# LaGrande Technology & Safer Computing Overview

**Mike Ferron-Jones**
Desktop Security Technologies Marketing Manager

**Luke Girard**
Desktop Security Technologies Product Marketing Engineer

# Safer Computing Track – Fall IDF

## Tuesday

- LT Overview
  SCMS-16
- TCG & TPM v1.2
  SCMS-17
- LT Architecture
  SCMS-18
- Tech Showcase
  Every Day
  Birds of a Feather Lunches
  Tuesday & Wednesday

## Wednesday

- Privacy Method for Assuring Trust
  SCMS-19
- Opt-In Strategy
  SCMS-156
- Trusted Mobile KB Controller
  SCMS-24
- Software for LT
  SCMS-20
- Fundamentals of NGSCB
  SCMS-21
- Migrating Apps to NGSCB
  SCMS-22

## Thursday

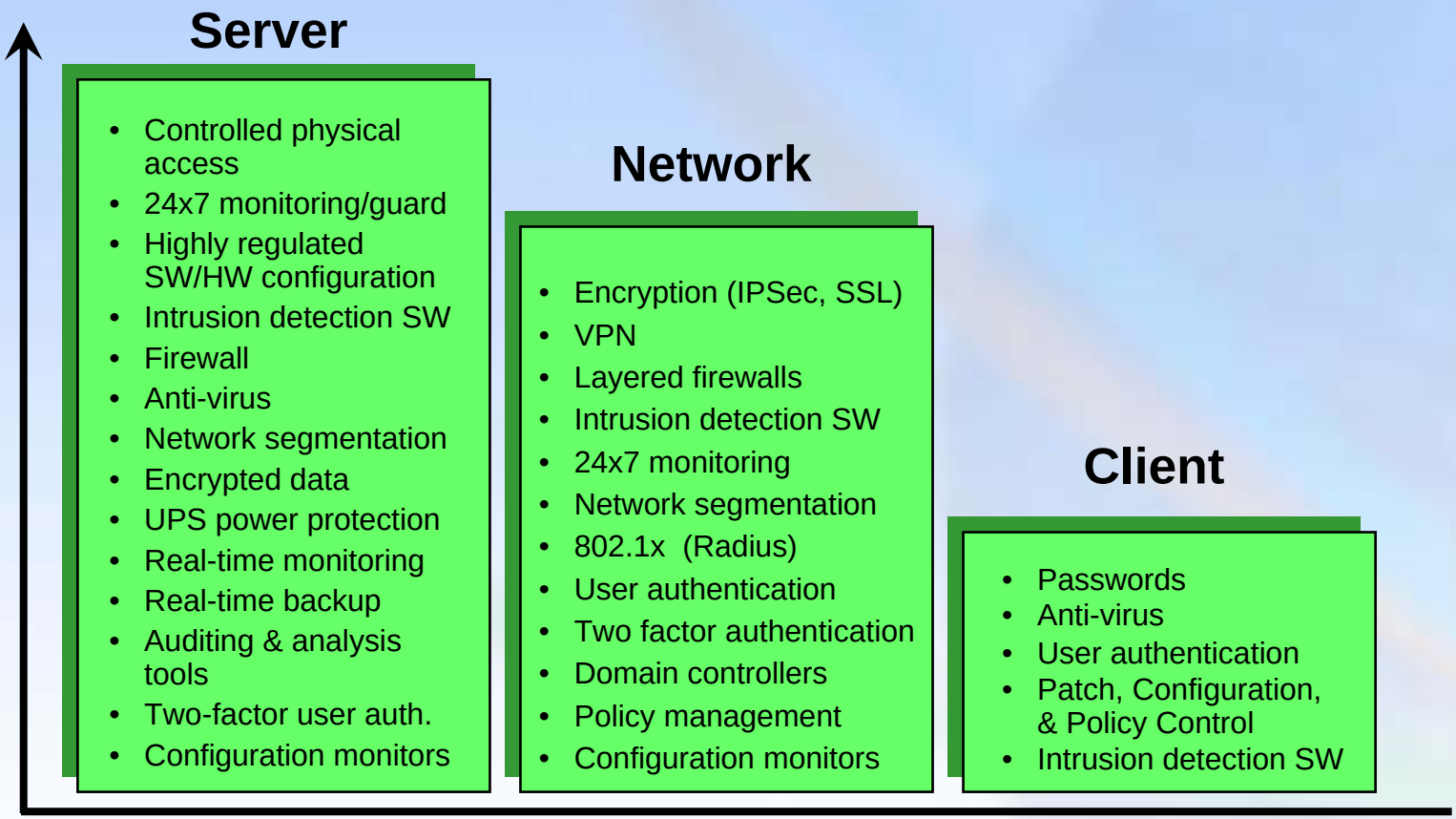
- TPM Recovery
  SCMS-25
- TCG Credentials
  SCMS-157
- TPM Mfg & Testing
  SCMS-180

