United States District Court,
N.D. California, San Jose Division.

**CRYPTOGRAPHY RESEARCH, INC,**
Plaintiff.
v.
**VISA INTERNATIONAL SERVICE ASSOC., et al,**
Defendant.

No. C 04-04143 JW

**Sept. 28, 2007.**

Darren E. Donnelly, J. David Hadden, Lynn Harold Pasahow, Laurie Michelle Charrington, Ryan Aftel Tyz, Saina Sason Shamilov, Fenwick & West LLP, Stephen Roger Dartt, Mountain View, CA, David Douglas Schumann, Jedediah Wakefield, Fenwick & West LLP, San Francisco, CA, for Plaintiff.

Brandon D. Baum, Dennis S. Corgill, Eric Butler Evans, Joshua Michael Masur, Michael A. Molano, Ian N. Feinberg, W. Joseph Melnik, Mayer Brown LLP, Palo Alto, CA, Elizabeth S. Campbell, Philadelphia, PA, Martin Frank Majestic, Alexandra V. Percy, Michael A. Duncheon, Hanson Bridgett Marcus Vlahos & Rudy, LLP, San Francisco, CA, Mary Elaine Johnston, Michael J. Gallagher, Joshua David Dick, White & Case LLP, Howard Marc Wettan, New York, NY, William Joseph Healey, Attorney at Law, Washington, DC, Joseph Helmsen, Pittsburgh, PA, for Defendant.

## FOURTH CLAIM CONSTRUCTION ORDER

JAMES WARE**, United States District Judge.**

## *I. INTRODUCTION*

This is the Fourth Claim Construction Order in this patent infringement action filed by Plaintiff Cryptography Research, Inc. (CRI) against Defendant Visa International Service Association (Visa). This Order sets forth the Court's construction of disputed words and phrases in claims of the 6,539, 092 Patent ('092) according to the previously stated legal standards. ( *See* Second Claim Construction Order, Docket Item No. 330.)

## *II. DISCUSSION*

### **A.** ***The '092 Patent-Claim 1***

Claim 1 provides in part FN1:

FN1. Unless otherwise indicated, all bold typeface is added by the Court to emphasize wordand phrases under consideration.

A computer-implemented process for securing a first device while performing transactions with at least one second device, wherein said first device includes a computer-readable memory having an internal **secret state,** and wherein said at least one second device has access to a **base secret cryptographic value** corresponding to said internal secret state, comprising the steps of:
(a) using an **index parameter** associated with said internal secret state to select **at least one state transformation operation;**

(b) applying at least said selected transformation operation to said internal secret state to produce an **updated secret state:**

(I) having associated therewith an updated secret cryptographic value **derivable** from said secret state, and

(ii) in a manner **inhibiting** leaked partial statistical information about said internal secret state from usefully describing said updated secret state;

(c) replacing in said memory:

(I) said internal secret state with said updated secret state, and

(ii) said **index parameter** with an **updated index parameter;**

(d) performing a cryptographic transaction with said at least one second device by transmitting said updated index parameter and at least one datum secured using said updated cryptographic value to said at least one second device configured to:

(I) regenerate said updated cryptographic value from said base cryptographic value, and

(ii) use said updated cryptographic value to process said secured datum;

(e) said steps (a) through (d) being repeated a plurality of times, and said regeneration in (d)(I) being performable in substantially fewer applications of state transformations than a total number of repetitions of said steps (a) through (d).

### 1. The Preamble of Claim 1

Claim 1 of the '092 Patent is an invention of a process for securing one device while performing transactions with at least one second device. The Preamble to Claim 1 discloses a **"first device"** which "includes a computer-readable memory having an internal secret state," and **"at least one second device"** which has access to a "base secret cryptographic value" corresponding to "said internal secret state."

Generally, the preamble of a claim does not limit the claim. Allen Eng'g Corp. v. Bartell Indus., Inc., 299 F.3d 1336, (Fed.Cir.2002). However, if a preamble is used as an antecedent, e.g., to define the apparatus which performs the claimed invention, it is limiting. Allen Eng'g Corp., 299 F.3d at 1346 (citing Bell Comm. Research, Inc. v. Vitalink Comm. Corp., 55 F.3d 615, 620 (Fed.Cir.1995)).

In this case, both the "first device" and "the at least one second device" are limitations on the method claimed in Claim 1. In addition, the parameters of those devices which are disclosed in the Preamble are limitations on the devices because the recited elements refer back to the Preamble as antecedents by using the referent "said." Accordingly, the Court finds that the Preamble of Claim 1 is limiting.

