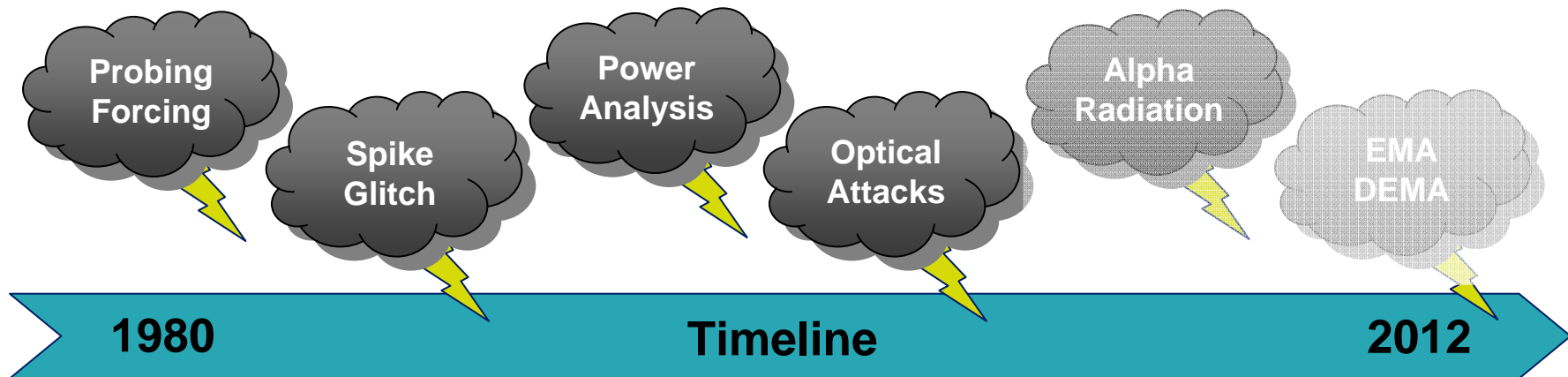
Joerg M. Borchert  
Vice President  
Chip Card & Security

**Infineon Technologies North America Corp.**



Never stop thinking

# Attacks And Countermeasures An Everlasting Fight ?



... taking into account all known attack scenarios such as ...

... stronger protection against known attacks. ...

**High Security**  
Dedicated Protection Against

Security enhancements against recent attacks

protected against known attacks

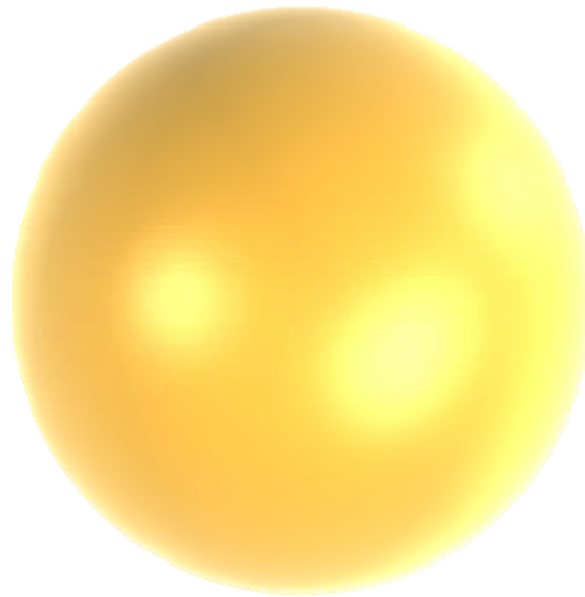
for known attacks in public domain

• Protection against known attacks-

includes several dedicated security features, like

**Is "protection against known attacks" enough for you ?**  
**What does "known" mean – by whom... and when ?**

# New Concepts Are Needed to Lead The Way Adapting Nature's Successful Strategies



**The next decade needs comprehensive and long lasting security.  
Nature demonstrates successful survival concepts.**

# Biological Cell Used For Inspiration Security Is An Integral Part



**Nature needs secure data storage and processing in each cell.  
A cell acts like a secured computer, working autonomously.**