= Overview
= Medium Technical
= Highly Technical

# Agenda:
## The Fundamentals of LaGrande Technology

- Security Environment & Opportunity
- LaGrande Technology Overview
- Market Segments & Usage Models
- User Choice & Control Policies
- Summary & Next Steps

# Today's Deployments Often Leave Clients Relatively Unprotected

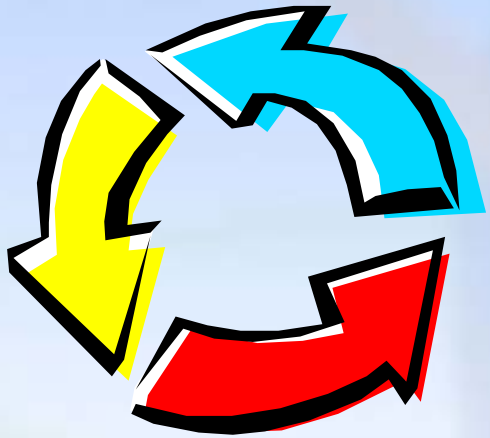



**Mismatch between security measures and the financial value of data created & stored on clients**

# The Security Opportunity

**Clients lightly protected relative to servers & network**

**High value data created & stored on client**



**Financial incentive & readily available means to attack clients**

**Ubiquitous connectivity (wired & wireless, local & remote)**

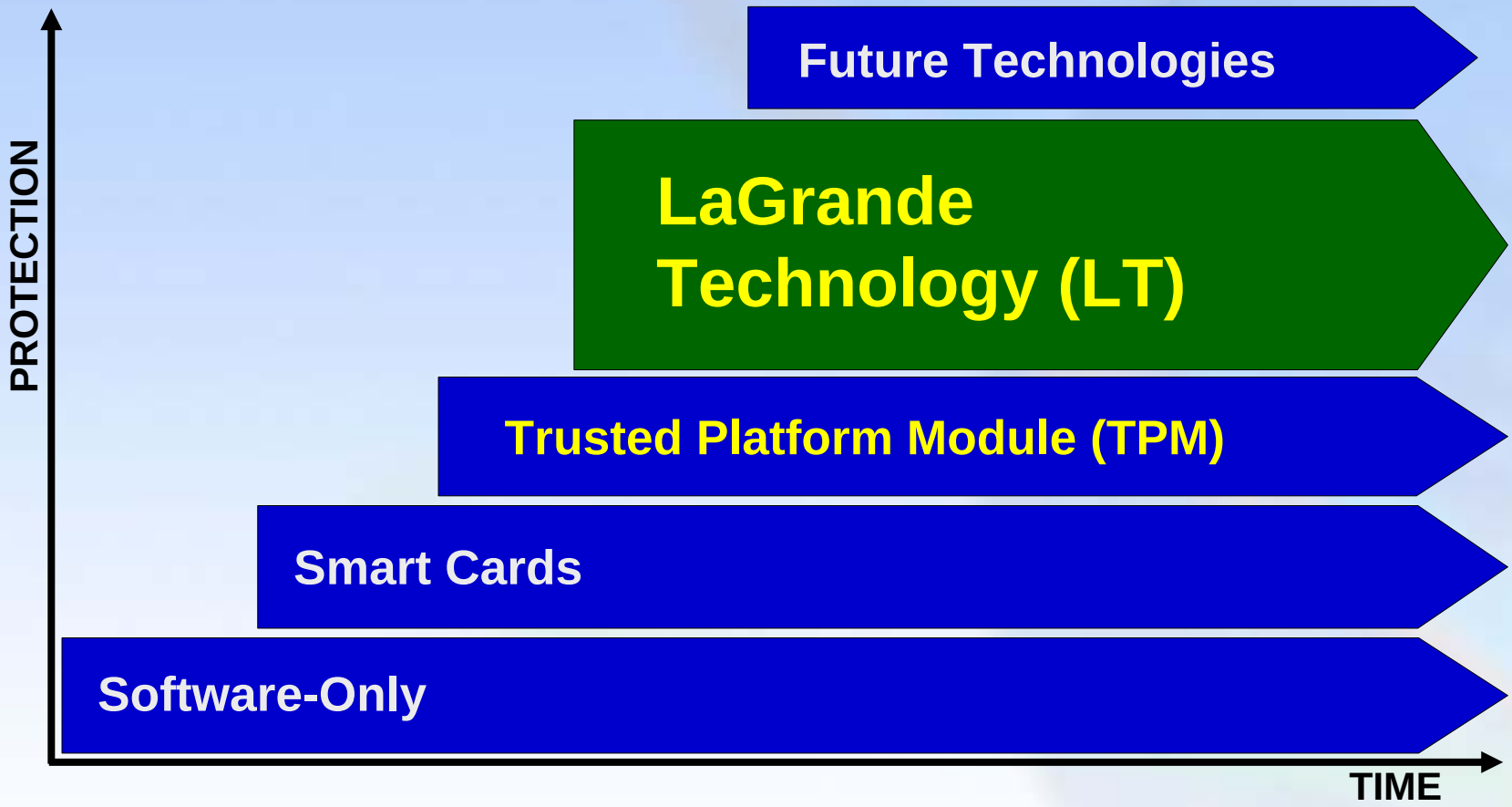
**Attacks outpacing today's protection models**

