* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

% *Judgment delivered on: 24.12.2025*

+ **C.A.(COMM.IPD-PAT) 119/2022**
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL). .....Appellant

versus

CONTROLLER GENERAL OF PATENTS, DESIGNS AND TRADEMARKS. .....Respondent

Advocates who appeared in this case

For the Appellant : Mr. Manish Aryan, Mr. Nishant Rai, Ms. Manisha Singh, Mr. Abhai Pandey, Ms. Anuja Agarwal, Mr. Gautam Kumar, Ms. Swati Mittal, Mr. Druv Tandan, Ms. Shivani Singh, Ms. Shruthi Venugopal and Ms. Akhya Anand, Advocates.

For the Respondent : Ms. Rukhmini Bobde, CGSC with Mr. Amlaan Kumar, Mr. Vinayak Aren, Mr. Jatin Dhamija and Mr. Anmol Jagga, Advocates.

CORAM:
HON'BLE MR. JUSTICE TEJAS KARIA

JUDGMENT

TEJAS KARIA, J

1. The present Appeal is filed under Section 117A of the Patents Act, 1970 ("**Act**") against the order dated 30.09.2019 ("**Impugned Order**") in the Indian Patent Application No. 6132/DELNP/2007 dated 06.08.2007

(“**Subject Application**”) rejecting the Subject Application by the Assistant Controller of Patents and Designs (“**Respondent / Controller**”) on the ground of lack of inventive step under Section 2(1)(ja) of the Act.

2. The Appellant, *Telefonaktiebolaget LM Ericsson (Publ)*, with its principal place of business at Stockholm, Sweden filed an International Application No. PCT/SE2006/000312 on 09.03.2006 (“**PCT Application**”), titled ‘*PROTECTION OF DATA DELIVERED OUT-OF-ORDER*’ (“**Subject Patent**”). The PCT Application claimed priority to US Patent Application No. 60/666,597 filed on 31.03.2005.

3. Based on the PCT Application, the Appellant filed the Subject Application with the Patent Office, Delhi (“**Patent Office**”). The Subject Application was examined under Sections 12 and 13 of the Act and the First Examination Report was issued on 11.03.2015 (“**FER**”). In response to the FER, the Appellant submitted its reply to the FER on 06.10.2015 (“**Reply**”).

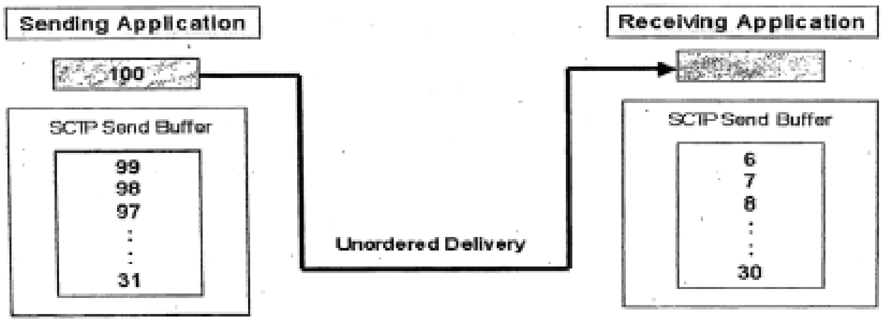
4. After considering the Reply to the FER, a hearing notice dated 24.06.2019 (“**Hearing Notice**”) was issued to the Appellant by Respondent No. 2 scheduling the hearing for 19.07.2019 (“**Hearing**”).

5. The Agent for the Appellant appeared before Respondent No. 2 for the Hearing at the Patent Office and subsequently, written submissions along with amended claims and other documents were filed by the Appellant on 01.08.2019 (“**Written Submissions**”).

6. Respondent No. 2 *vide* the Impugned Order refused the grant of the Subject Patent filed *via* the Subject Application on the grounds of lack of inventive step under Section 2(1)(ja) of the Act.

