CLAIMS

1. A system (100) for authorizing electronic transactions over a network, said system (100) comprising:

- a computing device (104) associated with at least one user, wherein the user is associated with an identification code, said computing device (104) prompts for an input of at least two authentication codes from the user and facilitates generation of a notification if said authentication codes are verified and transmits said notification along with said identification code to a data processing and storage unit (102) through a network (118);
- said data processing and storage unit (102) associated with at least one entity (106), wherein said data processing and storage unit (102) includes a processing unit (108) and a repository (110) coupled to said processing unit (108) that receives at least one notification and said identification code from a user associated with a computing device (104) for at least one entity and stores said notification in said repository (110) for the user; and
- said processing unit (108) comparing details of an actual transaction with the stored notification in said repository (110) for the user and authorizing a transaction in the event that said transaction is within the bounds of said notification and sends a confirmation message to the user;

wherein said authentication codes include at least one biometric sample and a single factor authentication code and/or a multifactor authentication code..

2. The system (100) as claimed in claim 1, wherein said biometric sample is received from the user during registration and said single factor authentication code and/or a multifactor authentication code is generated by said data processing and storage unit (102) before the actual

transaction or during the actual transaction.

3. The system (100) as claimed in claim 1, wherein said biometric sample is selected from the group consisting of a voice print, a fingerprint, a retinal image, an iris image, and a facial image.

4. The system (100) as claimed in claim 1, wherein said notification is a preemption message to notify said entity of a transaction.

5. The system (100) as claimed in claim 4, wherein said notification comprises information including specific / range based values pertaining to a transaction, monetary value / range bound monetary value for a transaction, currency details, credentials and geographical data of entities involved in the transaction, and time-limit associated with said notification.

6. The system (100) as claimed in claim 1, wherein said notification is generated for transactions at events including prior to initiation of a transaction, at initiation of a transaction, during a transaction and before completion of a transaction.

7. The system (100) as claimed in claim 1, wherein said computing device (104) transmits said notification to said data storage and processing unit (102) using communication techniques including Interactive Voice response, Touch Tone response, voice over data, and voice call.

8. The system (100) as claimed in claim 1, wherein said processing unit (108) sends a confirmation of delivery to said computing device (104) upon receiving said notification.

9. The system (100) as claimed in claim 1, wherein said processing unit (108) validates the authenticity of said notification and said identification code before storing in said repository (110).

10. The system (100) as claimed in claim 1, wherein said processing unit (108) updates the status of said notification on completion of an actual transaction, wherein said status includes details selected from the group consisting of the entity against which the notification is used; balance amount available in the notification and expiration details of the notification.

11. The system (100) as claimed in claim 1, wherein said processing unit (108) updates status of said transaction on completion of an actual transaction, wherein said status is selected from the group consisting of hold, cleared and posted.

12. The system (100) as claimed in claim 1, wherein said computing device (104) facilitates registration of a user, wherein said registration includes facilitating selection of at least one account associated with at least one entity; accepting a biometric sample from the user; prompting the user to select a preferred storage location for said biometric sample for future verification; and assigning an identification code to the user, wherein said preferred storage location includes in a memory (114) included in said computing device (104), said repository (110) of said data processing and storage unit (102) and a third party storage and verification server accessible to said computing device (104) and said data processing and storage unit (102).

13. The system (100) as claimed in claim 1, wherein said computing device (104) verifies said biometric sample with a sample stored therein to allow transmission of said notification to said data processing and storage unit (102).

14. The system (100) as claimed in claim 1, wherein said computing device (104) transmits said biometric sample to said data processing and storage unit (102), wherein said repository (110) stores a sample of said biometric sample and said processing unit (108) verifies said biometric sample with said sample and transmits verification result to said computing device (104).

15. The system (100) as claimed in claim 1 and 12, wherein said computing device (104) transmits said biometric sample to said third party storage and verification server, wherein said third party storage and verification server verifies said biometric sample with a biometric sample stored therein and transmits verification result to said computing device (104).

16. The system (100) as claimed in claim 1, wherein said processing unit (108) generates a reverse notification for a user associated with said computing device (104) in the event that no stored notification is retrieved from said repository (110) for an actual transaction.

17. The system (100) as claimed in claim 16, wherein said processing unit (108) transmits said reverse notification to said computing device (104) using communication channels selected from the group consisting of short message service (SMS), multimedia messaging service (MMS), direct messaging protocol and Email.

