Claims

1. A base for supporting a miniature figurine, the base comprising an electronic device, the electronic device comprising:
a wireless communication system; and
a controller comprising:
at least one processor; and
memory storing data associated with the base and program instructions accessible by the at least one processor,
the electronic device being configured to:
transmit, to a content host, dynamically generated object data associated with the miniature figurine or another object, to enable the content host to determine content data that is associated with the dynamically generated object data, said content data comprising user interface data configured to be rendered for display on a display or user interface; and
wherein the dynamically generated object data is determined based on at least a) a UID of the miniature figurine or other object; b) an encryption key of the miniature figurine or other object; and c) a time at which the object data is transmitted.

2. A base as claimed in claim 1, wherein:
the base comprises a recess;
the electronic device is secured within the recess; and the electronic device comprises a NTAG® 424 DNA tag.

3. An adaptor that in use is secured to an underside of a miniature figurine, the adaptor comprising an electronic device, the electronic device comprising:
a wireless communication system; and
a controller comprising:
at least one processor; and
memory storing data associated with the adaptor and program instructions accessible by the at least one processor,
the electronic device being configured to:
transmit, to a content host, dynamically generated object data associated with the miniature figurine or another object, to enable the content host to determine content data that is associated with the dynamically generated object

data, said content data comprising user interface data configured to be rendered for display on a display or user interface; and

wherein the dynamically generated object data is determined based on at least a) a UID of the miniature figurine or other object; b) an encryption key of the miniature figurine or other object; and c) a time at which the object data is transmitted.

4. An adaptor as claimed in claim 3, wherein:

the adaptor comprises a recess;

the electronic device is secured within the recess; and the electronic device comprises a NTAG® 424 DNA tag.

5. A method comprising:

receiving, by a content host, dynamically generated object data from an electronic device, the dynamically generated object data being associated with an object;

determining, by the content host, content data that is associated with the dynamically generated object data, said content data comprising user interface data configured to be rendered for display on a display or user interface; and

transmitting the content data,

wherein the dynamically generated object data is determined based on at least a) a UID of the object; b) an encryption key of the object; and c) a time at which the object data is transmitted by the electronic device.

6. The method of claim 5, further comprising rendering at least part of said user interface data for display on the user interface, wherein:

the user interface comprises one or more of:

a first section that is configured to enable a user to view, add, remove and/or group UID-key pairs;

a second section that is configured to enable generation or selection of shortcodes;

a third section that is configured to enable restriction of access to one or more aspects of the user interface; and

a fourth section that is configured to enable backing up and restoration.

7. The method of claim 5 or 6, further comprising:

transmitting encryption data to the electronic device;

validating, by the electronic device, the encryption data; and

transmitting, by the electronic device, the dynamically generated object data, in response to the validation.

8. The method of claim 7, further comprising:

exchanging encryption data with the electronic device;

transmitting, by the electronic device, the dynamically generated object data, subsequent to the exchanging of the encryption data; and

validating the dynamically generated object data, wherein validating the dynamically generated object data comprises comparing the dynamically generated object data to validation data.

9. The method of any one of claims 5 to 8, wherein the dynamically generated object data comprises a shortcode.

10. The method of any one of claims 5 to 9, wherein:

the dynamically generated object data comprises one or more of:

the UID of the object;

the encryption key of the miniature figurine or other object;

data indicative of a character identity that is associated with the object;

data indicative of a character type that is associated with the object;

data indicative of a character status that is associated with the object;

equipment data that is associated with the object; and

data indicative of a skill that is associated with the object; and the content data is associated with one or more of:

a quest of a game;

a character arc of the game;

dialogue of the game; and

a sidequest of the game.

11. A content host comprising:

at least one processor; and

memory storing program instructions accessible by the at least one processor and configured to cause the at least one processor to:

receive dynamically generated object data that is associated with an object, said dynamically generated object data being determined based on at least a) a UID of the object; b) an encryption key of the object; and c) a time at which the object data is transmitted;

determine content data that is associated with the dynamically generated object data, said content data comprising user interface data configured to be rendered for display on a display or user interface; and

transmit the content data to a user interface system.

12. The content host of claim 11, wherein the program instructions are further configured to cause the at least one processor to validate the dynamically generated object data, wherein validating the dynamically generated object data comprises comparing the dynamically generated object data to validation data.

13. The content host of claim 11 or claim 12, wherein the dynamically generated object data comprises one or more of:

a shortcode;

a character type that is associated with the object;

a character identity that is associated with the object;

a character status that is associated with the object;

equipment data that is associated with the object; and

a skill that is associated with the object.

14. A system comprising:

the content host of any one of claims 11 to 13; and

an electronic device comprising:

a wireless communication system; and

controller comprising:

at least one controller processor; and

controller memory storing:

the dynamically generated object data; and

controller program instructions accessible by the at least one controller processor.

15. The system of claim 14, further comprising the object, wherein the object comprises:

the electronic device;

the base of claim 1 or 2; and/or

the adaptor of claim 3 or 4.

16. An authentication device for use with an object management system, the

authentication device being configured to enable access, by an electronic device of an object, to content data stored at a content host, the authentication device comprising:

a body housing an authentication electronic device;

a wireless communication system comprising an antenna configured to enable transmission and/or receipt of radio frequency (RF) signals to and/or from one or more of the electronic device and a communication device that is in communication with the content host;

an authentication controller comprising at least one processor and memory storing authentication controller data, wherein the authentication controller is configured to:

(i) secure a connection between the electronic device and the communication device;

(ii) sign authentication messages, on behalf of the electronic device of the object, via a communication network, thereby enabling the content host to associate content data with the object; and

(iii) receive user roles and permissions from the content host, and apply the user roles and permissions to control access to the content data.

17. An authentication device for use with an object management system, the authentication device comprising:

a body housing an authentication electronic device;

a wireless communication system comprising an antenna configured to enable transmission and/or receipt of radio frequency (RF) signals to and/or from one or more of the electronic device and a communication device that is in communication with a content host;

an authentication controller configured to:

(i) secure a connection between the electronic device and the communication device;

(ii) sign authentication messages, on behalf of the electronic device of the object, via a communication network; and

(iii) receive user roles and permissions from the content host.