7. Being aggrieved by the Impugned Order, the Appellant has filed the present Appeal.

8. The learned Counsel for the Appellant submitted that the present invention is directed to security aspects of reliable transport protocol such as stream control transmission protocol (“**SCTP**”) and particularly to provide protection of data delivered out of order in reliable transport protocol. Normally, within a SCTP stream, data message is delivered in order from one device to another. If a data message arrives out of order, it is held back from delivering to upper layer. However, when a device receives a data chunk indicated for unordered delivery, it may bypass the ordering mechanism and immediately deliver the date to the upper layer. Figure 1 of the Subject Application is reproduced hereunder:



9. The learned Counsel for the Appellant submitted that an advantage of unordered delivery is that it helps in avoiding head of line (“**HOL**”) blocking i.e., the data chunk which is marked as unordered will be transferred to upper layer. In general, the data security of SCTP association can be achieved by using transport layer security (“**TLS**”) protocol on top of the transport layer, but TLS protocol can be used only for ordered delivery.

10. The learned Counsel for the Appellant submitted that the Subject Patent discloses separating ordered delivery data and unordered delivery data in a security protocol running on top of the reliable transport protocol and performing two different types of security processing i.e., one for

ordered delivery data and the another for unordered delivery data in the security protocol. Preferably, data messages using ordered delivery and data messages using unordered delivery within a secure data stream are separated into two message sequence spaces on the security protocol layer, and data security processing is then performed differently in these two spaces. The existing security protocols such as TLS are not competent to make this distinction. The present invention extends a security protocol, on top of the transport layer to allow a separation of ordered and unordered delivery data at the security protocol layer and to perform different types of security processing depending on the type of delivery.

11. The learned Counsel for the Appellant further submitted that the Subject Patent provides a solution for the TLS to make said distinction. In particular, the processing of unordered records can for example be implemented as an extension of a security protocol such as TLS and the use of this extension can be negotiated in-band during (TLS) handshake (which is done in the ordered delivery sequence space) to make it backward compatible with legacy (TLS) implementation. If a legacy (TLS) implementation is faced with unknown record types, the connection will be terminated. This implies that a legacy (TLS) implementation will not crash ungracefully if it gets records of the new types.

12. The learned Counsel for the Appellant submitted that technical solution of the present invention is achieved by the rejected claim 1. The rejected claim 1 recites the following solution:

> *"1. A method for providing data security for a reliable transport protocol that supports ordered delivery of data as well as unordered delivery of data, characterized by:*
>
> *separating ordered delivery data and unordered delivery*

> *data in a security protocol running on top of the reliable transport protocol;* (***Claim feature 1***)
>
> *inserting a sequence number in a header of the unordered delivery data, the sequence number used for ensuring the arrival and processing of all unordered delivery data;* (***Claim feature 2***) *and*
>
> *performing, in said security protocol, a first type of security processing for ordered delivery data and a second different type of security processing for unordered delivery data.* (***Claim feature 3***)"

13. The learned Counsel for the Appellant submitted that in order to effectuate replay protection for unorderly delivered messages in an efficient manner, it is beneficial to maintain a list of those messages that have been received, or alternatively of those messages that have not been received. The detailed description of the Complete Specification of the Subject Application describes the sequence number and advantages of the present invention is as under:

> "***For data dropping protection, a termination message for termination of a security protocol connection generally includes an end sequence number of the sent unordered data messages, and reliable reception of all sent records in the unordered record space may then be detected based on the end sequence number in the termination message.***
>
> *The invention is highly compatible and fully operable with existing protocols such as UDP, DCCP, and PR-SCTP.*
>
> *The invention offers the following advantages:*
>
> - *Improved data security.*
> - *A robust and efficient security solution on top of the transport layer for data that uses the unordered delivery feature.*
> - *Data security with efficient utilisation of valuable stream resources.*
> - *Highly compatible with existing underlying transport protocols.*"

14. The learned Counsel for the Appellant submitted that the present invention under the Subject Application is suitable for SCTP and the

security protocol running on top of the transport protocol is preferably based on the TLS or a TLS-like protocol. The relevant paragraph of the Summary of the Complete Specification is reproduced hereunder:

> "*The invention is particularly suitable for a reliable transport protocol such as SCTP (Stream Control Transmission Protocol). The security protocol running on top of the transport protocol is preferably based on the TLS (Transport Layer Security) or a TLS-like protocol with a security processing extension for unordered delivery. It should however be understood that other combinations of security and transport protocols can be made.*"

15. Citing the Paragraph No. 9 of the Impugned Order, the learned Counsel for the Appellant argued that D1 does not disclose the feature of unordered delivery of data, but D3 does. It was also submitted that Paragraph No. 12 and Paragraph No. 9 conflict with each other.

