

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

**VALTRUS INNOVATIONS LTD. and
KEY PATENT INNOVATIONS LTD.,**

Plaintiffs,

v.

SAP AMERICA, INC. and SAP SE,

Defendants.

Civil Action No. 2:24-cv-21

JURY TRIAL DEMANDED

**APPENDIX 3 TO EXPERT REPORT OF NICK FEAMSTER, PH.D.:
DETAILED ANALYSIS OF THE INVALIDITY OF THE '738 PATENT**

TABLE OF CONTENTS

I.	INVALIDATING PRIOR ART FOR THE '738 PATENT	1
A.	State of the Art	1
1.	According to the '738 Patent and Contemporary References.....	2
2.	Scope and Content of Prior Art.....	13
3.	OSI Models / Layers.	25
II.	INVALIDITY GROUNDS FOR THE '738 PATENT.....	28
A.	GROUND 1: Claims 1, 2, 3, 5, 10 and 33 Are Anticipated or Rendered Obvious Based on Akita and the Knowledge of a POSITA.....	28
1.	Akita is Analogous Art to the '738 Patent.	28
2.	Akita Anticipates, or in Combination with Knowledge of a POSITA, Invalidates the Asserted Claims of the '738 Patent.	28
B.	GROUND 2: Claims 1, 2, 3, 5, 10 and 33 Are Anticipated or Rendered Obvious Based on Kaler and the Knowledge of a POSITA.....	42
1.	Kaler is Analogous Art to the '738 Patent.	42
2.	Kaler, in Combination with Knowledge of a POSITA, Invalidates the Asserted Claims of the '738 Patent.....	43
C.	GROUND 3: Claims 1, 2, 3, 5, 10 and 33 Are Anticipated or Rendered Obvious Based on Sun and the Knowledge of a POSITA and/or Kaler.	58
1.	Sun is Analogous Art to the '738 Patent.....	58
2.	Kaler is Analogous Art to the '738 Patent.	58
3.	Motivation to Combine Sun and Kaler.	59
4.	Sun, in Combination with Kaler and Knowledge of a POSITA, Invalidates the Asserted Claims of the '738 Patent.....	60
III.	THE ASSERTED CLAIMS OF THE '738 PATENT ARE INVALID UNDER 35 U.S.C. § 101.....	76

I. INVALIDATING PRIOR ART FOR THE '738 PATENT

1. In addition to the opinions stated in my Expert Report regarding invalidity of certain claims, which I incorporate herein by reference, this Appendix includes additional detailed opinions regarding the '738 Patent.

2. Some of the terms used in the claims may have specific meanings and be understood to mean something different in the context of database systems and fault tolerant systems. But to the extent that certain functionality is accused of infringement based on the use of the same or similar word that is used in a claim term, that functionality existed well before the applicant filed the application for the alleged invention in the '738 Patent.

3. I understand that SAP served invalidity contentions in this case on May 20, 2024 (the "Invalidity Contentions"). While SAP's Invalidity Contentions refer to many items of prior art, this report addresses a subset of the prior art, namely:

- U.S. Patent No. 6,775,239, "Checking communication-path data in MPLS communication scheme," ("Akita")
- U.S. Patent Application Publication No. 2004/0139322, "Establishing a secure context at an electronic communications end-point," ("Kaler")
- Java™ Message Service, Sun Microsystems, Inc., Mark Hapner, et al. (April 12, 2002) ("Sun")

A. State of the Art

4. This Section summarizes some basic facts about each prior art reference included in my analysis below. This summary is not exhaustive and additional pertinent details about each reference are discussed in greater detail in later sections.

2. Scope and Content of Prior Art

a. Scope and Content of U.S. Patent No. 6,775,239 to Akita (Akita)

35. U.S. Patent No. 6,775,239 titled “Checking communication-path data in MPLS communication scheme” was filed on July 26, 2000 and issued on August 10, 2004. It is my opinion that Akita discloses and/or renders obvious each of the limitations of the Asserted claims, as discussed in greater detail below.

