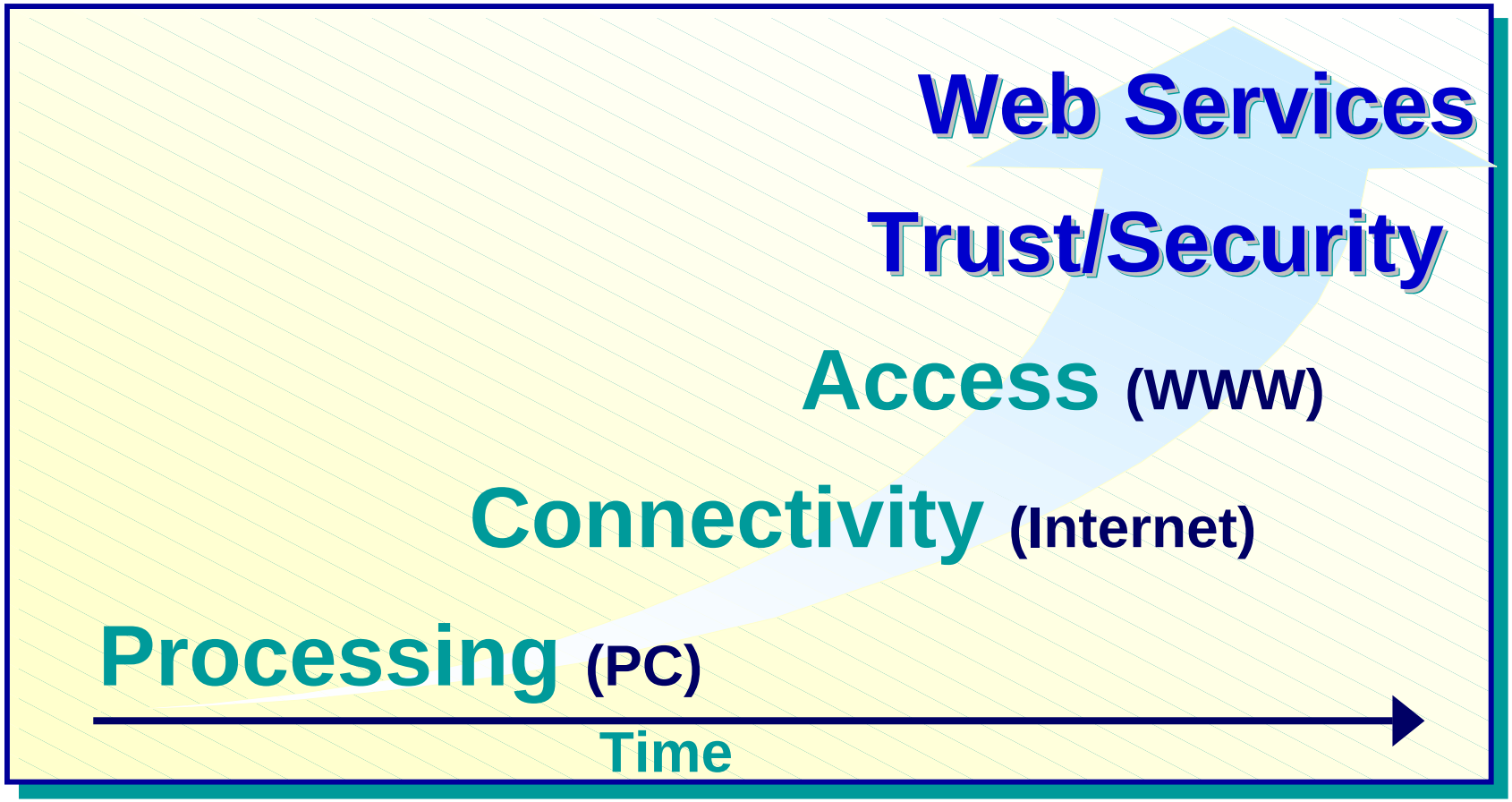
Infrastructures for Trusted Computing