**2. "secret state"**

A limitation on the "first device" is that it includes a computer-readable memory having an internal "secret state." The parties dispute the meaning of the phrase "secret state."

The plain and ordinary meaning of the word "state" is the condition of a device at a given instance. *See* Institute of Electrical and Electronics Engineering (IEEE) Dictionary of Standards Terms, 1102 (7th ed.2000). A person of ordinary skill in the art reading the patent documents at the time of the invention would understand that the phrase "secret state" refers to a collection of parameters which are stored in a memory. The "base secret cryptographic value" and the "updated secret cryptographic value" are examples of such parameters. The written description provides:

In one embodiment, a cryptographic client device (e.g., a smartcard) maintains a **secret key value as part of its state** ... [a] state's secret key value typically, but notnecessarily, includes a secret session key.

('092 Patent, Col. 2:22-24, 3:66-4:1.)

In addition, "secret state" also refers to the condition of the memory when it is holding a secret value:

In an exemplary embodiment, the client is initialized with a secret key $K_0$ for a symmetric cryptosystem, where $K_0$ is also known to (or derivable by) the server. Thekey $K_0$ is usually (but not necessarily) specific to a particular client device or party.

* * *

FIG. 1 shows an exemplary sequence of client device **secret state values** usable to perform a series of transactions, typically (but not necessarily) using **one state pertransaction.** (The client process used to produce the sequence will be described withrespect to FIG. 2 and the corresponding server process will be described with respectto FIG. 3.) A **state's** secret value typically, but not necessarily, includes a secretsession key; therefore, as a matter of convenience, the secret value will be denoted byK and the term "secret value" may be used somewhat interchangeably with "key."

('092 Patent, Col. 3:50-57, 4:1-3.)

Accordingly, the Court construes the phrase **"secret state"** to mean: **one or more parameters, the attributes, conditions or values of which are secret, which are stored in computer-readable memory of the device.**

**3. "a base secret cryptographic value"**

A limitation on the "at least one second device" is that it has access to "a base secret cryptographic value" corresponding to said internal secret. The parties dispute the meaning of "base secret cryptographic value."

The language of Claim 1 states that the "base secret cryptographic value" corresponds to "said internal secret state."

The "Detailed Description of the Invention" provides:

The server also obtains the client's **base key value $K_0$** (for example, by retrieving $K_0$ from the server's memory, by **cryptographically deriving $K_0$** using other secret keysor secret algorithms, by obtaining $K_0$ from a third party such as a key server, etc.).

('092 Patent, Col. 6:62-66.)

The court construes the phrase **"base secret cryptographic value corresponding to said internal secret state"** to mean: **an initial value sought to be kept secret which is used in the cryptographic method disclosed in Claim 1.**

The parties dispute the effect, if any, which step (b) has on the definition of "base secret cryptographic value." In step (b), substep (I), an "updated secret cryptographic value" is derivable. The parties dispute whether this "updated" value FN2 is a new value, leaving the "base" value *unchanged* or whether the "updated" value *changes* the base value. The Court is requested to indicate in its definition whether the "base" value is "unchanging."

FN2. The dispute also applies to successive "updated" values which are created as step (b) isrepeated a plurality of times under step (e).

A person skilled in the art at the time of the invention would understand from the "Detailed Description of the Invention" that the base value is not retained and used in succeeding processes. Instead, the inventor discloses a method in which the base value is changed in the updating process. Therefore, the Court finds it unnecessary to include the word "unchanging" in its construction of the phrase.

Moreover, the written description discloses an embodiment in which a base cryptographic value may be changed. The specification discloses a state in which "rekeying" could be performed:

Eventually, the client may reach a point at which the entire table has been traversed. For example, the end of the process of FIG. 1 is reached at step 170, where C=60. After this transaction (or at an earlier point if the table length exceeeds the maximum number oftransactions allowed by the system), the client device could, and might typically disableitself, such as by deleting its internal secrets. However, other actions may be preferable insome cases (e.g., by repeating back to step 110, entering a state in which **rekeying** is required, etc.).

('092 Patent, Col. 5:40-49.)

"Rekeying" could establish a new base cryptographic value. Therefore, the Court declines to include the word "unchanging" in the construction of the phrase because it would eliminate re-keying as part of the process.

### 4. "using an index parameter associated with said internal secret state to select atleast one state transformation operation"

Step (a) of the process provides: "using an index parameter associated with said internal secret state to select at least one state transformation operation." The parties dispute the construction of the phrases: "index parameter" and "state transformation operation."