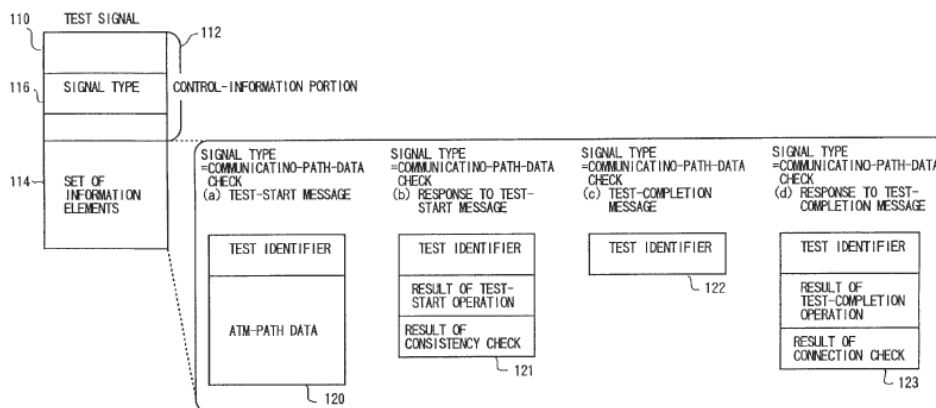
36. As can be seen in the abstract, reproduced below, Akita discusses the various modes of the communication system.

A method of checking communication-path data in a System, in which a router connecting first and Second networks operating on different protocols is connected to a Switch of the Second network, includes the Steps of changing the router and the Switch from a normal mode to a test mode, checking consistency between router communication-path data controlled by the router and Switch communication-path data controlled by the switch by sending the router communication-path data to the Switch during the test mode, and checking communication between the router and the Switch by sending cells from the router to the Switch and returning the cells from the Switch to the router during the test mode.

Akita, Abstract

37. Akita illustrates below, that in test mode, a context information related to the outgoing message, signal type, persists through all communications:

FIG. 5



Akita, Figure 5

38. Additionally, the Akita describes the indication of context information and obtaining context information at two different units, which could correspond to different layers of the protocol stack:

At a step S24, the Switch-side-check-control unit 140, when capturing resources for test control that correspond to the test identifier, keeps the ATM-path data, and, then, Sends an output request to the maintenance-message-output unit 94 to output the test-start message. The maintenance-message output unit 94 notifies the administrator at the ATM-Switch maintenance terminal 72 that a test is going to be conducted. At a step S26, the maintenance-message-output unit 94 Sends a response to the output request to the Switch-Side check-control unit 140.

Akita, 6:66-7:8

After reception monitoring begins, at a step S36, the Switch-side-check-control unit 140 requests the Switch-side Signal-control unit 141 to transmit a response to the test-start request based on results of test-start operation and the results of ATM-path-data-consistency check. At a step S38, based on the results of test-start operation and the results of ATM-path-data-consistency check, the Switch-Side-signal control unit 141 generates the test signal 150 having a set of information elements 156 as shown in FIG. 8, and transmits the test signal 150 from the ATM switch 90 to the MPLS router 80.

Akita, 7:23-33.

39. As discussed in greater detail below, Akita describes a method where context information is selectively added to outgoing messages. The context information is obtained in a different layer and is stored in a separate field of the message. As different messages pass between nodes of the communication system, the same context information is in the header of each message.

b. Scope and Content of U.S. Patent No. U.S. Patent Publication US 2004/0139322 to Kaler (Kaler)

40. U.S. Patent Publication US 2004/0139322 titled “Establishing a secure context at an electronic communications end-point” was filed on January 10, 2003 and published on July 15,

2004. It is my opinion that Kaler discloses and/or renders obvious each of the limitations of the Asserted Claims, as discussed in greater detail below.

41. As can be seen from the abstract, reproduced below, Kaler discusses the use of context information to establish a secure context between two nodes in a communication network.

A first application layer at a first message processor identifies a first portion of context information. A second message processor receives the first portion of context information. A second application layer at the second message processor identifies a second portion of context information. The second message processor sends the second portion of context information along with a first digital signature created from both the first and second portions of context information. The first message processor receives the second portion of context information and first digital signature. The first message processor sends a second digital signature created from the first and second portions of context information to the second message processor. If both the first and second digital signatures are authenticated, a secure context can be established between the first and second application layers.