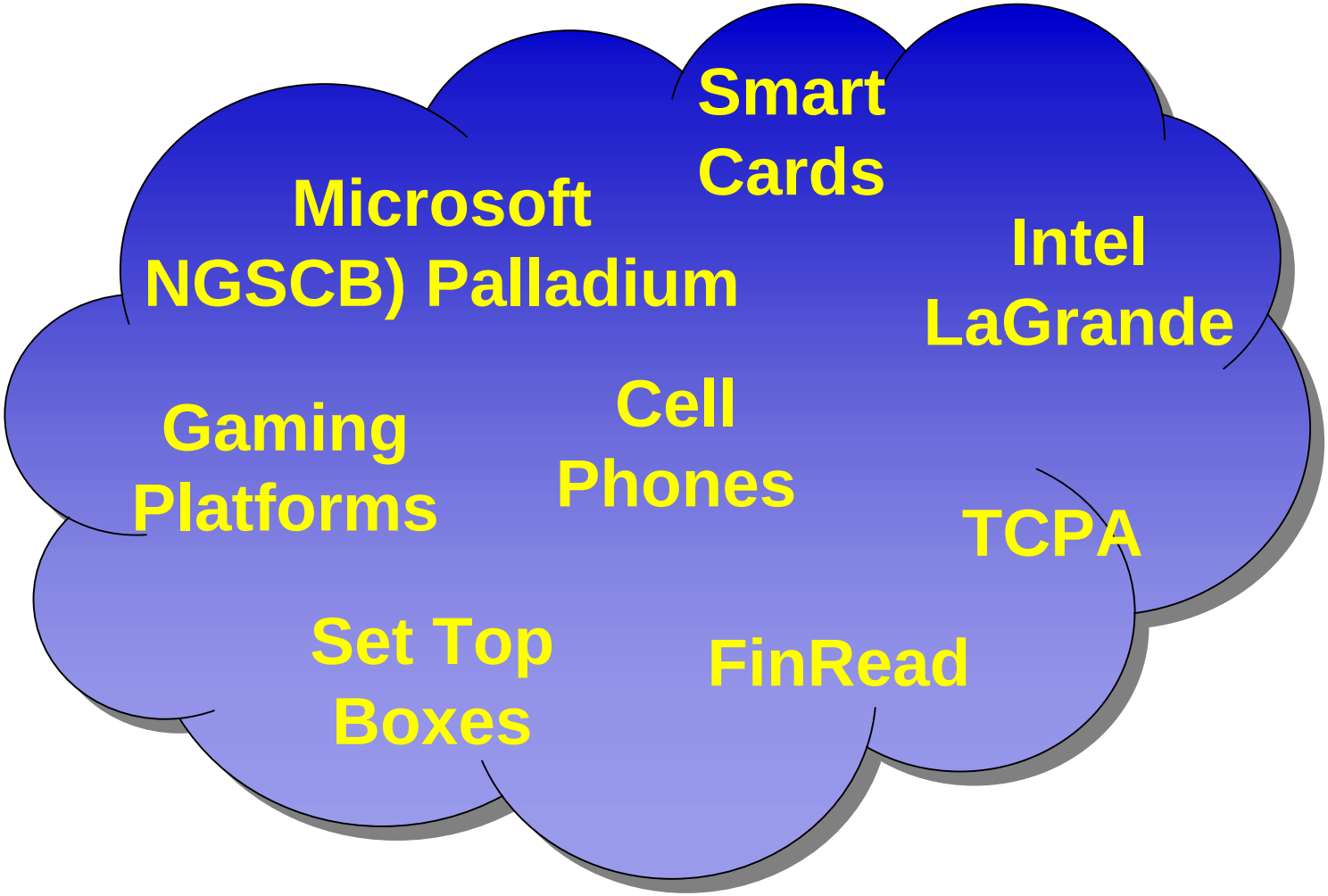
Smart Cards – Intelligent Readers
The Role of Trusted Peripherals