16. The learned Counsel for the Appellant further submitted that this is only reasoning provided by the learned Controller, which is self-contradictory. It was submitted that the Impugned Order to be set aside on this ground alone.

17. *Per Contra*, the learned CGSC for Respondent submitted that there is an inadvertent error in the Paragraph No. 9 and Paragraph No. 12. It was submitted that:

> "*3. At the outset, it is stated that there is an inadvertent error in para 9 and para 12 of the order. Though para 9 of the order as mentioned by the Appellant deals with the feature in respect of "inserting a sequence number in a header of the unordered delivery data, the sequence number used for ensuring the arrival and processing of all unordered delivery data" as disclosed in D3, in para 12 of the order it is inadvertently mentioned that the said feature was disclosed by D1 in place of document D3.*"

18. As regards, Document D1 (Pub. No.: US 2002/0112152 Al), the pertains to "*Method and Apparatus for Providing, Secure Streaming Data Transmission Facilities Using Unreliable Protocols*". The invention of D1 provides a method and apparatus for transmitting data securely using an unreliable communication protocol like User Datagram Protocol.

19. According to the submission of the learned Counsel for the Appellant, the data delivery is unordered under D1 as D1 only detects a special bit in the transmitted data-records that indicates that the data should undergo a different type of processing. D1 does not disclose the assigning sequence numbers to only the unordered data and hence D1 points in an entirely different direction. Therefore, the claim of inserting the sequence number in the Claim 1 of Subject Application is not disclosed.

20. Paragraph [0016] of the D1 states that relying on TCP / other guaranteed-delivery protocols makes SSL / TLS susceptible to the same performance problems that TCP incurs while using as under:

> "[0016] *Unfortunately, reliance on TCP or other guaranteed-delivery protocols renders SSL/TLS susceptible to the same performance problems that TCP incurs. For example, using SSL/TLS to transmit streaming video data incurs the same costs and penalties (e.g., "jerky" video) that the underlying TCP incurs. By its nature, SSL/TLS requires the use of a reliable connection such as provided by TCP, because they will terminate a connection if a packet is dropped or received out- of -order.*"

21. Other relevant paragraphs D1 that further discuss the use of using SSL/TLS are as under:

> "*[0014] FIG 1C shows a sample SSL/TLS record, which generally includes a header (HDR), encrypted data or ciphertext, and a MAC (Message Authentication Check). The MAC ensures message integrity by means of a keyed hash, similar to a strong checksum, and is generally calculated as a function MAC=h(key, plaintext,*

sequence number), where the sequence number is a one-up counter for successive records. The sequence number forms an important aspect of the MAC calculated by TLS, since it prevents so-called "splicing attacks" that could otherwise occur if a hacker attempted to intercept and re-order packets in an attempt to decrypt or disrupt secure communication between computers using TLS. If the recipient's TLS detects an incorrect sequence number for a received record, it will reject the record as an attempted breach and terminate the connection. This requires that the sender and recipient reestablish another TCP connection, which results in wasted time and resources."

"[0074] FIGS. 5A and 5B show a modified encryption and decryption scheme that can be used according to one variation of the present invention. In accordance with this variation, a slightly modified SSL/TLS record format 507 is used. A special bit (UDP) is embedded in the conventional header to indicate that the record contains encrypted UDP data and should be processed according to modified SOCKS processing function 3023. This bit can be used by record detectors 3021 and 3015 to determine whether any given SSL/TLS record should be routed to conventional SOCKS processing function 3022 or 3013, or to modified SOCKS processing function 3023 or 3014. This feature allows the principles of the invention to be applied with systems that conform to the existing SSL/TLS/SOCKS protocol, while also allowing enhanced security provisions to be used when UDP datagrams are transmitted."