Kaler, Abstract

42. Kaler discloses that this secure context is established between two applications on a separate nodes:

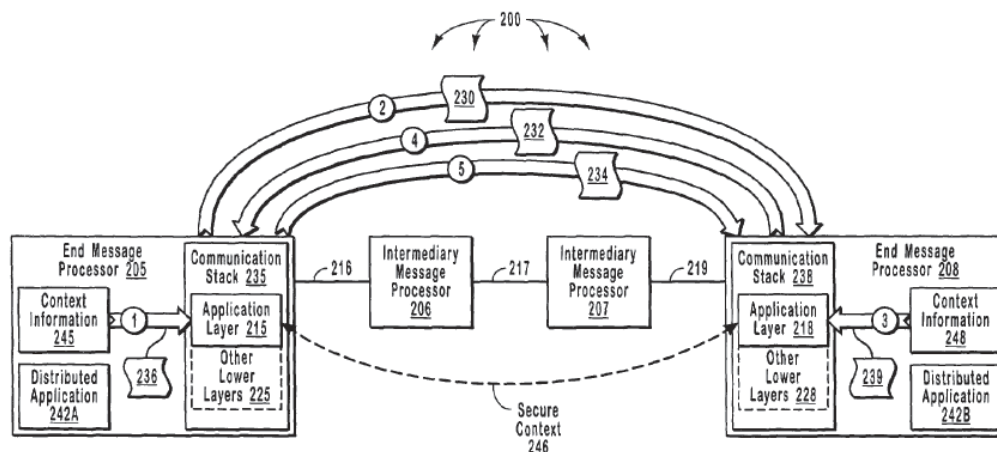


FIG. 2

Kaler, Figure 2

43. Kaler notes that the communication stack (protocol stack) utilized in the end message processors (nodes), comprises the OSI model:

The OSI model breaks down the operations for transferring an electronic message into seven distinct "layers," each designated to perform certain operations in the data transfer process. While protocol stacks can potentially implement each of the layers, many protocol stacks implement only selective layers for use in transferring data across a network. When data is transmitted from a computing system, it originates at the application layer and is passed admitdown to intermediate lower layers and then onto a network. When data is received from a network it enters the physical layer and is passed up to higher intermediate layers and then eventually received at the application layer. The application layer, the upper most layer, is responsible for supporting applications and end-user processes. Another layer incorporated by most protocol stacks is the transport layer. An example of a transport layer protocol is the Transmission Control Protocol ("TCP").

Kaler, [0005].

44. Additionally, the incompatibility between handshake protocols is resolved by sending context information in multiple portions:

A first application layer at a first end message processor identifies that a first portion of context information is to be used to establish a secure context with a second application layer at a second end message processor. This can include a first portion of a distributed application at the first message processor identifying context information for establishment of a secure context with a second portion of the distributed application at the second end message processor. The context information is identified such that a secure context can be established between the first and second application layers independent of other context data identified at other layers in a communication stack (e.g., independent of context data exchanged during a Secure Socket Layers handshake). Thus, an application designer can more easily design a distributed application such that portions of the distributed application can establish a secure context having particular desired properties.

Kaler, [0016]

45. As discussed in detail below, context information is utilized by the communication system between remote nodes, to create a secure context. Distinct layers from the hierarchical protocol stack selectively indicate and obtain and add context information related to the outgoing message to the outgoing message. This context information persists through communications and can be found in response messages from destination nodes.

c. Scope and Content of Java™ Message Service (“JMS”) Specification (Sun)

46. Java™ Message Service (“JMS”) Specification (“Sun”) (SAP_VAL_0368219) was published on April 12, 2002. It is my opinion that Sun discloses and/or renders obvious each of the limitations of the Asserted Claims, as discussed in greater detail below.

47. JMS provides a common service for enterprise messaging, including messaging between applications on various clients (“nodes”), as explained in Sun:

Enterprise messaging products (or as they are sometimes called, Message Oriented Middleware products) are becoming an essential component for integrating intra-company operations. They allow separate business components to be combined into a reliable, yet flexible, system.

In addition to the traditional MOM vendors, enterprise messaging products are also provided by several database vendors and a number of internet related companies.

Java language clients and Java language middle tier services must be capable of using these messaging systems. JMS provides a common way for Java language programs to access these systems.

JMS is a set of interfaces and associated semantics that define how a JMS client accesses the facilities of an enterprise messaging product.

Since messaging is peer-to-peer, all users of JMS are referred to generically as clients. A JMS application is made up of a set of application defined messages and a set of clients that exchange them.