# In Nature, Cells Are Permanently Under Attack Cell Protection Uses Intrinsic Mechanisms



**A cell is exposed to manifold attacks, like UV light or radiation.  
Although built from delicate materials, cell functions are robust.**

# Transferring Nature's Mechanisms Turning Ideas into Products



Nature's Mechanisms	Ideas for Smart Card Protection
Double Helix	Double CPU
Different Coding	Different Masking in the CPUs
Connection of Helices	Mutual Error Checks
DNA Encoding	Program Encryption
Coded Processing	Encrypted Calculation
Flexible Shell	Insensitive and Robust Design
Autonomous Control	Automation of Security Features
Self-Destruction	Security Alarms

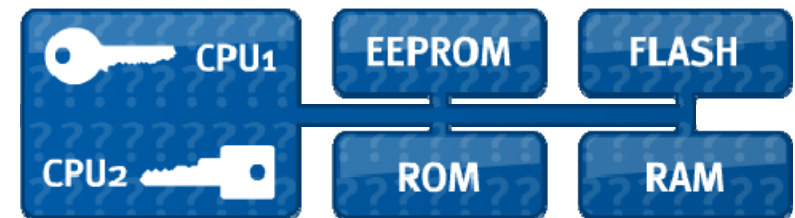
**Nature offers manifold mechanisms to protect a cell.**

**Analyzing nature yields many ideas for smart card security.**

# Important Findings In The Concept Phase Advantages For Customer And Manufacturer



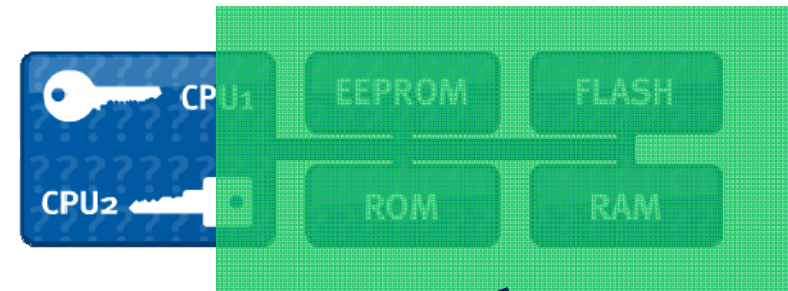
- The shift from analogue to digital security must be completed.
- Instead of millions of single attack variants, entire attack classes must be considered.
- Integral security must be comprehensive and must not hinder functionality.
- Detection of effects must be used instead of detection of cause.
- Secure products must be rugged.
- Security must be easy to use.



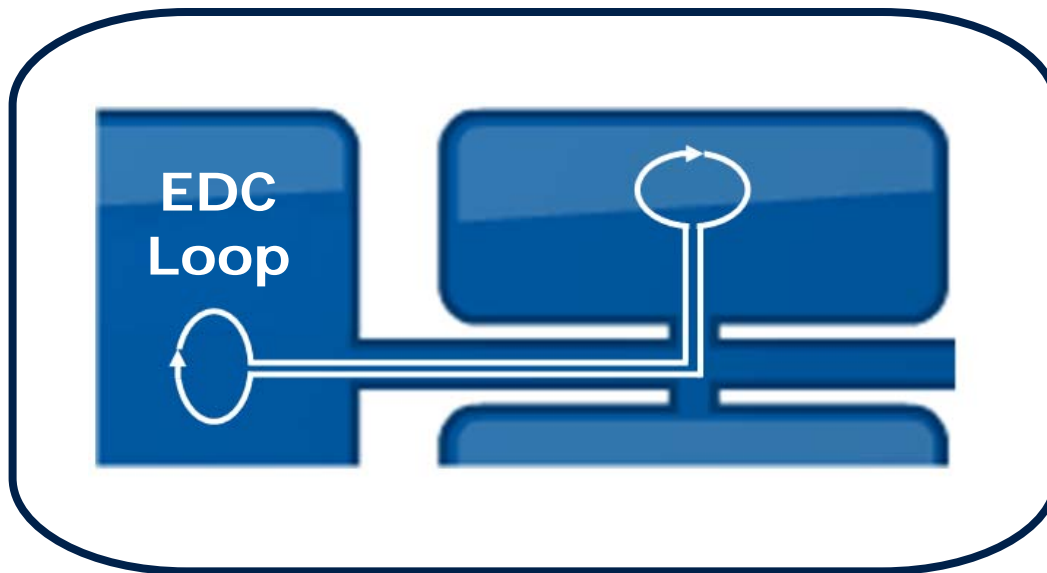
**Transferring nature's mechanisms to smart cards is possible !**  
**... and the realization has been accomplished by Infineon.**