"[0084] The use of a special UDP bit is only one technique for identifying records as conventional or modified SSL/TLS records. In one embodiment, no bit at all is needed, and the assumption is made that every record conforms to the modified SSL/TLS protocol as described herein. In other embodiments, different flags or methods can be used to signify that a particular record should be processed according to the modified scheme set forth above. As one example, during the initial handshaking that occurs between client and proxy server, a message can be sent indicating that subsequent records will be received according to the aforementioned protocol. In another embodiment, secure TCP can be used to exchange a set of

> *MAC or IV values, equivalent to the nonce, for comparison and identification of the data record. bit.*"

22. Therefore, Document D1 discuss the modification of SSL/TLS and its use along with different types of processing as per special bit. The learned CGSC for the Respondent relying on the above paragraphs of D1 also argued that that the argument presented by the Appellant with respect to Document D1 is not complete and satisfactory.

23. As regards D2, it discusses the Transport Layer Security over Stream Control Transmission Protocol. D2 discusses SCTP for the Internet community.

24. The learned Counsel for the Appellant submitted that D2 is the same as FIG 5 of the Complete Specification for the Subject Application. D2 is teaching aways as it specifies that the unordered delivery feature of SCTP must not be used together with TLS. The learned Counsel for the Appellant referred to Paragraph No. 6 of D2 and submitted that D2 also envisions sequence to make sure that data is delivered as under:

> "*The data sender MUST break the user message into a series of DATA chunks such that each chunk plus SCTP overhead fits into an IP datagram smaller than or equal to the association Path MTU. The transmitter MUST then assign, in sequence, a separate TSN to each of the DATA chunks in the series. The transmitter assigns the same SSN to each of the DATA chunks. If the user indicates that the user message is to be delivered using unordered delivery, then the U flag of each DATA chunk of the user message MUST be set to 1. The transmitter MUST also set the B/E bits of the first DATA chunk in the series to '10', the B/E bits of the last DATA chunk in the series to '01', and the B/E bits of all other DATA chunks in the series to '00'. An endpoint MUST recognize fragmented DATA chunks by examining the B/E bits in each of the received DATA chunks, and queue the fragmented DATA chunks for re-assembly. Once the user message is reassembled, SCTP shall pass the re-assembled user*

> *message to the specific stream for possible re-ordering and final dispatching"*

25. On the other hand, citing the Paragraph No. 6.2 of the D2, the learned CGSC for the Respondent submitted that D2 teaches that TLS requires that the underlying transport delivers TLS records in strict sequence and, therefore, the 'unordered delivery' feature of 'SCTP MUST NOT' be used on streams, which are used for TLS-based user data transmission as under:

> "*6.2 TLS-based user data transmission*
> *In general, the bi-directional stream will be used for TLS-based user data transmission and it SHOULD NOT be used for SCTP-based user data transmission. The exception to this rule is for protocols which contain upgrade-to-TLS mechanisms, such as those of HTTP upgrade [RFC2817] and SMTP over TLS [RFC3207].*
>
> *TLS requires that the underlying transport delivers TLS records in strict sequence. Thus, the 'unordered delivery' feature of SCTP MUST NOT be used on streams which are used for TLS based user data transmission. For the same reason, TLS records delivered to SCTP for transmission MUST NOT have limited lifetimes."*

26. The learned CGSC for the Respondent also relied on the article "Stream Control Transmission Protocol" publication by "Network Working Group, Request for Comments: 2960". Document D2 has referred this document at various places. Citing Page Nos. 9, 14, 81-82 and 22, it was submitted that D2 also teaches 'transmission sequence number', 'stream sequence number' and 'insertion of transmission sequence number' in the header of message used for ensuring arrival. The relevant paragraphs are reproduced hereunder:

> *Point 1.3.4 at page 9*
> *SCTP assigns a Transmission Sequence Number (TSN) to each user data fragment or un- fragmented message. The TSN is independent of any stream sequence number assigned at the*