#### a. "index parameter"

With respect to the phrase "index parameter" the parties dispute whether the parameter is limited to a "transaction counter."

The phrase "index parameter" is not used in the "Detailed Description of the Invention." In the Claims, the inventor used the phrases "index parameter" and "index value" interchangeably,FN3 and used the phrase "index value" in the written description. Therefore, the Court examines the inventor's definition of "index value" to define "index parameter."

FN3. *See e.g.,* Claim 44: "The method of claim 40 wherein said second device also contains an **index parameter,** and comprising the further steps of: (a) selecting the **larger index parameter** of the two devices, (b) using **said larger index value** to secure said transaction, and (c) both of saiddevices incrementing and storing said larger index value for use in subsequent transactions.

A person of ordinary skill in the art at the time of the invention would understand that the phrase "index value" refers to a value which can perform the function of indexing. Transaction counting produces a value which can be used for indexing. However, the "Summary of the Invention" clearly states that the "index value" claimed in the invention is not limited to a transaction counter:

The present invention can be used in connection with a client and server using such a protocol. To perform a transaction with the client, the server obtains the client's **current transaction counter (or another key index value).**

The "Detailed Description of the Invention" discloses an embodiment where the value used for indexing is not limited to a transaction counter:

FIG. 3 shows an exemplary server-side process compatible with the exemplary client-side process of FIG. 2. Prior to commencing the process of FIG. 3, the server obtainsthe client's counter value C (typically by receiving C from the client device via adigital I/O interface), which is used as a key index. (In this exemplary embodiment, atransaction counter is used as a key index, but alternate embodiments can use adifferent value or representation of the key index.)

('902 Patent, Col. 6:54-61.)

Accordingly, the Court construes the phrase **"index parameter"** to mean: **a parameter used to derive another value. For purposes of the process disclosed in Claim 1, a transaction counter can be used as an "index parameter." However, an "index parameter" is not limited to a transaction counter.**

#### b. "state transformation operation"

The parties dispute the meaning of the phrase "state transformation operation." The Court has already defined the word "state." *See supra* A(2). The word "transformation" is a common term generally meaning "to change." The Court finds no basis for giving the phrase **"state transformation operation"** any different construction than its plain ordinary meaning of **"a process for changing the state."** The Court declines to include in its construction the phrase "mathematical function," on the ground that its inclusion would improperly import a limitation into the claim.

### 5. "updated secret state"

Step (b) of the process provides: "applying at least said selected transformation operation to said internal secret state to produce an updated secret state." For convenience, the Court will refer to step (b) as the "applying step." In the applying step, the parties dispute the construction of the phrase "updated secret state." In particular, the dispute is over whether an exemplary "mathematical function" disclosed in the written description FN4 should be included in the construction. Defendant would like to import the limitation that the "transformation operation" is a "mathematical function."

FN4. ( *See* '092 Patent, Col. 4:35-39.)

The ordinary and customary meaning of "to update" is "to change." Nothing in the specification, including the claim, indicate that the inventor intended to limit "updated secret state" to the exemplary mathematical function disclosed in the written description. Therefore, the Court finds that the ordinary and customary meaning attributed to the term "updated secret state" by those skilled in the art should be applied.

Accordingly, the Court construes the phrase **"updated secret state"** to mean: **a changed secret state.**

### 6. "value derivable from said secret state"

The "applying step" contains two substeps. Substep (I) discloses performing the "applying" step: "having associated therewith an updated secret cryptographic value derivable from said secret state." The parties dispute the construction of the word "derivable" as it is used in substep (I).

The word "derive" and the related term "derivable" have plain and ordinary meanings; they are: obtain or obtainable from a source. *See* Webster's New Twentieth Century Dictionary, 491 (2d ed.1983). This broad definition does not exclude copying or any other means for deriving a value.

In the '092 Patent, the word "derive" is used with its plain ordinary meaning. For example, the "Summary of the Invention" states:

The server then performs a series of operations to determine the sequence of transformations needed to **re-derive** the correct session key from the client's initial secret value. These transformations are then performed, and the result is used as a transaction session key (or used **to derive** a session key).

* * *

Using methods that will be described in detail below, such update functions are applied by the client in a sequence that assures that any single secret value is never used or **derived** more than a fixed number of times (for example, three).

('092 Patent, Col. 2:48-65.) Since the patentee did not define derive or derivable, the Court finds that the plain and ordinary meaning controls. Accordingly, the Court declines to construe the word "derivable."

