LaGrande Technology Policy on Owner/User Choice and Control

Draft for Industry Comment

(Rev 0.8, September 2003)

Purpose of this Policy Statement

Intel's LaGrande Technology (LT) is the code-name for a set of hardware components designed to enhance the security capabilities of the PC. Expected to launch in the next two to three years, LT will provide a hardware-based security foundation that will help enable greater levels of protection for information stored, processed and exchanged on the PC. For the PC industry, LT creates a new value category in addition to traditional performance improvements. LT, and the associated software and usage models, have implications in areas where there is significant public interest, including personal choice and privacy.

Intel believes that a clear, unambiguous statement of policy is very important as the industry embarks on a path toward greater PC security. These policies should provide guidance for responsible product development, help define use models that rely on LT capabilities, and help buyers make more informed purchase decisions. To achieve these ends, this draft policy statement describes Intel's initial position regarding choice, privacy and visibility into LT platform operations. Intel seeks feedback on this draft statement from customers, industry experts, government bodies, concerned individuals and public interest groups.

These policies are written to comprehend both the owner and user of the system. For consumers or small businesses, the owner and user may be the same person. In other cases, such as a corporate environment, the owner and user are not the same person. We use an "owner/user" terminology convention in cases where control may be delegated or balanced between owners and users based on company policies or local laws. "Owner" and "user" are used when the policy applies specifically to that party. The intended role of these policies is one of guidance, and they are not proposed to supplant any existing local laws or regulations.

LaGrande Technology Summary

Designed to help protect against software-based attacks, LT integrates new security features and capabilities into the processor, chipset and other platform components. When coupled with an enabled operating system and applications, LT helps protect data confidentiality and integrity in the face of an increasingly hostile security environment. It provides a general-purpose safer computing environment capable of running a wide variety of operating systems and applications. Intel is initially targeting LT for applications in the business segment.

LT's capabilities include:

- **Protected execution and memory spaces** where sensitive data can be processed out of view of any other software
- **Sealed storage** shields encryption keys and other data from attack while in user or stored.
- **Protected input** shields keystrokes and mouse clicks from interception and theft.
- **Protected graphics** creates output windows that cannot be intercepted, copied or "spoofed" by software.
- **Attestation** enables a system to provide assurance that it has correctly invoked the protected LT environment, as well as a measure of the software running in the protected space. The information exchanged during an attestation function is called an Attestation Identity Key credential and is used to help establish mutual trust between parties.

Choice and Control

Policy Statement #1: "LT based platforms must have a straightforward mechanism for ensuring choice in controlling the LT operation."

PC owner must have a choice whether they want to "opt-in" to LT protections and, to the degree feasible, maintain control over the various functions.

The Choice and Control policy must be implemented in a manner similar to the following:

- Unless the owner explicitly requests the capability "on" at the time of purchase, the capability must be "off." For example, if a large IT organization wants to purchase a fleet of LT-enabled systems but does not want to manually activate LT on each machine, they may choose to instruct their system supplier to configure them with LT "on."

- Feature control must be straightforward and must only be turned on or off with owner knowledge and consent. For example, LT systems must be built so that LT state cannot be changed by software without owner consent. A physical presence requirement is one way to affect this.

- Owner must have the choice to not use the attestation function (opt-out), yet still achieve the benefits of the non-attestation capabilities of the LT platform, such as enhanced file encryption. In addition, the owner/user should be free to choose to opt-out of attestation on a per transaction basis while not being required to completely shut off the feature.

- The system's attestation identity keys (AIK), which provide a measurement of the LT state and protected software configuration, must be under the owner's or user's control, depending on which party created the AIK. The owner or user must have the ability to delete AIKs they created and no longer wish to use.

Visibility

Policy Statement #2: Users of the system must have clear visibility into the operational state of the LT hardware and LT enabled software.

The Visibility policy is intended to provide system users with easy access to information about the state of their LT hardware and the software that is running in the protected areas.

The Visibility policy must be implemented in a manner similar to the following:

- Users must be provided with an interface that prominently and reliably identifies the current functional state of the LT hardware. Implementation could take the form of a message at boot time, an icon or status indicator, a system LED or other means.

- Users must be provided with an interface that prominently and reliably identifies the current functional state of the protected operating system kernel and any protected applications it has running.

- Users must have full visibility into information communicated over the network as part of attestation. This requires visibility into AIK credentials and associated integrity metrics.

Privacy Protection

Policy Statement #3: On the LT platform, privacy protection mechanisms must be made available and must not be associated with any Personally Identifiable Information.

Intel's objective with LT platforms and solutions is to deliver higher levels of security while continuing to respect privacy.

The Privacy Protection policy must be implemented in a manner similar to the following:

- Any unique keys and credentials required for the LT platform must be protected and used in a privacy-preserving manner. The platform's endorsement key (EK) must be protected and used only for creation of alias keys, such as AIKs. Owners and users must have complete control over unique keys they created.

- Personally identifiable information (PII) must be used only when necessary to complete a transaction, and must be included within an AIK credential and attestation only if necessary to complete a transaction. If PII is required, the user must be informed as to what, why and how it will be used and be afforded visibility into PII included with any AIK credential.

- PII must only be included in an AIK credential when the owner of the information provides specific informed consent. This is an opt-in model. In addition, PII owners must have the ability to delete any AIK credential that contains their PII.

LaGrande Technology Policy Implementation

Intel will adhere to these policies in the development and deployment of its own LT products. At the same time, we recognize that many aspects of successful policy implementation depend on software and hardware development from third party providers whose implementations are outside Intel's direct control. Intel believes adherence to these or equivalent policies is critical to delivering the full benefits of LT and complementary security technologies, and will vigorously encourage our fellow travelers in the industry to internalize and implement these policies.

Feedback

Intel requests that our customers, fellow travelers in the industry, interested individuals and groups provide feedback on this draft of the LaGrande Technology Owner/User Choice and Control policies. Please e-mail your comments to **LT.policy.feedback@intel.com** until December 31, 2003. Although we cannot respond directly to every message, all feedback will be read and considered during the evolution of these policies. Thank you for your interest and participation in this important process.

For more information on LaGrande Technology, visit www.intel.com/developer.

0903/MF/AY
Part number: 253787-001