# SLE 78 Security Mechanisms

## Comprehensive Error Detection



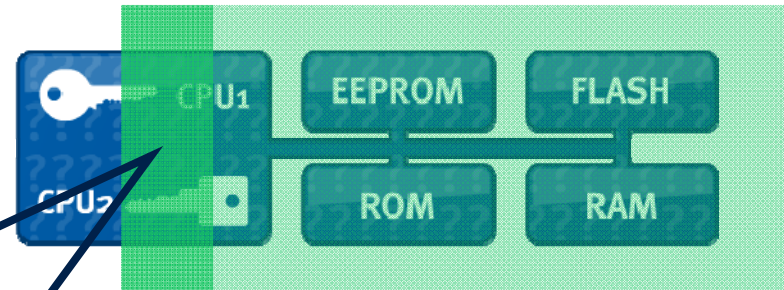
### EDC Protection



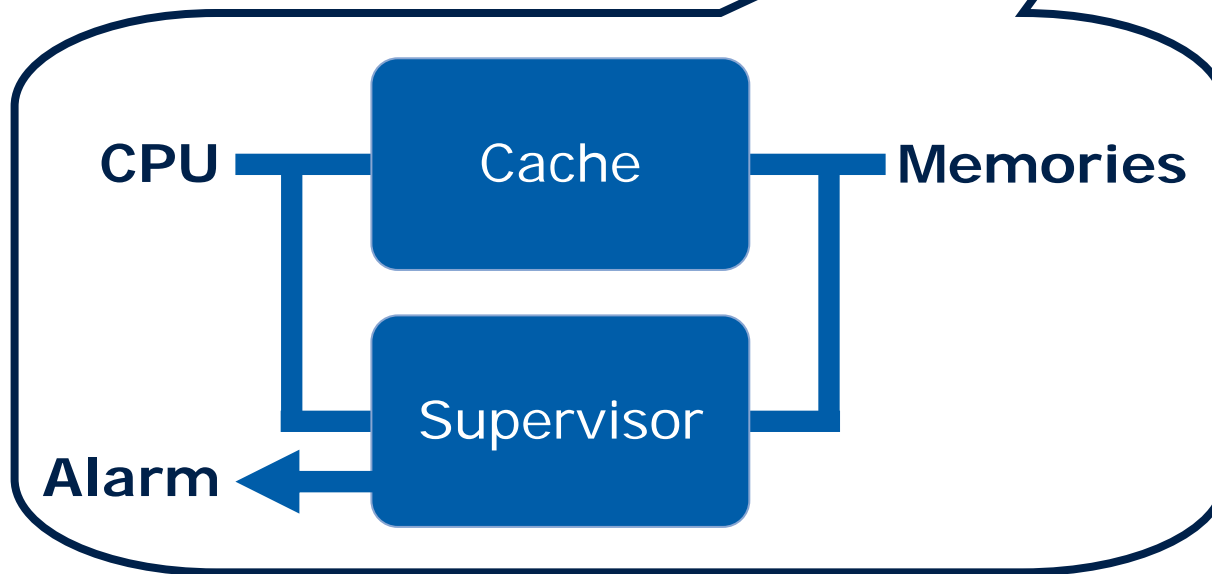
**Error Detection Codes protect memories, buses and core-parts.**  
**Single bit errors are corrected, multi-bit errors generate alarms.**