**Sophisticated attack tools readily available**

**A hardened client can reduce the risk of serious financial loss and compromised data**

# Safer Computing Initiative

## Advancing Client Platform Security




**Goal is to create a hardware framework for continued security innovation**

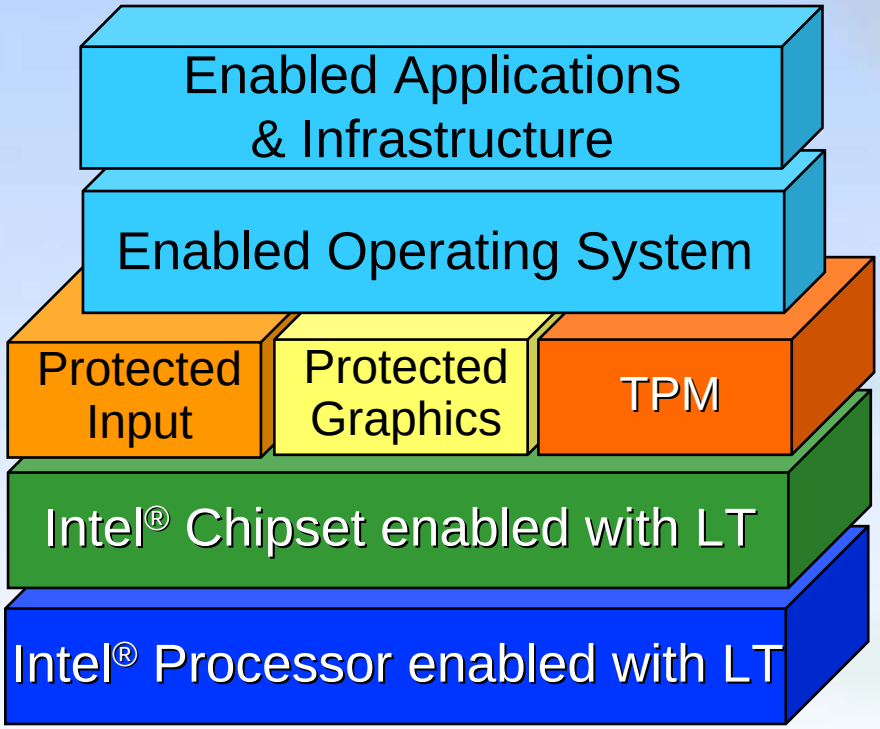
# LaGrande Technology Objectives

| | |
|---|---|
| **Protect:** | • Confidential corporate & personal data<br>• Sensitive communications<br>• E-commerce transactions |
| **From:** | • Attack software on the system<br>• Attack software on the network<br>• Inadvertent exposure due to compromised software |
| **Without compromising:** | • Ease of Use<br>• Manageability<br>• Privacy<br>• Performance<br>• Versatility<br>• Backwards compatibility |

