Title: SELF PROVISIONING TOKEN

Abstract: The invention relates to authentication for online services and/or online content based on token based authentication, while using a portable device. The invention provides a system and method for token based authentication, without the need for a hardware token. The invention further provides a token based authentication system and method with a limited validity period for tokens, in order to provide a high level of protection against fraud.
Title
Self Provisioning Token

Field of the invention
The invention relates to authentication for online services and online content. More specifically, the invention relates to the downloading and paying for online content, the using and paying for online services and the offering of online content and services.

Furthermore, the invention relates to token based authentication for portable devices like mobile phones and handheld computers.

Background of the invention
Known authentication methods comprise, amongst others, user-password based authentication methods and hardware token based authentication methods. Hardware token based authentication based methods comprise e.g. a mobile phone SIM card and a key-ring based authentication method like the MacOSX Keychain or the Keystore concept of Java.

A hardware token may also be referred to as a security token, an authentication token or a cryptographic token. A hardware token is a physical device that an authorized user of online services and online content is given to aid in the authentication. Hardware tokens are typically small and often are designed to attach to the user's keychain. Hardware tokens may store cryptographic keys, such as a digital signature.

It is common knowledge that hardware token based authentication methods provide a better protection against fraud than user-password based methods. But hardware token based methods also have drawbacks. These drawbacks include, amongst others, more complexity for the end user because
the end user needs to install and manage a hardware token for each mobile device he is using. Another drawback of hardware token based methods is that the use of hardware tokens is strictly bound to the device to which the hardware token is directly connected.

**Problem definition**

Currently available hardware token based authentication methods have the disadvantage that a hardware token needs to be distributed and handed over per device. For users using a number of devices, this results in the distribution of the same number of hardware tokens.

Another disadvantage of hardware token based methods is that a single user of multiple mobile devices has to manage a number of hardware tokens in combination with a number of mobile devices.

Yet another disadvantage of hardware token based methods is that the use of hardware tokens adds a level of complexity to the operation of the mobile device, i.e. the hardware token needs to be "installed" and "maintained" at the mobile device, both in software and physically.

Furthermore, some types of hardware tokens can be "cloned" (i.e. copied), which can lead to fraud.

**Aim of the invention**

It is an object of the invention to eliminate the above-mentioned and other drawbacks of the prior art and to provide a system and method for token based authentication, without the need of a hardware token.
Summary of the invention

The present invention provides a system for authentication for online content and services by a mobile device, based on a self provisioning token.

According to an aspect of the invention, a mobile device comprises means that generates a code that is unique to the mobile device. The means generating a unique code can be provided in hardware or in software, or in a combination of hardware and software. The means generating a unique code is referred to as the self provisioning token SPT.

According to a further aspect of the invention, the generation of the code that is unique for the mobile device involves local hardware aspects. Local hardware aspects are e.g. a processor serial number, an Ethernet MAC address or the amount of memory installed in the mobile device.

According to an aspect of the invention, a unique code Z is generated and stored in memory, by applying a hash function to at least one local hardware aspect X and a cryptographic salt S, illustrated by the expression Z=hash(X,S). The hash function provides a way of creating a small digital "fingerprint" from the data read as the local hardware aspect. The hash function chops and mixes (i.e. substitutes or transposes) the data to create a fingerprint, often called a hash value. The salt is a non-public value or number stored in memory, used to modify the hash of the local hardware aspect. Preferably the location in memory of the salt is not public. The addition of the salt provides protection against a "brute force attack", i.e. the use of salt S in the hash function prohibits that the hash of local hardware aspect X can be reproduced, when the summary of local hardware aspects Z is read from the memory. "Known-hash attacks" will therefore be much more
difficult as a result of the use of salt $S$ in the generation of the summary of local hardware aspects $Z$.

Preferably at least two local hardware aspects and a salt are used in order to generate a unique code, illustrated by the expression $Z=\text{hash}(X,Y,S)$. The use of two local hardware aspects further improves the uniqueness of the summary of local hardware aspects $Z$.

According to an aspect of the invention, the summary of local hardware aspects $Z$, a user name $U$ and a password $P$ are sent to a provisioning server by the self provisioning token $SPT$ during a registration of a mobile device. A registration is needed to acquire a valid token (i.e. a device identifier $D$) for online authentication. A registration comprises a communication session between a mobile device and a provisioning server.

According to another aspect of the invention, the provisioning server performs at least one check based on username $U$, password $P$ or summary of local hardware aspects $Z$ and responds with a device identifier $D$ and a validity interval $T$.

By using a summary of local hardware aspects $Z$ during registration, the device identifier $D$ is related to the hardware of the registered device. As a result, authentication for online services and content, based on device identifier $D$, can be related to the hardware of the mobile device.

According to an aspect of the invention, the device identifier $D$ is valid for a limited time period. After the elapse of the time period, the registration is preferably performed again, whereby a new device identifier $D$ can be
provided, as explained above. In this way a high level of protection against fraud can be achieved. Especially when the device identifier D is compromised (i.e. "cloned"), the compromised device identifier D can only be used for a limited time period. This improves the protection level against fraud.