# SLE 78 Security Mechanisms

## Comprehensive Error Detection



### Cache Protection

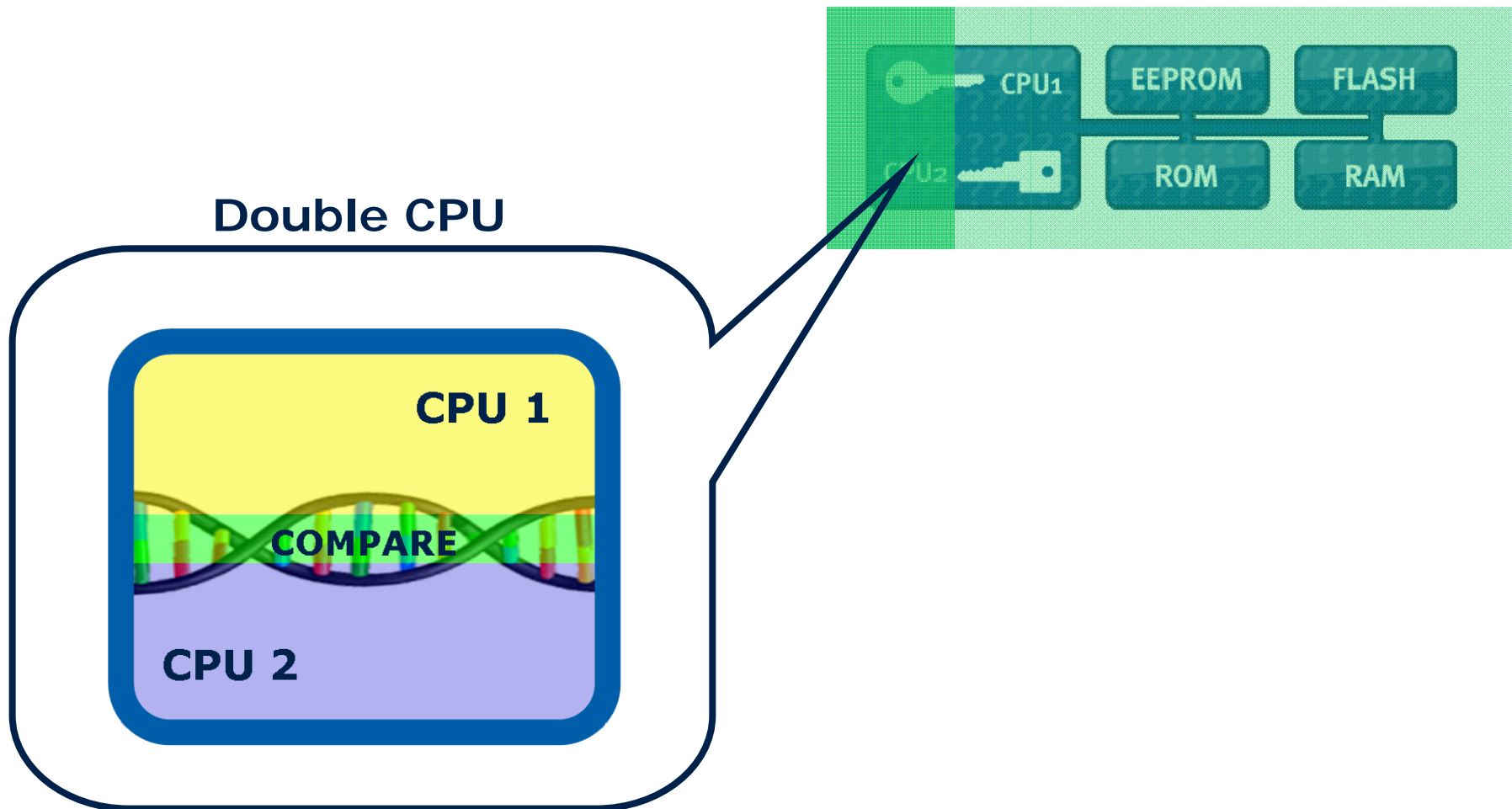


**Various attacks are published for unprotected caches.**

**The hardware automatically supervises the cache data integrity.