Lark M. Allen
Wave Systems Corp.
lallen@wavesys.com

The Evolving Digital Infrastructure



Trusted Computing Initiatives



Trust Infrastructures – Open, Shared

- ***Open***, ***Programmable*** and ***Interoperable Trust*** Required for Internet Devices

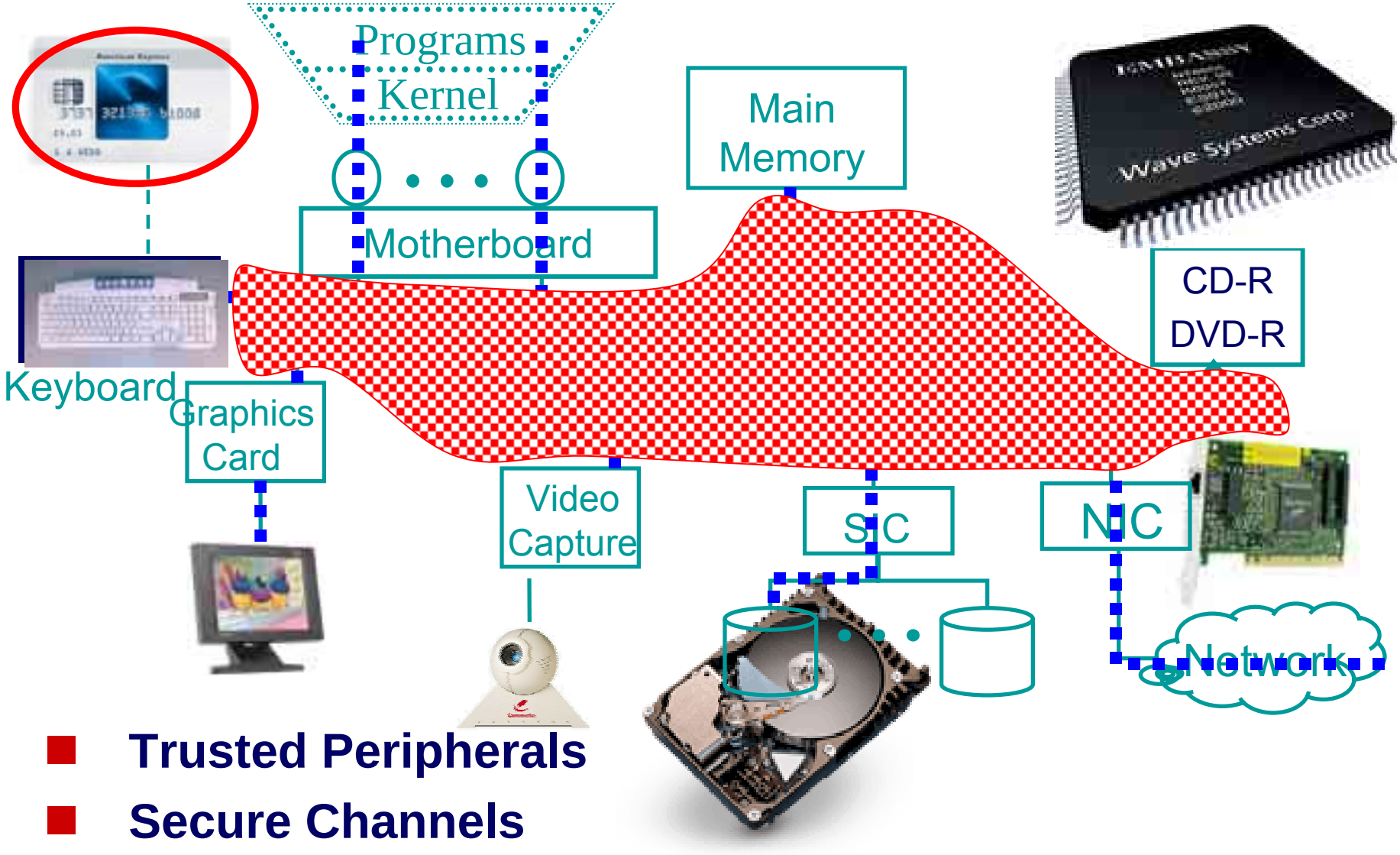
"Incredibly secure and trustworthy computer systems exist today, but they are largely independent, single-purpose systems that are meticulously engineered and then isolated."