**Greater data protection with the flexibility & productivity of PC computing**

# Summary of LT Capabilities

## Enhanced protection against software based attacks




- **Protected Execution**
- **Protected Memory Pages**
- **Sealed Storage (TPM)**
- **Protected Input (KB & Mouse)**
- **Protected Graphics**
- **Attestation**

**A versatile hardware foundation for operating systems and applications**

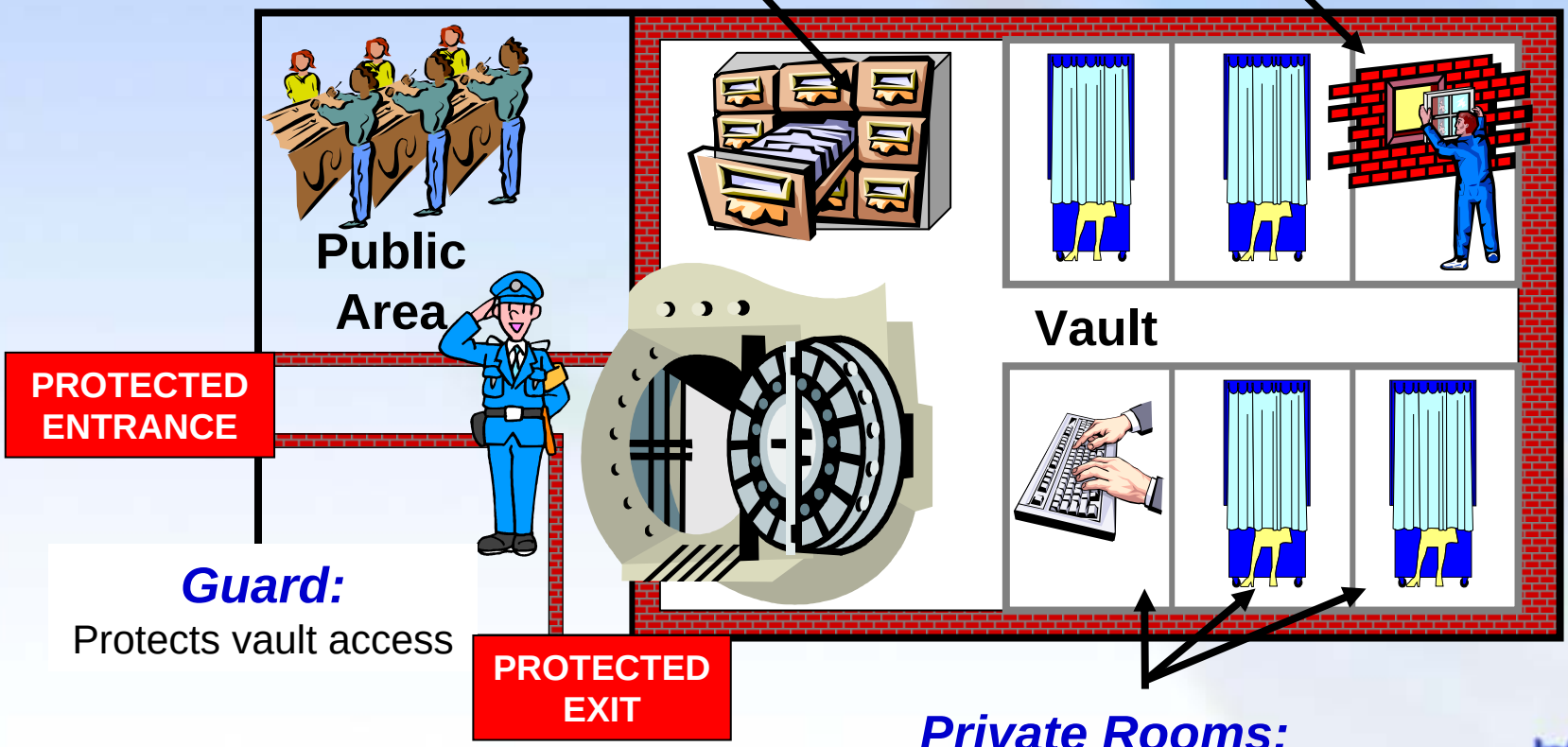
# An LT Metaphor – "The Bank Vault"