> *stream level. The receiving end acknowledges all TSNs received, even if there are gaps in the sequence. In this way, reliable delivery is kept functionally separate from sequenced stream delivery.*
>
> *Point 1.4 at page 14*
> *TSN is 32-bit sequence number used internally by SCTP. One TSN is attached to each chunk containing user data to permit the receiving SCTP endpoint to acknowledge its receipt and detect duplicate deliveries.*
>
> *Point 6.7 at page 81*
> *Upon the reception of a new DATA chunk, an endpoint shall examine the continuity of the TSNs received. If the endpoint detects a gap in the received DATA chunk sequence, it SHOULD send a SACK with Gap Ack Blocks immediately. The data receiver continues sending a SACK after receipt of each SCTP packet that doesn't fill the gap"*

27. Further, citing Page Nos. 83, 84 and 86, it was also submitted by the learned CGSC for the Respondent that D2 also teaches separating ordered data and unordered data according to flat bit and also processes the same according to the type of ordered data and unordered data as under:

> *"The data sender MUST break the user message into a series of DATA chunks such that each chunk plus SCTP overhead fits into an IP datagram smaller than or equal to the association Path MTU. The transmitter MUST then assign, in sequence, a separate TSN to each of the DATA chunks in the series. The transmitter assigns the same SSN to each of the DATA chunks. If the user indicates that the user message is to be delivered using unordered delivery, then the U flag of each DATA chunk of the user message MUST be set to 1. The transmitter MUST also set the B/E bits of the first DATA chunk in the series to '10', the B/E bits of the last DATA chunk in the series to '01', and the B/E bits of all other DATA chunks in the series to '00'. An endpoint MUST recognize fragmented DATA chunks by examining the B/E bits in each of the received DATA chunks, and*

> *queue the fragmented DATA chunks for re-assembly. Once the user message is reassembled, SCTP shall pass the re-assembled user message to the specific stream for possible re-ordering and final dispatching.*
>
> *SCTP can deliver data to its upper-layer protocol even if there is a gap in Transmission sequence number (TSN) if the Stream Sequence Numbers are in sequence for a particular stream (i.e., the missing DATA chunks are for a different stream) or if unordered delivery is indicated.*

28. Accordingly, it is clear that Document D2 teaches separating ordered data and unordered data according to flat bit and also processes the same according to the type of ordered data and unordered data.

29. Document D3 (JP2004080070A) pertains to '*DATA TRANSFER METHOD, DATA TRANSFER SYSTEM AND CONTENT DISTRIBUTION SYSTEM*'. The invention under D3 relates to a data transfer method and system for performing broadband and reliable data transfer between terminals, and a content distribution system using this data transfer method.

30. The learned Counsel for the Appellant submitted that D3 does not separate ordered delivery data and unordered delivery data in a security protocol running on top of the reliable transport protocol. D3 does not disclose the inserting a sequence number in a header of the unordered delivery data; the sequence number used for ensuring the arrival and processing of all unordered delivery data; and performing in the said security protocol where a first type of security processing for ordered delivery data and a second different type of security processing for unordered delivery data.

31. According to the learned CGSC for the Respondent, D3 teaches a method and apparatus for realizing high-reliability and high-speed data

transfer service similar to TCP with a small overhead for a higher-level application as under:

> *FIG. 4 illustrates the operation of the feedback control in the data transfer system shown in FIG. The system forms two feedback loops. That is, a transmission content feedback loop LO1 and a transmission speed feedback loop LO2. The transmission content feedback LOl is for retransmitting a packet loss or an error packet based on the sequence number of the unreceived packet included in the acknowledgment, and passing error-free data to a higher-level application. The transmission speed feedback LO2 is for obtaining an optimum transmission speed for improving network utilization efficiency and reducing packet retransmission based on the reception speed information of the receiving terminal device included in the acknowledgment.*
>
> *FIG. 5 shows an example of a format of a data packet transferred from the transmitting terminal to the receiving terminal in the data transfer system of the present invention shown in FIG. This packet contains four fields. That is, it includes an IP header 21, a UDP header 22, a packet sequence number 23, and a payload 24. The IP header 21 is used to transfer a packet between a transmitting terminal and a receiving terminal via an IP network.* ***The UDP header 22 is used in the terminal to distinguish packets from a plurality of applications. Further, the UDP header 22 has a checksum field, and can check a packet for errors during transmission. The packet sequence number 23 is used for detecting the order inversion, loss, and duplication of the packet in the network. A part of the entire transmission data is stored in the payload.***

32. Therefore, it was submitted by learned CGSC for the Respondent that D3 discloses the insertion of sequence numbers in the header of the message that is used for detection of order inversion, loss and duplication of the packet in the network.

