GEMPLUS
beyond smart

NGSCB: new stakes for smartcards

Gemplus vision

Context

GEMPLUS
beyond smart

TCPA
TRUSTED COMPUTING PLATFORM ALLIANCE

- 1999: HP, Compaq, Microsoft, Intel, IBM
  - *Gemplus member*
- 2001: TPM Specification v1.1b publicly available
- 2003: 190+ members

TCG

- 2003: HP, AMD, Microsoft, Intel, IBM
  - *Gemplus member*
  - TPM Specification v1.2 under study

TPM

- Security hardware module for chain of trust
- Tamper-evident, cryptographic support (storage & reporting)
- Currently integrated to motherboard
- Close to smartcard design

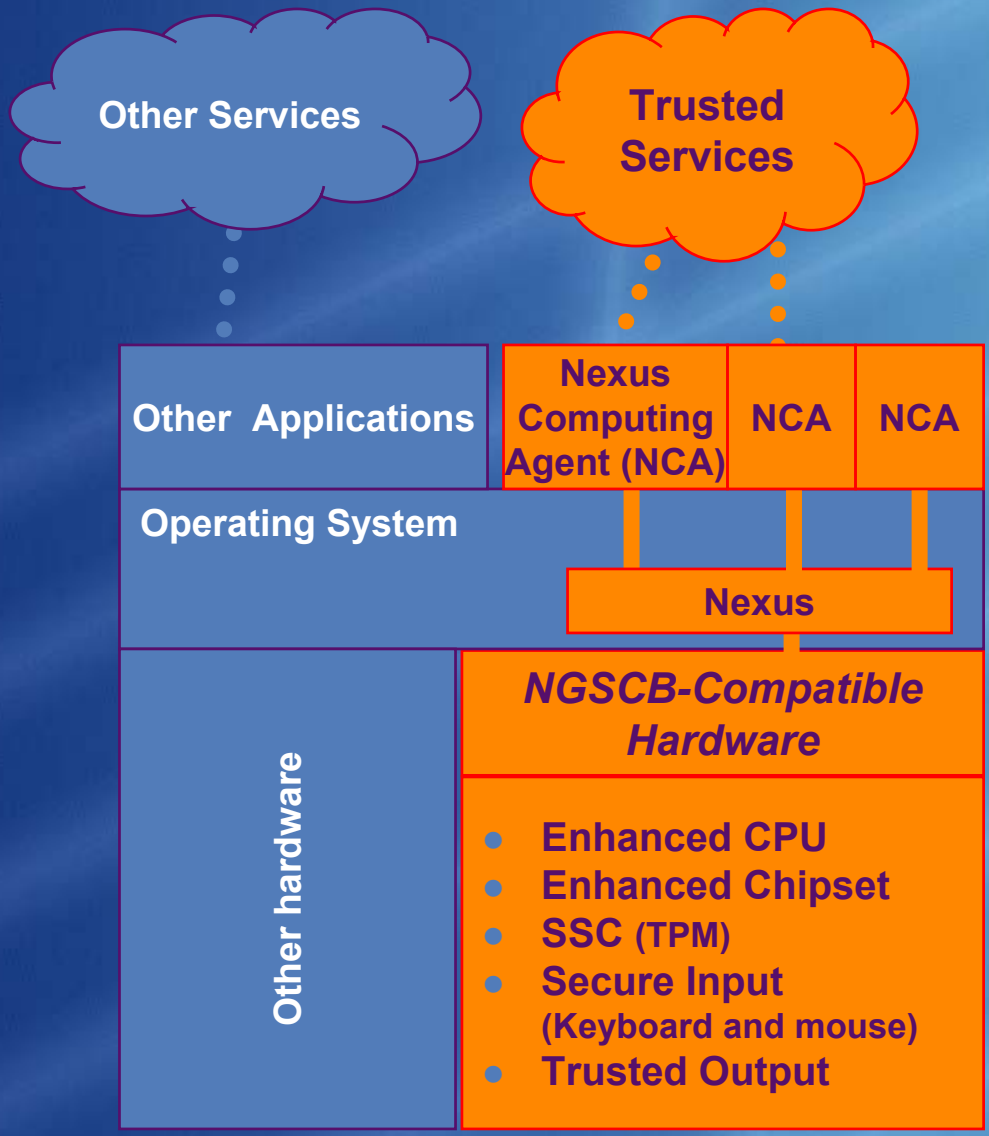
Technology Evolution

GEMPLUS
beyond smart

Consortium	**TCPA**	**TCG**	**Microsoft**
Product	TPM 1.1b	TPM 1.2	NGSCB 1.0 with TPM 1.2
Availability	Now	Q4 2003 - Q1 2004	Future version of Windows (Longhorn?) and when compatible HW : LT, …
Migration steps		• TPM 1.1b specification to TPM 1.2	• TSS applications will run on NGSCB hardware • TPM to be SSC. Role of SSC still unclear (Nexus PK functions vs SSC cryptographic support)