18. A computing device (104), said computing device (104) comprising: a processor (112); a memory (114) co-operating with the processor (112) and a data capturing unit (116) co-operating with said memory (114) and said processor (112),

wherein said memory (114) hosting a transaction application that when executed by said processor (112) performs operations including: prompting for an input of at least two authentication codes from a user using said data capturing unit (116); facilitating generation of a notification if said authentication codes are verified; transmitting said notification for authorizing an actual transaction; and receiving a confirmation and status of the transaction and said notification on completion of said actual transaction, wherein said

notification is a preemption message to notify said entity of said actual transaction.

19. The computing device (104) of claim 18, wherein said processor (112) initiates an interface for said transaction application, wherein said interface is at least for: initiating a

prompt to a user to login to the transaction application; registering at least one account associated with at least one entity with said transaction application; input of at least one biometric input from the user through said data capturing unit (116); selecting storage preference of said authentication code; capturing at

5

least one biometric input from the user via said data capturing unit (116); and verifying said biometric input to confirm registration.

20. The computing device (104) of claim 18, wherein said interface is at least for: initiating a prompt to a user for selecting at least one entity for generation of a notification; composing a notification by entering information including credentials and geographical data of the parties involved in the transaction, specific or range based value for the transaction and time-limit associated with the notification; performing authentication code verification; scrambling and compressing the composed notification for transmission on successful verification of the authentication codes; and displaying a notification delivery confirmation to the user.

21. The computing device (104) of claim 18, wherein said interface is at least for: checking the status of the notification including if the notification has been received by the entity; the entity against which the notification is used; balance amount available in the notification and expiration details of the notification.

22. The computing device (104) of claim 18, wherein said data capturing unit (116) is at least one device selected from the group consisting of a microphone, a biometric scanner and a biometric sensor.

23. The computing device (104) of claim 18, wherein said computing device (104) receives a reverse notification for verification of details of an actual transaction.

24. The computing device (104) of claim 23, wherein said computing device performs authentication code verification for a user in response to said reverse notification to facilitate a verified user to approve a transaction.

25. A method for authorizing electronic transactions over a network, said method comprising the following steps:

- verifying at least two authentication codes associated with a user;
- facilitating a verified user to generate a notification for conducting a transaction using a computing device;
- transmitting said notification along with an identification code to a data storage and processing unit;
- storing said notification corresponding to said identification code for a validated user in a repository at the data storage and processing unit;
- verifying an actual transaction based on the notification for a user at the data storage and processing unit;
- authorizing said actual transaction in the event that said actual transaction is within the bounds of said notification; and
- sending a confirmation message to the user.

26. The method as claimed in claim 25, wherein the step of facilitating a verified user to generate a notification includes prompting the verified user to enter credentials and geographical data of parties participating in the transaction; specific or range based value for the transaction;

time limit associated with the notification; and compressing and scrambling the composed notification for transmission.

27. The method as claimed in claim 25, wherein the step of storing said notification corresponding to said identification code includes sending a delivery receipt confirmation

message back to the computing device for displaying to the corresponding user.

28. The method as claimed in claim 25, wherein the step of verifying an actual transaction based on the notification includes the following steps:

- comparing the details of the notification with the details of the actual transaction to verify if actual transaction is within the bounds of said notification; and
- marking the notification as used / partly used in the repository and updating the status of the transaction.

29. The method as claimed in claim 25, wherein the step of verifying an actual transaction includes:

- generating a reverse notification at the data processing and storage unit in the event that no stored notification is retrieved;
- transmitting said reverse notification to a user on the corresponding computing device;
- conducting authentication code verification for the user; and
- enabling the user to approve a transaction if the authentication codes are verified.

30. The method as claimed in claim 25, wherein the method includes registration of users for facilitating authorization of transactions, said method comprising the following steps:

- prompting a user to select at least one account associated with at least one entity;
- prompting for input of at least one biometric reference from the user;

- prompting the user to select at least one storage preference of said biometric sample, wherein said storage preference is selected from the group consisting of in a memory included in the computing device, in the repository of the data processing and storage unit, and a third party storage and verification server accessible to the computing device and the data processing and storage unit;
- capturing at least one biometric sample from the user; and
- verifying said biometric sample with said stored sample to confirm registration and assign an identification code to the user.

31. The method as claimed in claim 25 and 30, wherein the step of verifying at least two authentication codes associated with a user includes verifying said biometric sample with a sample stored in the computing device.

32. The method as claimed in claim 25 and 30, wherein the step of verifying at least two authentication codes associated with a user includes verifying said biometric sample with a sample stored in the repository of the data processing and storage unit and transmitting the verification result to the computing device.

33. The method as claimed in claim 25 and 30, wherein the step of verifying at least two authentication codes associated with a user includes verifying said biometric sample with a sample stored in a third party storage and verification server and transmitting the verification result to the computing device.