**

# SLE 78 Security Mechanisms

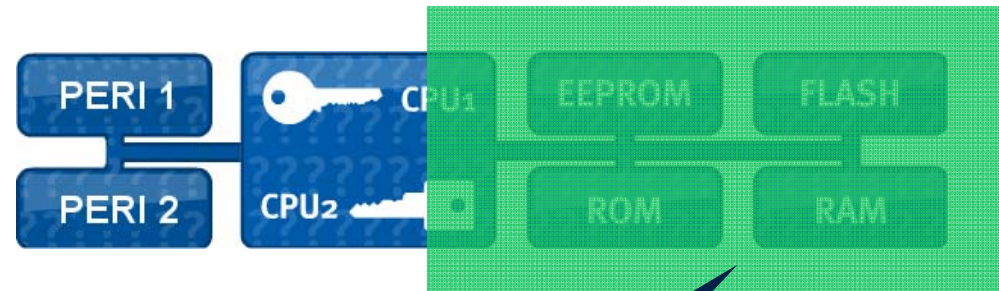
## Comprehensive Error Detection



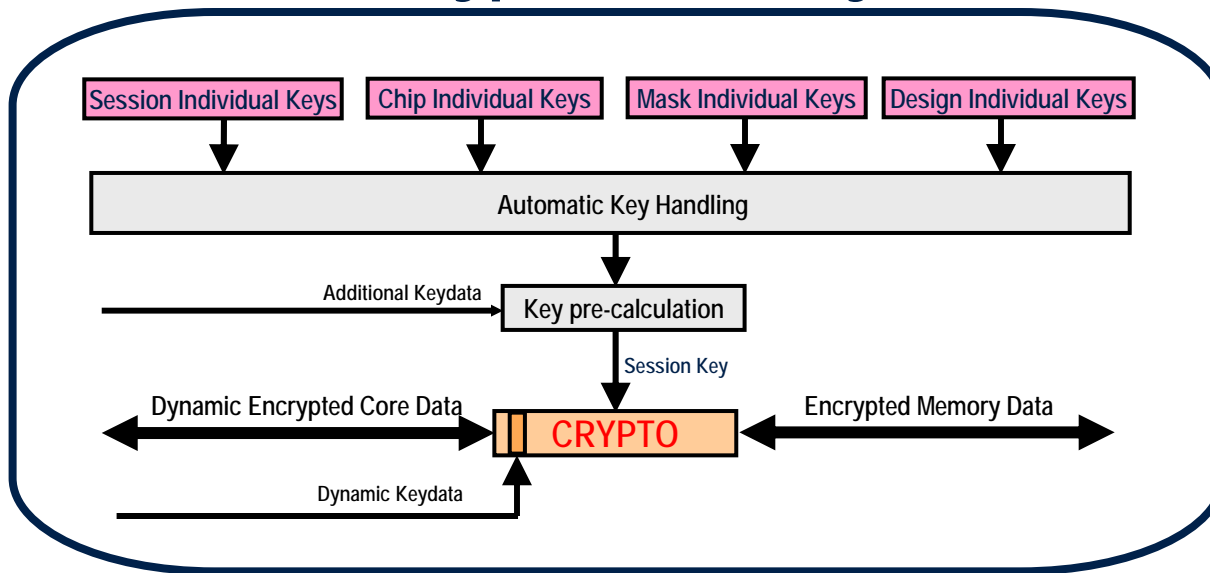
**Conventional designs would leave the CPU as a weak point.**  
**A double CPU can provide true intrinsic error detection.**