Craig Mundie
SVP, CTO
Microsoft

Trust and the Platform

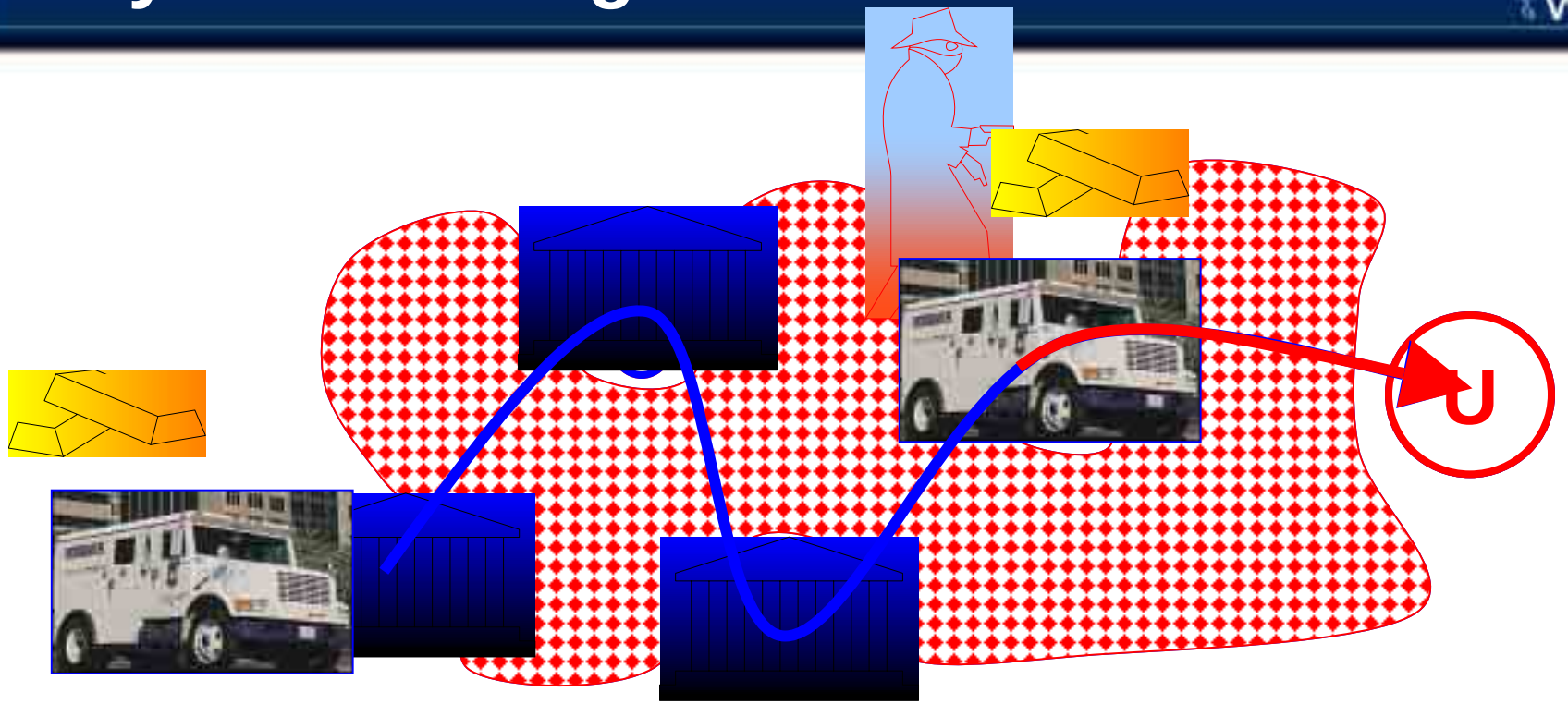
- Security at any layer can be defeated by accessing the next lower layer
- Trusted Computing requires security hardware as the foundation for platform security
- Plus security enablement features in each layer