33. However, the Appellant has contended that inserting a sequence number in a header of the unordered delivery data, and the sequence number

is used for ensuring the arrival and processing of all unordered delivery data is "inventive feature" in the Claim 1 of the Subject Application. The Claim 1 of the subject application claims the "separating ordered delivery data and unordered delivery data in a security protocol mining on top of the transport protocol and "perform different type of security processing for ordered delivery and unordered delivery data."

34. Therefore, the question arises that if the said feature of the Claim 1 of the Subject Application is not disclosed, does the disclosure made in these documents render the claimed invention obvious. Does the teaching the of D1 to D3 render the abovementioned feature obvious.

35. Documents D1 to D3 as discussed earlier, disclose about TCP, SCTP, UPD, TLS and insertion of sequence number in message and sequences. These cited Documents also discuss the ordered and unordered delivery of data / message and modified SSL / TLS. In other words, these features are available in the prior art at the priority date of the Subject Application.

36. The Impugned Order provides the detailed reasoning on how it would be obvious for PSITA to separate 'ordered delivery data' and 'unordered delivery data' in a security protocol mining on top of the transport protocol in the light of Document D1 to D3. The reasoning provided in the Impugned Order is that after duly considering the extensive hearing submissions, the subject matter of the Claim 1 is not inventive step at the time of the alleged invention as it would have been obvious to PSITA to arrive at the said claimed features of the alleged invention mentioned as separating ordered delivery data and unordered delivery data in a security protocol running on top of the reliable transport protocol; inserting a sequence number in a header of the unordered delivery data, the sequence number used for

ensuring the arrival and processing. of all unordered delivery data; and performing, in said security protocol, a first type of security processing for ordered delivery data and a second different type of security processing for unordered delivery data” in the light of document D 1 where "unordered delivery data", D3 where "ordered delivery data" and D2 where "Transport Layer Security over Stream Control Transmission Protocol" and the feature "separating ordered delivery data and unordered delivery data" is a common general knowledge and is obvious to a person skill in the art which is nothing but a mere workshop result.

37. It is clear from the above reasoning that the Claim 1 of the Subject Application claims the *“separating ordered delivery data and unordered delivery data in a security protocol mining on top of the transport protocol”* and *“perform different type of security processing for ordered delivery and unordered delivery data.”* D1 to D3, as discussed above, discloses about TCP, SCTP, UPD, TLS and insertion of sequence number in message and sequences. These cited documents also discuss the ordered and unordered delivery of data / message and modified SSL / TLS. In other words, these features are available in the prior arts at the priority date of the Subject Application.

38. Document D2 makes it obvious for the PSITA to separate data messages for "ordered delivery" and data messages for "unordered delivery" into two message sequence spaces on the security layer and perform data security processing differently in these two spaces and use of transmission sequence number in data chunks in SCTP.

39. Since the insertion of sequence number in the header of the message is disclosed and separation of ordered delivery data and unordered delivery

data in a security protocol mining on top of the transport protocol, performing different type of security processing for ordered delivery and unordered delivery data is rendered obvious in the light of disclose in the cited documents, the Impugned Order has rightly concluded that the claimed invention has no inventive step under Section 2 (1) (ja) of the Act.

40. The Impugned Order provides the detailed and adequate reasoning on how it would be obvious for PSITA to separate ordered delivery data and unordered delivery data in a security protocol mining on top of the transport protocol in the light of documents D1 to D3.

41. It is also obvious that there appears to be an inadvertent error in Paragraph Nos. 9 and 12 of the Impugned Order as submitted by the learned CGSC for the Respondent. Accordingly, the Impugned Order does not require any interference.

42. Accordingly, this Appeal is dismissed and the Impugned Order dated 30.09.2019 is upheld.

TEJAS KARIA, J

DECEMBER 24, 2025
KC/NS