According to another aspect of the invention, the provisioning of the device identifier D by the provisioning server is denied as a result of a comparison of the summary of unique local hardware aspects Z with a previously stored value of Z at the provisioning server. In this way it can be verified if the hardware of the mobile device that is currently requesting a token is consistent with a previously known hardware configuration of the mobile device. This can also improve the level of protection against fraud.

Another advantage of the invention is that, by locking into existing unique local hardware aspects of the mobile device in which both the self provisioning token SPT and device identifier D are located, the self provisioning token SPT and device identifier D cannot be cloned (copied) without an effort which is at par with the value of the service consumption at risk. Furthermore, by using existing device properties the disadvantage of physical distribution and handover of hardware tokens is relieved.

As yet another advantage, an aspect of the current invention brings the opportunity to force the user to refresh the authentication token at a regular basis, to counter the risk of snooped authentication traffic.
Brief description of the drawings

The invention will be explained in greater detail by reference to drawings, in which:

Fig. 1 shows a schematic representation of a Provisioning Server and a Device during registration, in which a self provisioning token is generated.

Fig. 2 shows a schematic representation of authentication for online Services or Content, making use of a self provisioning token.

Detailed description of the invention

For the purpose of teaching of the invention, exemplary embodiments of the method and system of the invention are described in the sequel. It will be apparent to the person skilled in the art that other alternative and equivalent embodiments of the invention can be conceived and reduced to practice without departing from the true spirit of the invention, the scope of the invention being only limited by the claims as finally granted.

A system according to the invention makes it possible to use unique local hardware aspects of a mobile device as a basis for authentication to online services and online content such as online music, video on demand, internet TV, remote working, etc.

The mobile device can be any type of device used for online services and online content, like e.g. a mobile phone, palm computer, PDA or combined types like Blackberry and Hiptop. These devices are being used more and more for online services and online content. The service and content
providers protect their content e.g. through username-password protection, which is considered user-friendly but weak from a security point of view, or hardware token-based methods, which are considered as being strong from a security point of view, but less user friendly.

The current invention provides a solution to protect online services and content from unauthorized access by mobile devices, with a security level better than username-password authentication but more user friendly than hardware token-based authentication. For this purpose unique local hardware aspects of the mobile device are used during the provisioning of a device identifier D. The device identifier D serves as an authentication token, which is related to the hardware of the mobile device by which it is being used.

In an exemplary embodiment according to figure 1 the mobile device (10) connects with a provisioning server (20) via a network (30) in order to be registered. Registration can be started automatically or on initiative from the user. When registration is performed automatically, the trigger can be either that the mobile device (20) is new and therefore unregistered, or the device identifier D present in the mobile device can have become invalid, e.g. as a result of the elapse of the validity time.

During registration of a new device, the device is administrated in the User Profile (22) of the provisioning server, which contains information of the mobile device user U and is part of a user database (21). User U can be already known in the Provisioning Server at the time the registration starts and the username and password can have been sent to user U in advance. The mobile device contains
a software or hardware element SPT (11), which contains the functionality and routines to perform registration and authentication. Preferably SPT is isolated from user programs running on the mobile device. As a part of the hardware of the device, SPT can access hardware components, peripherals and memory present in the device.

As a first step during registration, unique local hardware aspects are gathered by SPT. As an example, these can be a microprocessor identification number, IP/Network peripheral MAC number, hardware serial/ID number, OS or software license or version number, harddisk serial number and/or amount of memory. But also other hardware related aspects that can be identified and read by programs or operating system can be used. Based on the gathered hardware information, a summary of the unique local hardware aspects, \( Z \), is generated. \( Z \) is a hash of at least one local hardware aspects \( X \) and a salt \( S \). Mathematically represented as \( Z=\text{hash}(X,S) \). Preferably \( Z \) is a hash of at least two local hardware aspects \( X \) and \( Y \) and a salt \( S \), to improve the uniqueness of \( Z \). In this case the mathematical representation is \( Z=\text{hash}(X,Y,S) \).

The unique local hardware aspect(s) used to generate \( Z \) is selected from the gathered local hardware aspects mentioned before, based on one or more of the following criteria:
- uniqueness;
- difficulty of spoofing;
- long term stability;
- reproducibility.

After generation, \( Z \) is stored in the user-profile-config (12).

Also a hash of \( X \) and \( Y \) (\( X' \) and \( Y^1 \)) are stored in the mobile device, as part of the user-profile-config (12). The
rationale of storing a hash instead of the original value of X and Y is the protection against brute force attacks on the device.

SPT also generates a timestamp T, which is for example a concatenated string of date and time down till milliseconds, like T=20051115095912269. U, P and T are stored in the user-profile-config (12).

After connecting with the Provisioning Server, preferably in a secure way (e.g. by using SSL), SPT sends the username U, password P, timestamp T and the summary of unique local hardware aspects Z to the provisioning server.

