

Trusted Computing Platform Alliance

An industry work group focused on enhancing trust and security on computer platforms



Industry Environment

- PC and network designed to be open and flexible
- Lack of trust in performing high-value e-business transactions on connected PCs
- Software security solutions are vulnerable

Security issues pose a significant barrier to the ubiquitous adoption of Internet-based e-Business applications (*source: IDC*)



T C P A
Trusted Computing Platform Alliance



TCPA Organization

- Open membership to companies developing security technology, products and services
- Structure
 - Members
 - 135+ member companies
 - Steering Committee consisting of Compaq, HP, IBM, Intel, Microsoft
 - Ad-hoc Workgroups
 - Technical, Marketing, Legal
 - Technical Workgroups
 - BIOS, PKI, Conformance



Trusted Computing Platform Alliance



Objectives

- **Develop an industry standard specification**
 - Providing a ubiquitous and standardized means to address trustworthiness of computing platforms
 - Improving the authenticity, integrity, and privacy of Internet-based communications and commerce
- **Promote the adoption of the TCPA Specification**
 - Affordable and interoperable
 - Exportable
 - Adaptable to work with existing standards and evolving solutions



T C P A
Trusted Computing Platform Alliance



TCPA Spec Adoption Benefits

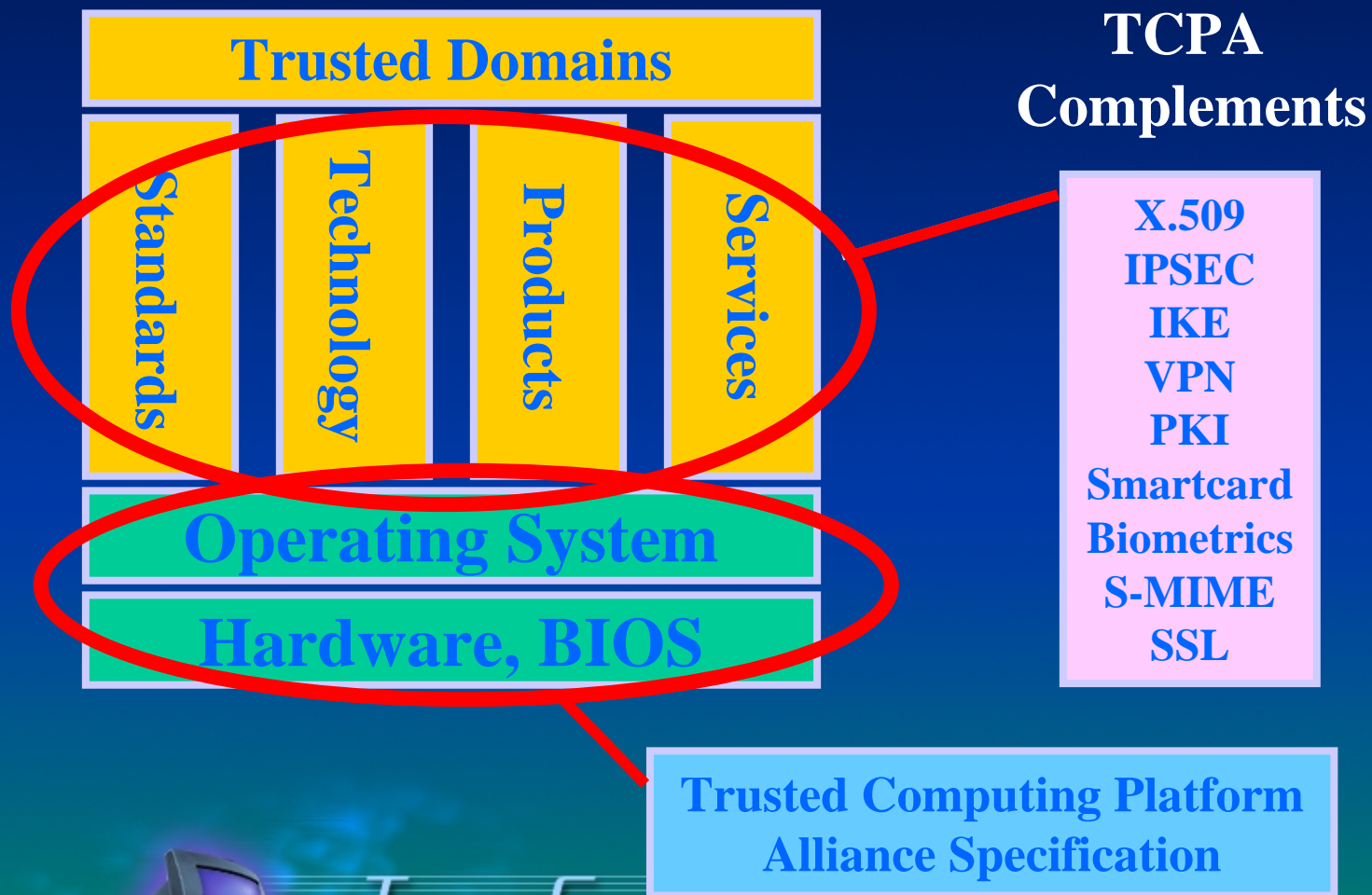
- PC is a trustworthy vehicle for e-Business
 - Retains existing openness and flexibility
 - H/W and S/W combined solution
- Improved fundamentals of computer authenticity, integrity and privacy
 - Authenticity: users are confident that they know to whom and to what entity they are talking
 - Integrity: assurance that information is transmitted accurately
 - Privacy: confidence that the privacy of information is respected
- Enhanced support for privacy of identity data



T C P A
Trusted Computing Platform Alliance



TCPA Specification Scope



TCPA
Trusted Computing Platform Alliance

TCPA Specification Overview

- **Baseline hardware capabilities**
 - Improved traditional security features
 - Persistent storage of confidential information
 - Platform authentication
 - Random number generator
 - New security capabilities
 - Anonymous/multiple identities
 - Integrity metrics
- **Exportable worldwide**
 - Excludes general purpose encryption
- **Owner has complete control of policy**
 - Opt in - Owner decides if and when to use capability



T C P A
Trusted Computing Platform Alliance



Example Applications

- Security applications can provide better security using trusted platforms
 - Public Key Infrastructure
 - Smart Card transactions
 - VPNs
- Applications that use security can be improved with trusted platforms
 - Web browsers use of SSL
 - E-mail use of S-MIME



T C P A
Trusted Computing Platform Alliance



Industry Call to Action

- **Vendors**
 - Drive TCPA-based solutions into your products
 - Help your customers understand how TCPA-based solutions improve your products
- **Customers**
 - Foresee the benefits of TCPA-enabled solutions in your environment
 - Drive your hardware and software vendors to produce TCPA-enabled products