### 7. "inhibiting"

Substep (ii) discloses performing the "applying" step: "in a manner inhibiting leaked partial statistical information about said internal secret state from usefully describing said updated secret state." The parties dispute the construction which should be given to the word "inhibiting." The dispute centers on whether the word "inhibiting" should be construed as "prohibiting" leaked information or whether "leak resistance" is meant.

This dispute is a manifestation of the continuing dispute over the degree of security claimed by the patents-in-suit.FN5 The Abstract provides:

FN5. In its First Claim Construction Orders, the Court construed the phrase "resistant to" as "less susceptible to external influence." ( *See* Docket Item No.269 at 5.) In its Second Claim Construction Order, the Court further construed the same phrase as requiring "no particular amountof resistance." ( *See* Docket Item No. 282 at 6.)

Methods and apparatuses for increasing the leak-resistance of cryptographic systems using an indexed key update techniques are disclosed.
The "Detailed Description of the Invention" provides:

The invention enables parties to perform cryptographic operations with increased security against external monitoring attacks.

('092 Patent, Col.3:34-36.)

Accordingly, the Court construes **"inhibiting"** to mean: **restricting.**

## B. *Claim 2 of the '092 Patent*

Claim 2 provides:

The process of claim 1 wherein values for said updated secret cryptographic value are **never recreated** more than a **fixed number of times** when said step (b) is repeated a large number of times.

Claim 2 depends from Claim 1. Specifically, Claim 2 is a limitation on step (b) of Claim 1. The parties dispute the meaning of two phrases in Claim 2: "never recreated more than" and "a fixed number of time."

### 1. "never recreated more than"

In the process disclosed in Claim 2, the inventor used the word "never." The word "never" is a commonly used word which means "not ever; not at any time; under no circumstances." *See* Webster's New Twentieth Century Dictionary, 1208 (2d ed. 983). The phrase "never recreated" refers to values for the "updated cryptographic value" disclosed in Claim 1(b). Claim 2 limits the transformation operation to "never" recreate the same secret cryptographic value "more than a fixed number of times."

**2. "fixed number of times"**

The dispute over "fixed number of times" centers around whether the limit on the recreation of the "values" is pre-determined. The plain ordinary meaning of the phrase "fixed number" is a number which is "established or set." *See* Webster's New Twentieth Century Dictionary, 694 (2d ed.1983). The inventor used the phrase with its plain ordinary meaning:

Using methods that will be described in detail below, such update functions are applied bythe client in a sequence that assures that any single secret value is never used or derived morethan a fixed number of times (for example, three).

('092 Patent, Col. 2:62-65.)

On the face of Claim 2, the parameters and cryptographic operations which determine the limit and impose the "no further re-creation of values" limitation are part of the cryptographic algorithm of Claims 1 and 2.

The Court construes the entire phrase of Claim 2, "values for said updated secret cryptographic value are **never recreated** more than a **fixed number of times"** to mean: **identical secret cryptographic values are never recreated more than a fixed number of times. The number of times is determined by the transformation operation algorithm and the initial parameters.**

**C.** ***Claim 15 of the '092 Patent***

Claim 15 provides:

The device of claim 13 wherein:

(I) said plurality of update operations is performed n times; and

(ii) the value of said updated secret parameter after said processor has performed said n update operations can be derived by said receiving device from the value of said secret parameter before said n operations **with substantially less computational effort** than would be required to perform n update operations.

The parties dispute the construction of the phrase "substantially less computational effort." The "Summary of the Invention" section of the specification describes the process as follows:

If the number of operations that can securely be performed by a client is n (i.e., n different transactions can be performed, without using the same secret value more than a fixed number of times), a server knowing or capable of obtaining the client's initial secret value K (or initial state corresponding thereto) can derive any resulting secret value (or corresponding state) in the series of transactions significantly faster than by performing n corresponding updates. Indeed, the state for any given transaction can often be derived by a server using O(log n) calculations of F sub A or F sub B (or their inverses).

('092 Patent, Col. 3:5-15.)

A person of ordinary skill in the art at the time of the invention would understand that the invention is a server which derives a "resulting secret value or corresponding state" by using an algorithm, which is different than the algorithm of the transformation operation used in the client device. Using this algorithm, the server arrives at the same result with fewer computations than it would have to perform if it repeated the transformation operations performed by the client device.

Accordingly, the Court construes **"with substantially less computational effort"** to mean: **with substantially fewer computations.**

**D.** ***Claim 21 of the '092 Patent***

Claim 21 provides:

The device of claim 20 wherein said at least one memory further contains a **depth parameter D** and where said processor is configured to select said at least one cryptographic transformation based on the current value of said index parameter and said parameter D.