Trusted Computing – Platform Design



- **Trusted Peripherals**
- **Secure Channels**

Systems Design – End to End Solutions

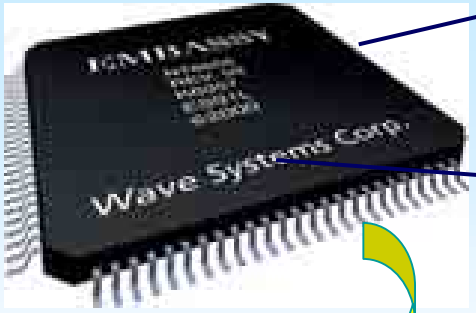


- Untrusted
- Trusted

- Untrusted devices cause the result to become untrusted

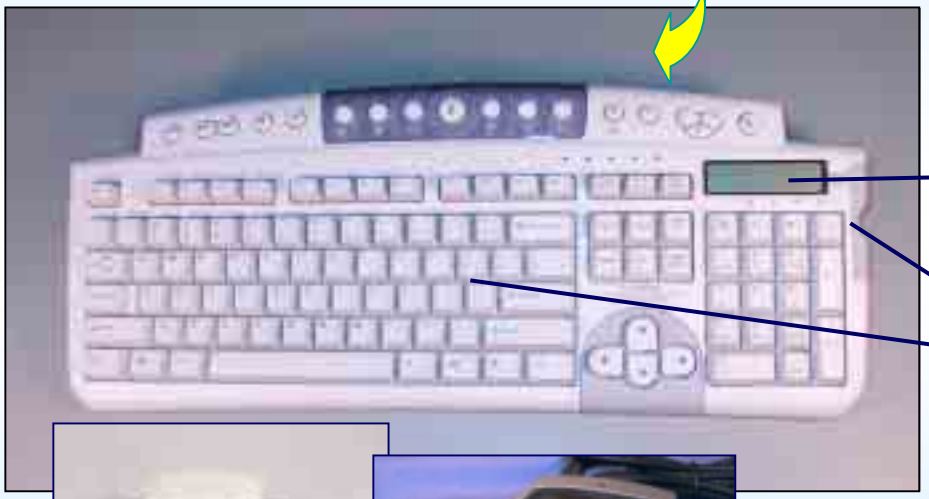
Trusted Peripherals - FinRead

Embedded Trusted Client Processor



Strong Cryptography

Secure
- Processing
- Storage
- Java



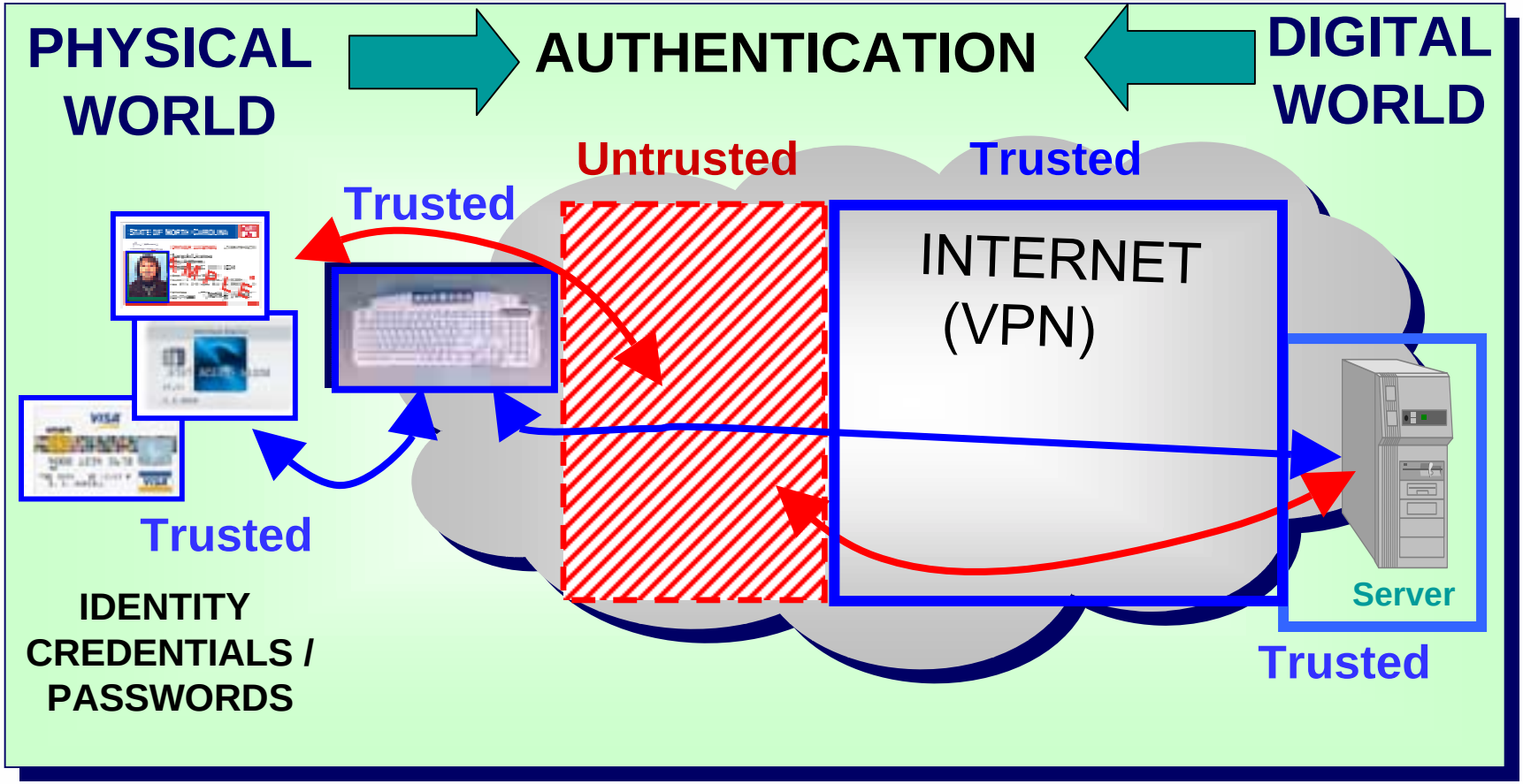
Secure Display

Secure Input

- Financial Transactions
- Multi-factor Authentication
- EU Finance Industry Spec
- Java Support- Finlets
- Keyboards, smart card readers, cell phones

Authentication: Role of Trusted Peripherals

- Extending the trust boundary creates a strong foundation for trusted interactions



Trusted Systems Eco System

wave

Trust Infrastructure

Life Cycle Management

- Trusted Applications
- Trusted Hardware

Trusted Services and Applications

Platform Security
Content Protection
User Authentication
Digital Signatures
Access Control
Premium Services
Dist. Transactions