# SLE 78 Security Mechanisms

## Full On-Chip Encryption



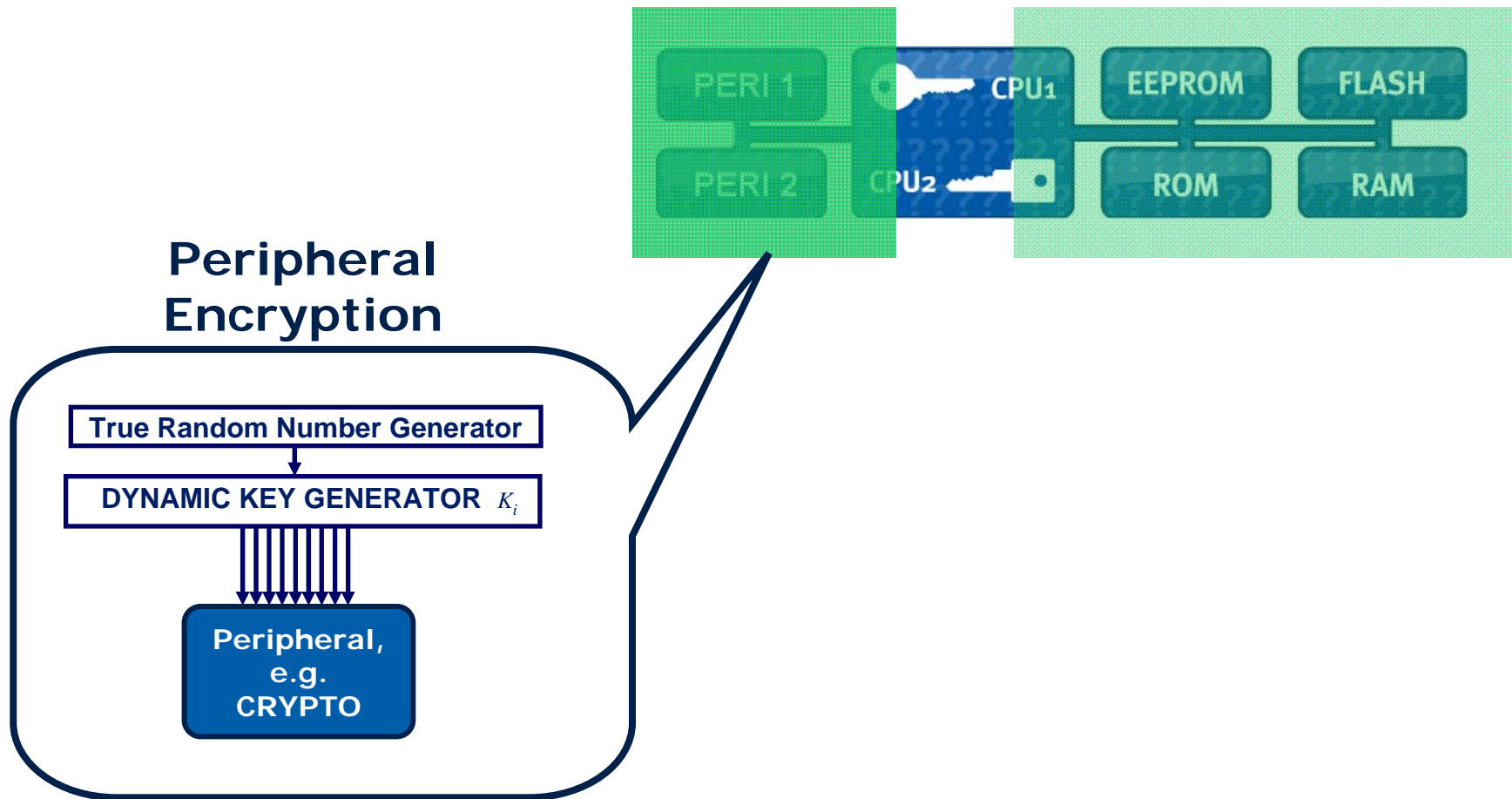
### Encrypted Memory



**Data in all memories and buses are profitable attack targets.**  
**Strong block cipher memory encryption protects these values.**