NGSCB principles

GEMPLUS
beyond smart



NGSCB-SC synergies…

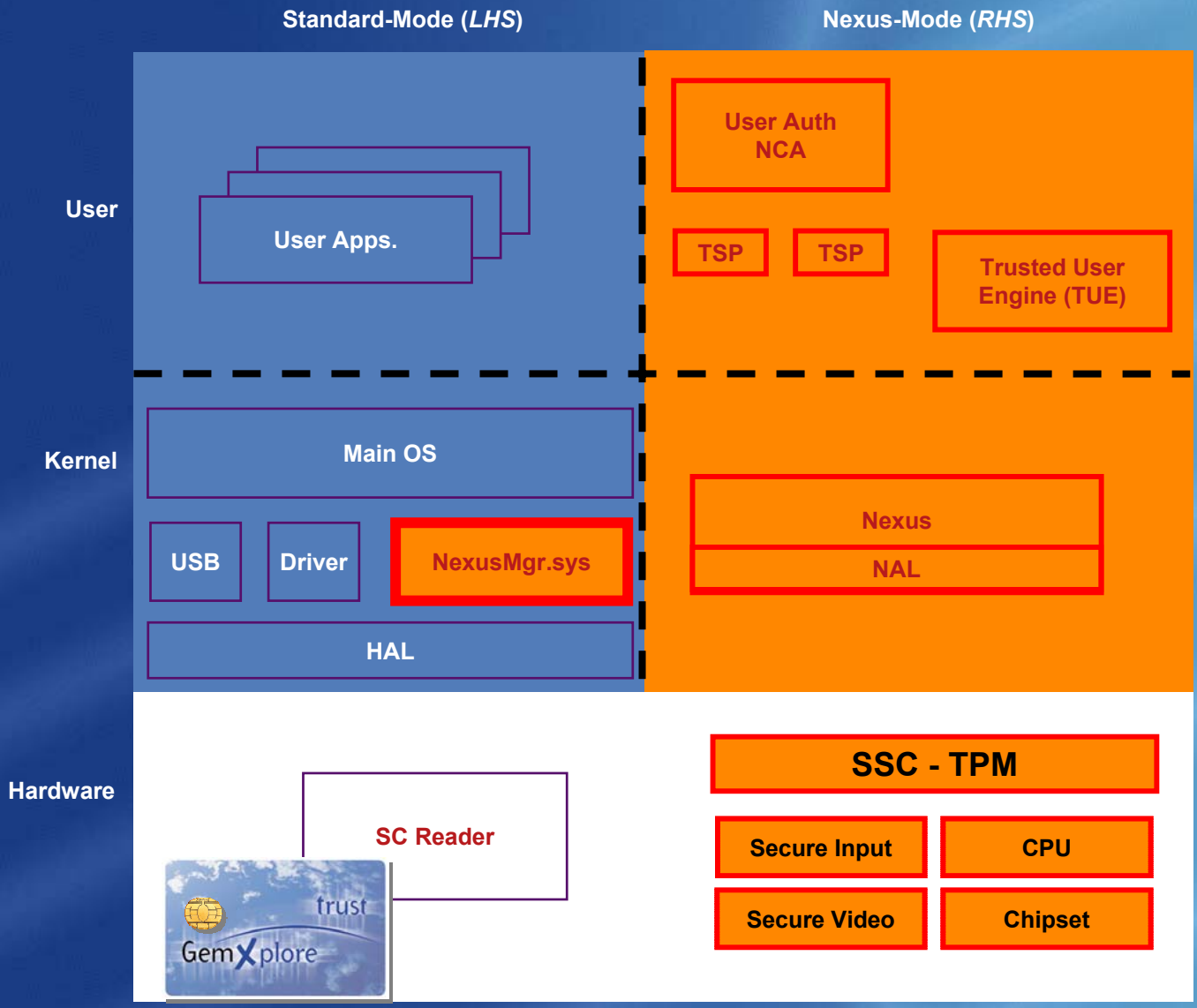
GEMPLUS
beyond smart

User-related applications or secrets

- Secrets
  - User authentication (password, biometrics…)
    - ➔ what you know
    - ➔ what you have
    - ➔ what you are
  - User credentials
  - User secret information (bank, e-business…)
- Applications
  - User clients (mail, browser, logon…)
  - File encryption
  - …