***Safe Deposit Boxes:***

Store & protect secrets

***One-Way, Protected Window:***

Display certain secure data w/o going through Public Area



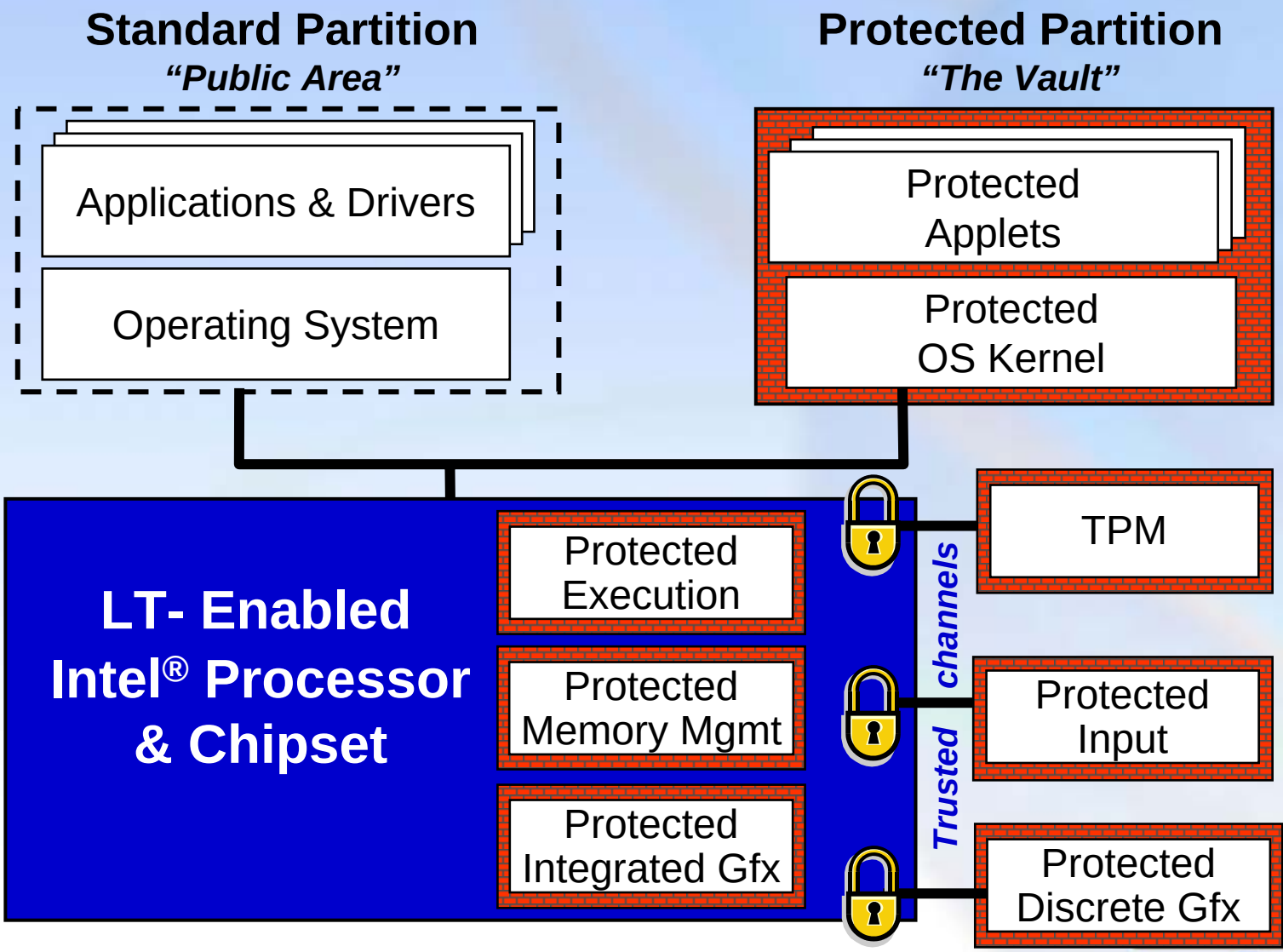

***Guard:***

Protects vault access

***Private Rooms:***

Input & process secrets out of others' view

# Protected LT Environment



# LT Platform Requirements & Status

| | |
|---|---|
| TPM v1.2 | See www.trustedcomputing group.com for latest specs |
| Protected Desktop KB & Mouse | Intel specs available now under NDA<br>Contact vendors for product specifics |
| Trusted Mobile Keyboard Controller | Intel specs available now under NDA<br>See course SCMS24 |
| BIOS | Intel specs available now under NDA |
| Discrete Graphics Solutions | Contact graphics vendors |
| Preliminary LT Platform Design Guide available Q4'03 under NDA | |