Trusted Platforms, Tokens and Peripherals

TCPA EMBASSY LeGrande Palladium

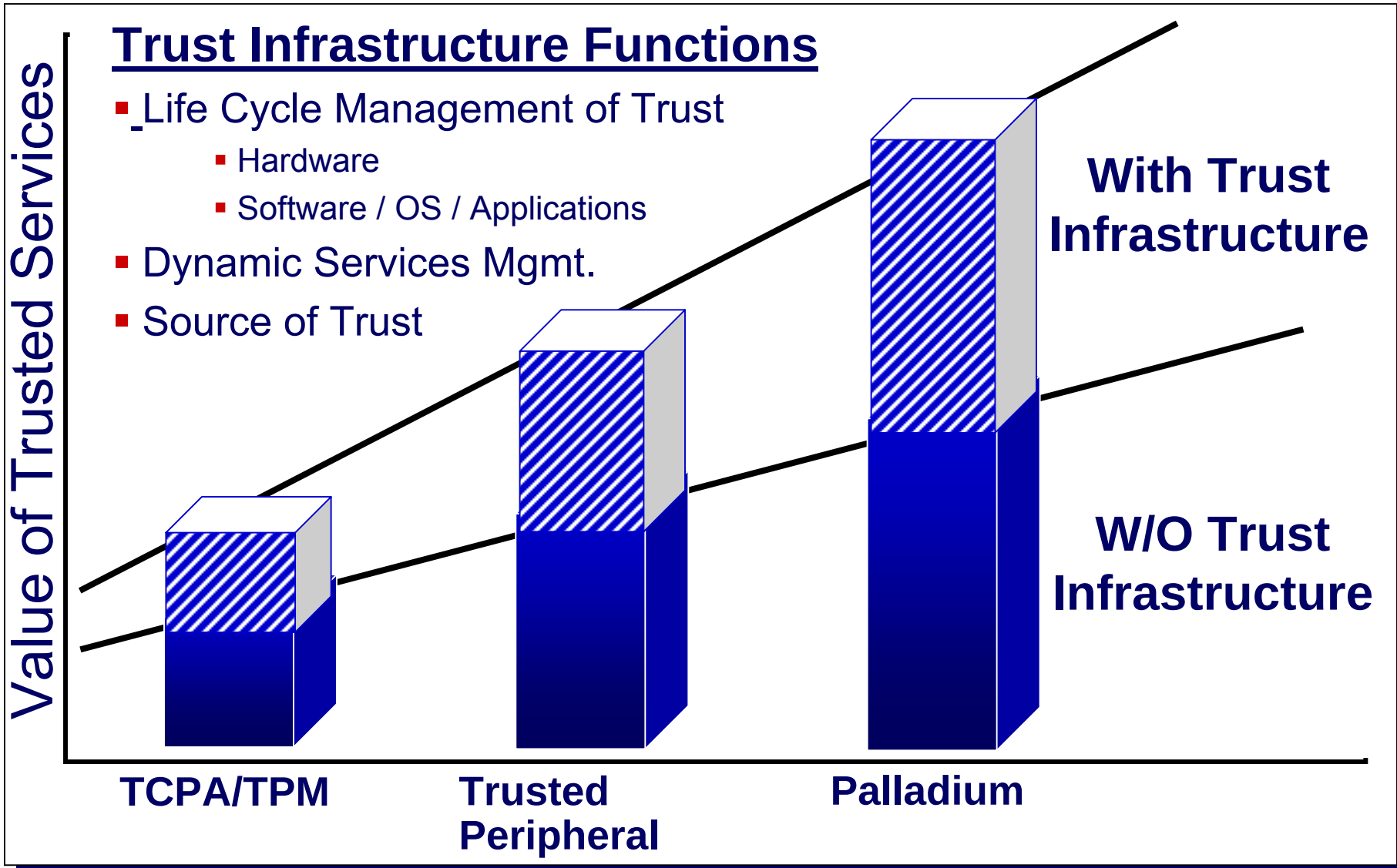
PC Motherboards
Keyboards
Smart Card Readers

