
e-Diagnostics Security Requirements

Anant Raman, Intel

anant.raman@intel.com, 480.554.1538

July 20, 2001

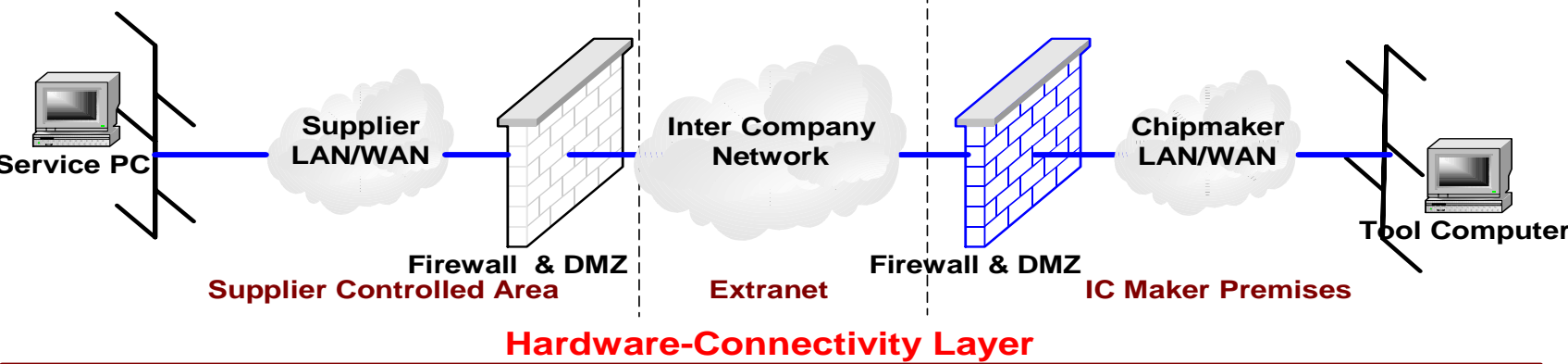
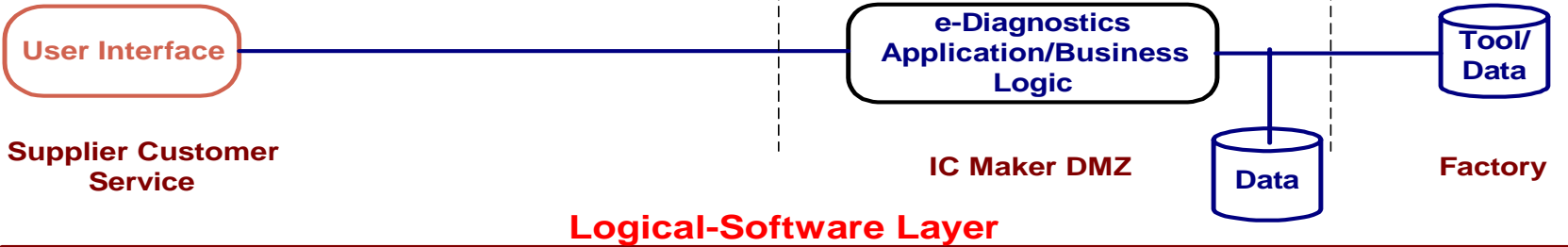
Agenda

- **e-Diagnostics Security Architecture (2 minutes)**
- **Business requirements (5 minutes)**
- **System Requirements (5 minutes)**
- **Summary (3 minutes)**

e-Diagnostics Security Architecture

- **e-Diagnostics has three components**
 - **Hardware-Connectivity Layer:** includes computers and networks to provide end-to-end secure connection between remote support personnel and equipment located at IC Makers.
 - **Software-Logical Layer:** includes the security elements of remote support applications and handling of related data.
 - **Business Layer:** includes the secure practice of remote support with activities such as troubleshooting, installation, configuration, & data analysis.

e-Diagnostics Security Architecture



Business Requirements

- **Supplier Responsibilities:**
 - **Identifying with currency, of remote support personnel**
 - **Company employees, third-parties, other OEMs.**
 - **Security of the credentials of the remote support**
 - **Authentication elements, remote access connections for telecommuting & traveling employees**
 - **Security of IC Maker data in supplier premises**
 - **Security of supplier-end of the e-Diagnostics connection**
 - **Appropriate external and internal protections**
 - **Provision of addresses for the customer service networks**

Business Requirements

- **Chipmaker Responsibilities:**

- **Providing identification for remote support personnel.**
 - Username/password, hardware/software tokens, digital certificates, etc.
- **Authentication of remote support personnel.**
- **Authorization of remote support personnel.**
 - Role based versus policy based
- **Access Control – user access based on role and data classification levels**
- **Administration of the e-Diagnostics system.**
- **Security of supplier data at IC maker premises.**

e-Diagnostics System Requirements

- **Security Requirements:**
 - **Identification** – across all suppliers
 - **Authentication** – for e-Diagnostics
 - **Authorization** – for task at hand
 - **Confidentiality & Integrity** – for data & system
 - **Non-repudiation** – taking ownership
 - **Administration** – total cost of ownership
 - **Logging** – for system management

e-Diagnostics System Requirements

- **Firewall requirements**
 - **Packet Filtering** – Hardware-Connectivity Layer.
 - **Application Proxy** – Software-Logical Layer.
 - **Transparency** – Hardware-Connectivity Layer.
 - By default turned off
 - Turned on for very limited cases (business driven)
 - **Perimeter Security** – support against DoS, etc.
- **Inter Company Network Connection**
 - **Public versus private** – ubiquity, performance, security, cost
- **System Requirements**
 - **Availability** – leads to redundancy, fault-tolerance, etc.
 - **Performance** – throughput, number of concurrent users.

Summary

- **System requirements need to match business requirements closely for overall security**
- **System requirements will need synergy between Hardware-Connectivity & Software-Logical Layers**
- **Business process bound by contracts**