# SLE 78 Security Mechanisms

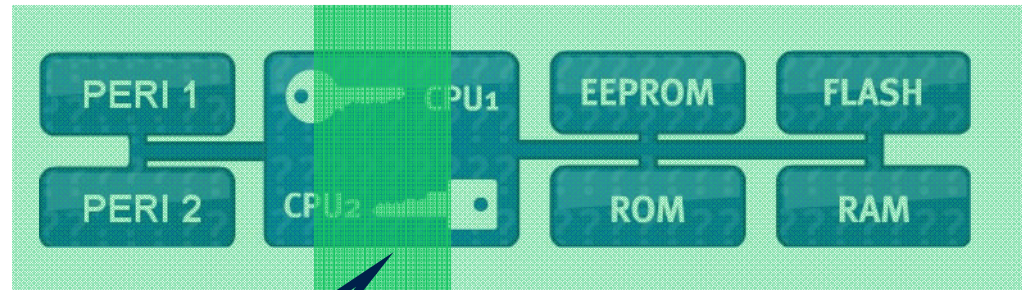
## Full On-Chip Encryption



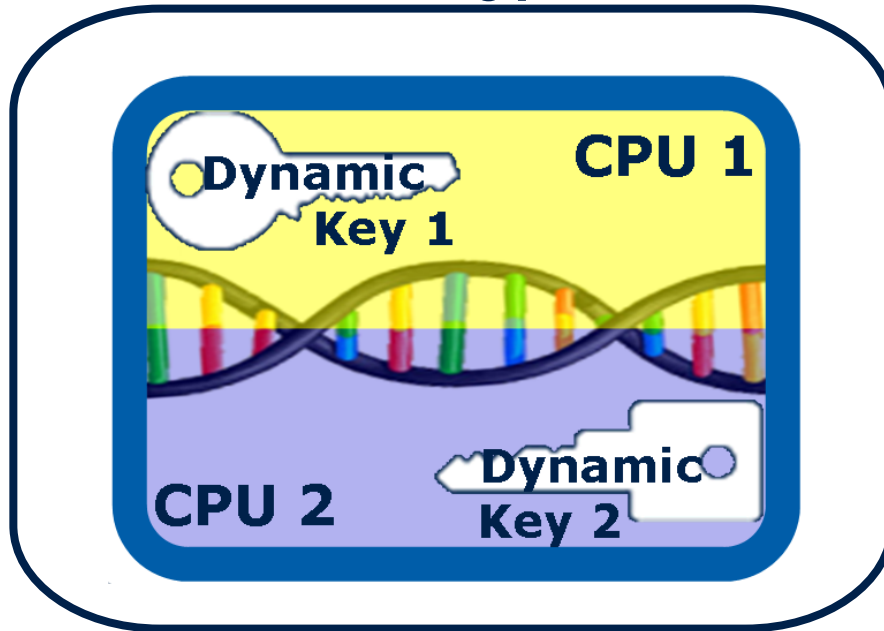
**Peripherals handle secrets and therefore are endangered.**  
**Dynamic bus encryption protects data for peripherals.**

# SLE 78 Security Mechanisms

## Full On-Chip Encryption



### CPU Encryption

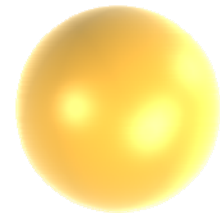


**All data processed in standard CPUs would attract attackers.**  
**Encrypted CPUs using encrypted calculation are implemented.**

# Learning From Nature Brings Advantage Customers And Manufacturers Both Benefit



- The future-proof security system is designed against all attack classes, encountering even the unknown.
- Digital, mathematically modeled mechanisms are utilized for self-contained security.
- Rugged design allows robust security ICs and smart card applications. High tolerance against environmental variations is achieved.
- Customer-friendly and easy-to-use security features enable convenience and efficiency.
- The new concept is focused on Return-On-Security-Investment and breaks the cost spiral of conventional countermeasures.



**In the near future, conventional concepts will reach their limits.  
The new SLE 78 security concept allows long-term sustainability.**

# The Integrity Guard And Its Key Facts Pioneered In The New SLE 78 Family



## ■ Integrity Guard is ...

- Fully encrypted data path leaving no plaintext.
- Comprehensive error detection over the complete data path.
- Digital security instead of analogue environmental checking.
- The protection of smart cards for the next decade !

**Future smart card security will rely on Integrity Guard concepts.  
Integrity Guard is available today to encounter future attacks.**



**We commit.**

**We innovate.**

**We partner.**

**We create value.**



Never stop thinking