The provisioning server first checks username U and password P with the values stored in the user profile (22). If username and password are correct, then Z and T are added to the user profile (22). The provisioning server generates a device identifier D and a validity interval I and sends D and I to the mobile device. For example D is a randomly generated string of 16 bytes and I is a concatenated string of days (2 digits), hours (2 digits) and minutes (2 digits), like I=275959. SPT stores D and I in the user profile config (12) as token for authentication and validity interval. This concludes device registration and the mobile device can now access online services and online content, using D as a token in the authentication process.

In an exemplary embodiment according to figure 2, SPT authenticates the mobile device to an authentication server (40) of a content provider by sending U, P and D to the content provider. In addition to the checking of the username and password by the authentication server, the
authentication server verifies the validity of D via a connection to the provisioning server (20).

In another exemplary embodiment of the invention, the provisioning server and the authentication server are combined in 1 system.

In another exemplary embodiment, the device identification D has become invalid and the device needs to be re-registered. This can for example be triggered by the expiration of validity interval I in the device or the denial of access by means of D to by an authentication server. The re-registration can however also be triggered by the mobile device user.

To initiate re-registration, SPT firstly generates X, Y, Z and T in the same way as before and stores them in the user profile config (12). Before storing X' and Y', a check can be carried out to identify hardware changes. In case the new and stored values do not match, SPT can block itself from further operation.

Next, the device connects with the provisioning server and sends U, P, Z and T, as during previous registration. The provisioning server checks U and P and verifies Z with the previously stored value of Z in the user profile (22).

If the new and stored value of Z match, the provisioning server generates a new device identifier D and validity interval I and sends D and I to the device. SPT stores D and I in the user profile config (12). Online services and content can now again be accessed using D.
Claims

1. System for authentication for online content and services based on a self provisioning token by a device, whereby the self provisioning token is provided to the device after device registration involving unique local hardware aspects.

2. System according to claim 1, in which the self provisioning token is valid for a limited time period.

3. System according to claim 1 or 2, in which the provisioning of the self provisioning token by the provisioning server is denied as a result of a comparison of the unique local hardware aspects with stored information.

4. Device comprising a means for generating a code that is unique for said device.

5. Device according to claim 4, in which said code is stored in said device.

6. Device according to claim 4, in which said code is stored in said means.

7. Device according to any of claims 4 to 6, wherein local hardware aspects are stored in a memory.

8. Device according to claim 7, wherein said memory resides in said device.
9. Device according to claim 7, wherein said memory resides in said means.

10. Device according to any of the claims 4 to 9, wherein a salt is available in said device.

11. Device according to claim 10, wherein said salt is stored in memory.

12. Device according to claim 11, wherein said memory resides in said device.

13. Device according to claim 11, wherein said memory resides in said means.

14. Device according to claim 10, wherein a salt is available in said means.

15. Means designed to be connected to a device according to any of the claims 4 to 14, which when connected to said device, generates a code that is unique for said device.

16. Means according to claim 15, generating a code that is unique for the point in time at which said code is generated.

17. Means according to claim 15 or 16, using local hardware aspects for generating said code.

18. A computer program designed to be executed in a device, which when executed in said device, generates a code that is unique for said device.
19. A computer program according to claim 18, generating a code that is unique for the point in time at which said code is generated.

20. A computer program according to claim 18 or 19, using local hardware aspects for generating said code.

21. Method for generating a code that is unique for a device comprising the steps of:
- acquiring local hardware aspects;
- selecting the better one of said local hardware aspects, and indicating the better one as X;
- generating a timestamp T;
- acquiring a salt S from said device;
- generating said code as a result of the function \( Z = \text{hash}(X, S) \);
- storing in memory \( X' = \text{hash}(X) \) and Z.

22. Method for generating a code that is unique for a device comprising the steps of:
- acquiring local hardware aspects;
- selecting the better two of said local hardware aspects, and indicating the better two as X and Y;
- generating a timestamp T;
- acquiring a salt S from said device;
- generating said code as a result of the function \( Z = \text{hash}(X, Y, S) \);
- storing in memory \( X' = \text{hash}(X) \) and \( Y' = \text{hash}(Y) \) and Z.

23. Method for acquiring an authentication code to be used for online services, comprising the steps of:
- acquiring username U and password P from the device user;
- acquiring summary of local hardware aspects Z and
timestamp T from memory in said device;
- sending user name U, password P, summary of local hardware aspects Z and timestamp T to a provisioning server;
- receiving device identifier D and validity interval I from said provisioning server;
- storing D and I in memory of said device.

24. Authentication method for online services offered by an online Service Provider, comprising the steps of:
- acquiring username U and password P from the device user;
- acquiring device identifier D from memory in said device;
- sending U, P and D to the online Service Provider.

25. System that is capable of receiving a first code that is unique for a device and that responds by generating a second code that is unique to the device.

26. System according to claim 25 that responds with a second code that has a time limited validity.

27. System according to claim 26 that responds with a validity interval.