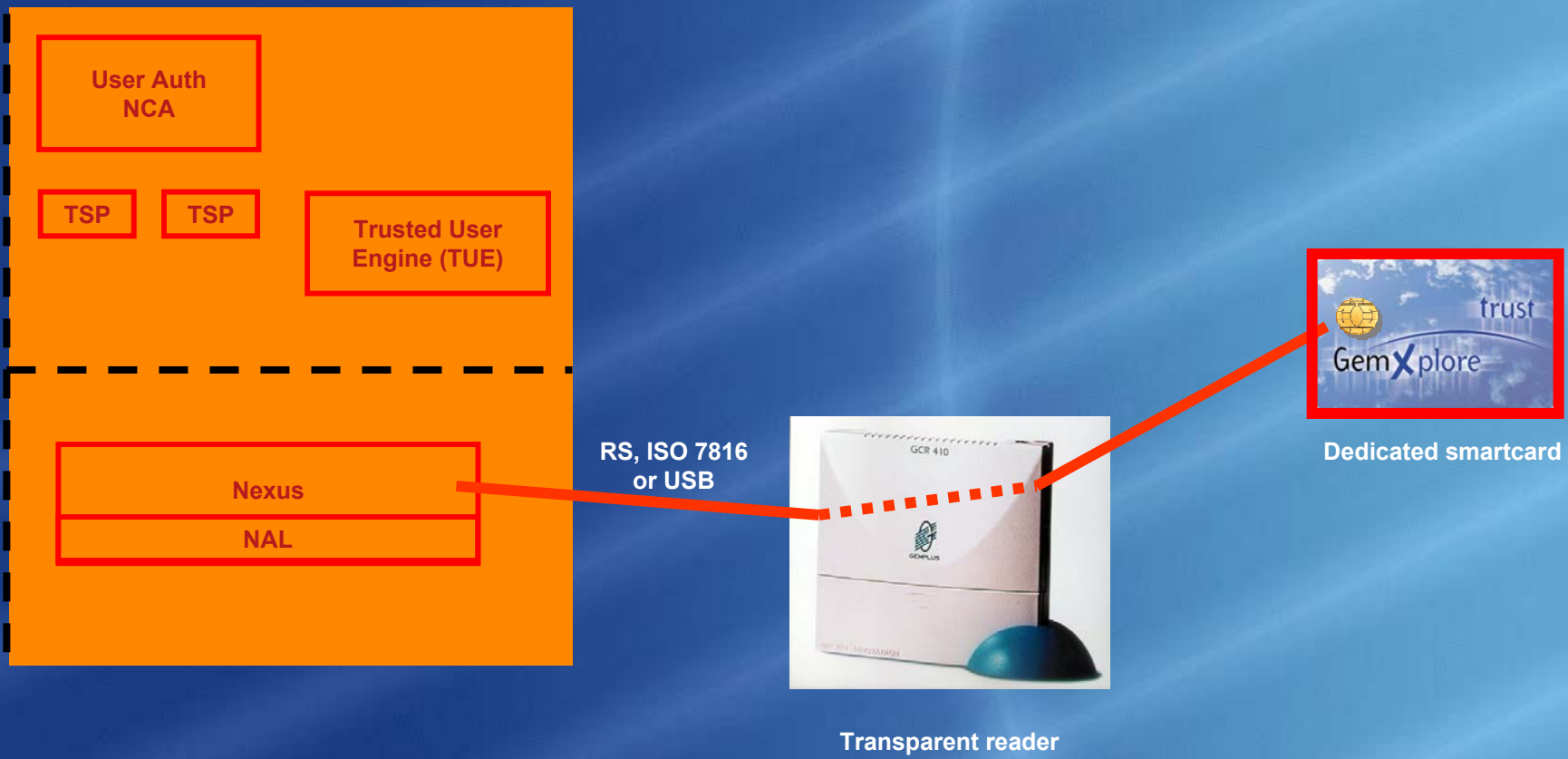
NGSCB extension

GEMPLUS beyond smart



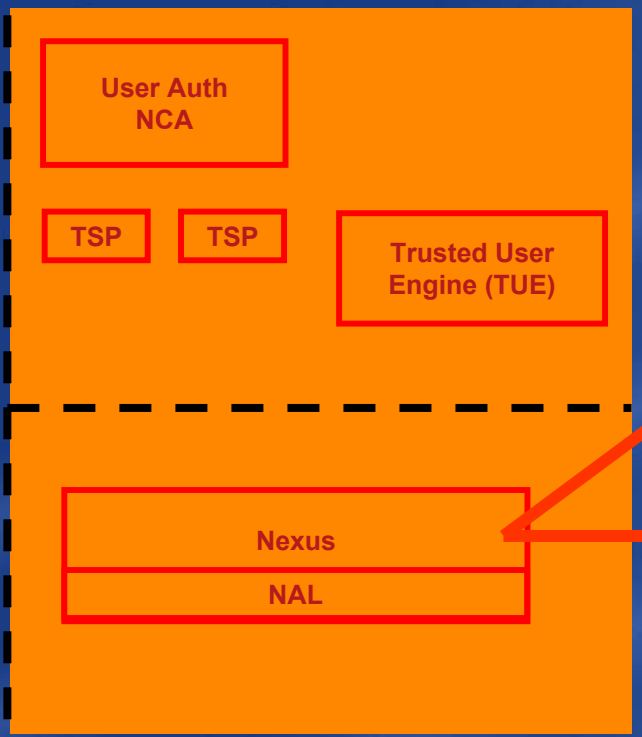
Focus on the reader

- Secure path Nexus-SC



Focus on the reader

- Secure path Nexus-Reader



RS or USB

Biometric reader

Intelligent reader

Multi-purposes
smartcards

Conclusion

GEMPLUS
beyond smart

- Bring new markets, modify current ones:
  - New bank transactions and protocols
  - Improved value for signatures schemes (regarding laws…), deployment of PKIs
- Multiple business points of view:
  - Users (privacy, ease of use, user-friendliness…)
  - IT professionals (corporate solutions, security…)
  - Content providers (DRM, billing…)

Smartcards are secure **and** personal: the perfect intermediate solution