**Factor LT ingredients into future product & procurement plans**

* All dates are for planning purposes only and subject to change without notice

# LT Availability & Target Segments

- **Desktop & Mobile availability in next 2-3 years***
- **Focused on the Business Segment**
  - Places higher value on security
  - Greater experience with security methods and infrastructures
  - Demonstrated propensity to invest in security
- **Expected “fast adopters” in this segment**
  - Finance, Banking, Insurance, Government, and Health Care
  - Mission-critical and high-value applications
- **Consumer segment not a focus at launch**

* All dates are for planning purposes only and subject to change without notice

# Applying LT to Business Security

## Some Usage Examples

### Network Access Control

- Hardened VPN
- Credential & identity mgmt
- Strengthened platform & user authentication
- IT policy compliance checking

### Protected Transactions

- Protected input, authorization and signature processes

### Protect User & Company Data

- Enhanced file access mgmt
- End-to-end encrypted mail
- Protected document viewer

### Malicious Software Protection

- Protect virus scanner & signatures
- Harden intrusion detection software

**LT can strengthen existing security measures and enable new usages**

# Intel's LT Policy

- **LT and associated usages touch on areas of significant public interest**
- **Intent of Intel's LT policies**
  - Guide internal product development
  - Provide recommendations to fellow travelers
  - Promote responsible deployment and best known methods
  - Help users make informed decisions

**Focus on Choice, Control & Privacy**

# Summary of LT Owner/User Choice & Control Policy

- **Choice and Control**
  - Straightforward mechanism for ensuring choice & control
  - Opt-in model
- **Visibility**
  - Clear visibility into state of the LT hardware and software
- **Privacy Protection**
  - Privacy protection mechanisms must be made available
  - Any Personally Identifiable Information must be under its owner's control

**Draft policy white paper available now for review and comment at intel.com/developer**

# Summary

- LT is a versatile set of hardware enhancements to Intel processors, chipsets, and platforms
- LT creates a hardware foundation that helps protect data from software-based attacks
- LT is expected in Desktop & Mobile platforms for the Business segment in the next 2-3 years
- Intel is committed to user control & privacy

# Next Steps

**Hardware Developers & OEMs**

- Factor LT into Business platform planning
- OEMs contact component vendors for specific product plans
- Contact your Intel representatives for available specifications & schedules

---

**Software Developers**

- Factor LT into Business software planning
- Contact your Intel representatives for information on Intel Early Access Program

---

**IT**

- Factor LT into enterprise security strategy and infrastructure planning
- Communicate needs for LT to your PC vendors

# Thank you for attending.

# Please fill out the Session Evaluation Form.

# Acronyms/Definitions

| Acronym | Description |
|---|---|
| Attestation | American Heritage Dictionary: To affirm to be correct, true, or genuine. In the LT sense, a cryptographic reporting mechanism that provides assurance of the current protected environment. |
| LT | Intel® LaGrande Technology. Features added to Intel CPU and Chipsets when used in conjunction with other platform components, provides hardware based security support for the platform. |
| Platform Authentication | By using a hardware signing engine, and hardware protected keys to sign a challenge, A TPM can give a spoof resistant proof that a platform responding to a challenge is the one that was originally registered. |
| TMKBC | Trusted Mobile Keyboard Controller: A keyboard controller with changes made to it that allow a “trusted channel” to the keyboard while in a mode that supports LT. |
| TPM | Trusted Platform Module as defined by the Trusted Computing Group (TCG) www.trustedcomputinggroup.org |
| Trusted Channel | A means by which two trusted sub-systems can communicate with each other at a confidence level that meets the expected security policy (attack mitigation, data protection, key exchange, strength of function, etc.). |