The parties dispute the construction of the phrase "depth parameter D." The written description discusses the D parameter:

An additional parameter is an index depth D. The value of D may also be non-secret, and (for example) may be client-specific or may be a system-wide global constant. The value of D determines the cycle length of the key update process.

('092 Patent, Col. 3:54-60.)

In the context of Claim 21, the reference to parameter D concerns the usage of parameter D in the key update process of the client device, not the server device.FN6 The specification states, "D determines the cycle length." The parties dispute whether the inventor's use of the word "determines" means that D is used in the process of the secret key transformation operation to determine the cycle length or whether D is the cycle length value. In this regard, the specification provides:

FN6. The Court declines the constructions of the parties which apply this claim to the "receiving device." The Court finds that the claim applies to a client device.

In the client cryptographic update operations parameter D is used for two purposes:

Note that each iteration of the process of FIG. 2 corresponds to moving down one level in thedrawing of FIG. 1, until the correct update operation is determined. Thus, the number of iterations of the loop cannot exceed D.

('092 Patent, Col. 6:38-41.) Thus parameter D represents the maximum number of iterations a transformation operation may have to iterate until a new updated secret parameter is found.

In addition, parameter D is also used to determine which update function to use during the transformation operation:

At step 230, the device tests whether the variable V is equal to the quantity 2.sup.N-3. If equal, function F.sub.A.sup.-1 should be applied, and processing proceeds to step 235 where the device increments C and updates K.sub.C by computing K.sub.C.rarw.F.sub.A.sup.-1 (K.sub.C). Otherwise, at step 240, the device tests whether the variable V is equal to the quantity 2(2.sup .N-2). If equal, function F.sub.B.sup.-1 should be applied, and processing proceeds to step 245 where the device increments C and updates K.sub.C by computing K.sub.C.rarw.F.sub.B.sup.-1 (K.sub.C) ...

('092 Patent, Col. 6:8-16.) A person of ordinary skill in the art reading the patent documents at the time of the invention would understand that the inventor used the word "determines" to mean that D is used in the cycle length calculation and that D itself is not the cycle length.

Accordingly, the Court construes "depth parameter D" in the context of Claim 21 to mean: **a system parameter used to determine which transformation function to use in the secret state transformation process, and a parameter whose value is greater than or equal to the number of transformation iterations in a transformation operation.**

**E.** ***Claim 28 of the '092 Patent***

Claim 28 provides:

A cryptographic server device comprising:

(a) an interface for receiving a value of an index parameter and cryptographictransaction data; and

(b) **a processor configured to derive a current value of a secret parameterfrom an initial value of said secret parameter, said value of said indexparameter, and a value D representing the depth of a secret parametertransformation loop, within O(D) iterations of said secret parametertransformation loop and where the number of acceptable values for said indexparameter is substantially larger than D.**

On the Joint Claim Construction Chart the parties list every word and phrase in element (b) as in dispute. The parties' proffered constructions appear to reword the language of the claim without identifying any particular word or phrase in dispute. The Court declines to construe Claim 28 under these circumstances. The Court invites the parties to resubmit any dispute with respect to a word or phrase in Claim 28.FN7

FN7. Though there are differences in the wording proffered by the parties, at least one partyrequests the Court construe D to be a "maximum number of transformations performed." The Court declines to add a limitation to the construction that the maximum number of transformation operations to be performed by the receiving device be limited to the value of system parameter D. The specification cites: "... the state for any given transaction can often be derived by a serverusing O(log n) calculations ..." ('092 Patent, Col. 3:13-14.) Thus, although D is used in thealgorithm to determine the maximum number of transformations performable under thecircumstances disclosed in the process, the value of D, itself is not the maximum.

Although the Court declines to construe Claim 28, the request to do so drew the Court's attention to Claim 30, which depends from Claim 28. Claim 30 is arguably indefinite as ambiguous because it uses the phrase "said server comprises an ISO 7616-compliant smartcard." The language of Claim 30 equates a "server" with a "smartcard." This precise language is used in Claims 14 and 18, referring to *client devices*. Therefore, Claim 30 is arguably indefinite.

### *III. CONCLUSION*

In this Order the Court has construed some of the disputed words and phrases of the '092 Patent. Some of the words and phrases for which the parties initially requested construction are not addressed in this Order because the Court finds that they are the same or substantially the same as words and phrases construed in earlier Orders. To the extent a party contends that an omitted word or phrase should be addressed, a supplemental request for construction should be made on a timely basis.

N.D.Cal.,2007.
Cryptography Research, Inc. v. Visa Intern. Service Assoc.

Produced by Sans Paper, LLC.