Evolution of Trust Infrastructures

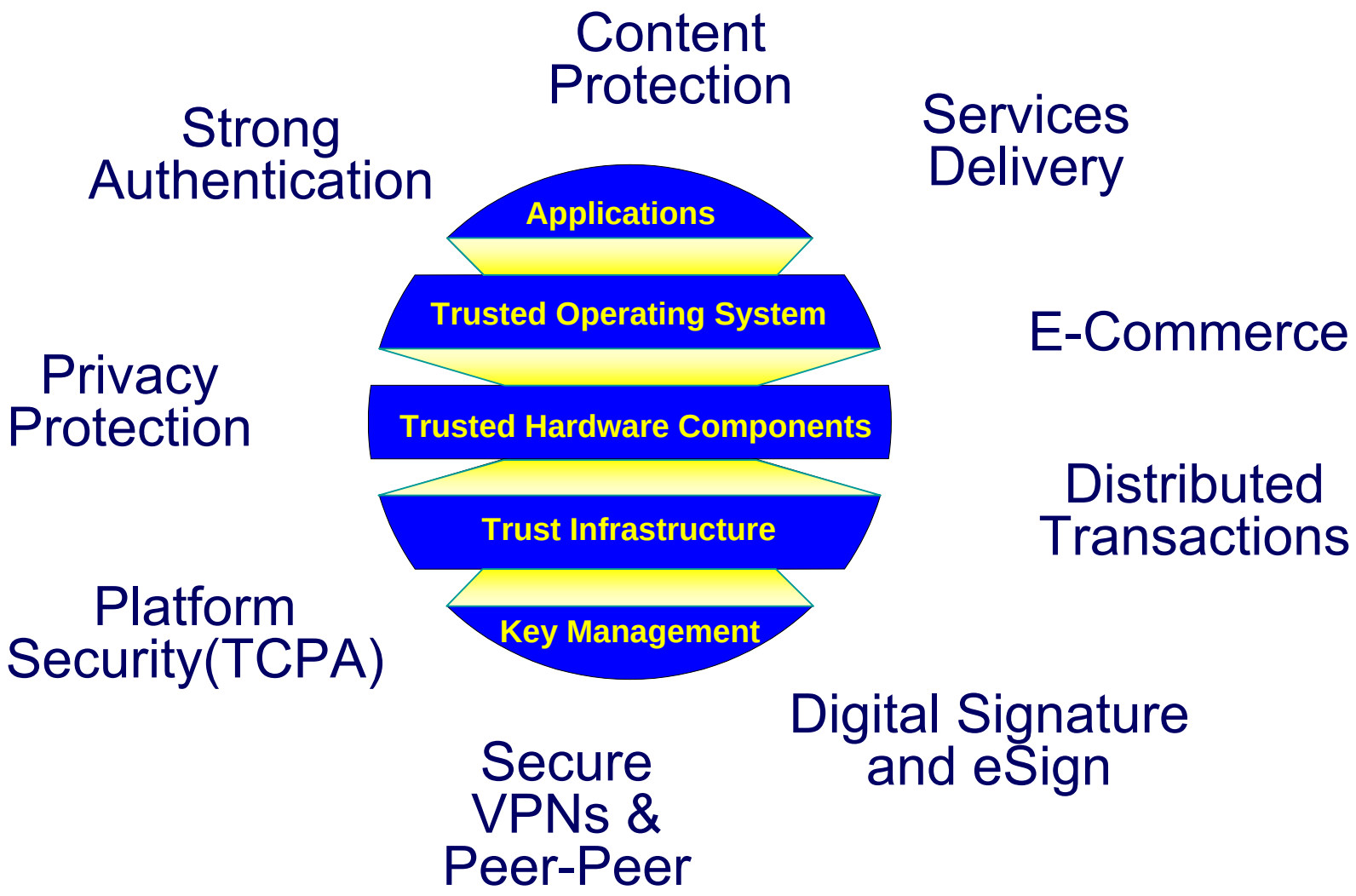
- Closed
- Centralized
- Dedicated
- Isolated
- Unmanaged
- Static

- Open
- Distributed
- Shared Multi-party
- Interconnected
- Managed
- Dynamic

Why Open, Multi-Party Trust?



Trusted Web Services



Summary

- Trusted Identity requires *trusted tokens and trusted peripherals*
  - Cards provide portability, rights, credentials
  - Readers provide expanded storage, processing, and secure I/O

- Trusted Computing initiatives are driving a new generation of *open trust infrastructures*
- End result: development and delivery of families of robust *trusted Web* services