Untraceable Nym Creation on the Freedom 2.0 Network™

Russell Samuels
Ed Hawco
November 1, 2000

Version 2.0

This whitepaper, targeted at users with a basic understanding of Freedom™, describes the Freedom systems that prevent any association between purchasers of Freedom and their nyms[1]. It is primarily a review of the transactional processes involved in purchasing a nym, outlining possible lines of attack along with prevention mechanisms.

Introduction

One of the design goals in creating an infrastructure that provides pseudonymous Internet privacy is to create a system that allows consumers to create nyms without compromising their identities. Given the lack of an anonymous e-cash standard, the challenge is how to use proven payment mechanisms to ensure the transaction's fiscal integrity, yet ensure that a nym's owner is untraceable. This document describes such a system, as implemented on the Freedom 2.0 Network, managed by Zero-Knowledge Systems.

The basic building blocks of Freedom's untraceable nym creation system are activation codes[2] and nym tokens. Activation codes are akin to travelers cheques which are traceable to a given individual, while nym tokens are analogous to "Camel bucks" or any other store-specific currency which is untraceable because it includes no identifying information. Users obtain activation codes, convert those activation codes into untraceable nym tokens, and then use the nym tokens to anonymously purchase nyms.

The major components of Freedom's untraceable nym creation system consist of:

1. Credit card or cash payment mechanisms, which allow consumers to purchase premium services activation codes. Although cash-based mechanisms are untraceable, credit card mechanisms are not, as users must provide credit card and/or address information in order to purchase an activation code.

[1] For the 2.0 release there are two kinds of nyms—standard and premium. Standard nyms are free of charge, while premium nyms require the purchase of an activation code. This white paper describes the transaction system from the perspective of premium nyms, although the process is essentially the same for both. The main difference is the lack of a financial exchange for standard nyms.

[2] Previously known as "serial numbers".

© 2000 Zero-Knowledge Systems Inc. All rights reserved.

2. An untraceable currency subsystem, which allows consumers to convert traceable activation codes into untraceable nym tokens. Nym tokens are untraceable in the sense that it is impossible to associate any nym token with any IP address or with an individual who may have purchased an activation code.

3. The nym purchase subsystem, which permits untraceable nym tokens to be redeemed for nyms. This system allows nyms to be created or extended, and because it is based on nym tokens, it ensures that any nym cannot be associated with any particular identity or any other nym.

Together these components comprise an untraceable transaction system that prevents the association of user identity information with nyms that are created.

Payment Mechanisms

Freedom payment[3] mechanisms are designed to handle cash or credit card transactions for activation codes. The payment subsystem is designed so that it can be outsourced entirely without compromising a nym's privacy. A description of its processes and components follows.

Free Transactions

When a user installs the Freedom client software and chooses not to purchase premium services, an activation code is acquired in a background process that is transparent to the user. As there is no financial exchange, most of the traceability issues associated with nym creation are not present.

Credit-card Transactions

Most consumers who purchase a premium services activation code will do so through the Zero-Knowledge web store via a credit card. The entire purchase cycle transpires within an SSL channel to prevent anyone from listening in. However, the customer must submit his/her name, address, phone number, email address, and credit card number and expiry date. This information is then passed through third-party credit card transaction systems for fraud screening and transaction processing.

Customer information is retained by Zero-Knowledge for a period limited to 6 months (a legal liability requirement in the event of fraud) after which it is deleted. Information collected by Zero-Knowledge's transaction processing partner is maintained indefinitely (in case of fraud), but may not be shared with third parties not involved in the transaction. Information collected by credit card companies may be maintained indefinitely, and Zero-

[3] Activation codes for standard nyms are free. Users wishing to use Freedom premium services (for Freedom Mail and pseudonymous Internet privacy through the Freedom Network) pay for their activation codes.

© 2000 Zero-Knowledge Systems Inc. All rights reserved.

Knowledge has no control over how cardholders' transaction information is used. Effectively, the record of a purchase transaction should not be considered private.

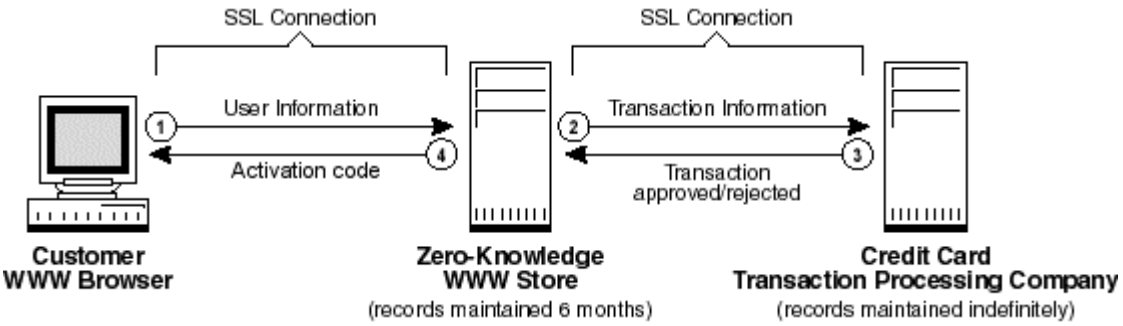

Figure 1: Standard credit card transaction

Once a transaction has been approved, Zero-Knowledge provides the customer with an activation code through the SSL connection, and logs the activation code (entitling the owner to free 1-800 support). Although purchasers' identifying information is available to Zero-Knowledge for 6 months, and potentially to others for a longer period of time, the system completely dissociates this information from nyms that are created, as explained later.

Note that customers who link to Zero-Knowledge's web site via a banner on a partner's web site are given a cookie or sent to a custom URL that allows Zero-Knowledge to compensate affiliate referrals. The only information that is stored or recorded in this cookie is an identification number for the referring web site. We believe that this is of little consequence from a privacy standpoint, since this information cannot be used for anything other than indicating that a user linked to Zero-Knowledge via a partner.

Cash Transactions

Consumers who wish to use Freedom's premium services yet completely avoid providing any identifying information to Zero-Knowledge or any associated transaction processing agents can do so via cash transactions.

The customer initiates a cash transaction via the Zero-Knowledge web store and is provided with a reference number that they send with cash to Zero-Knowledge in payment for an activation code. This reference number can then be used by the purchaser to verify whether the cash has been received by Zero-Knowledge, and if so, to download an activation code. As with credit card transactions, the web-based portion of the purchase cycle is SSL encrypted, including any query or response that includes the transaction reference number or the activation code itself.

© 2000 Zero-Knowledge Systems Inc. All rights reserved.

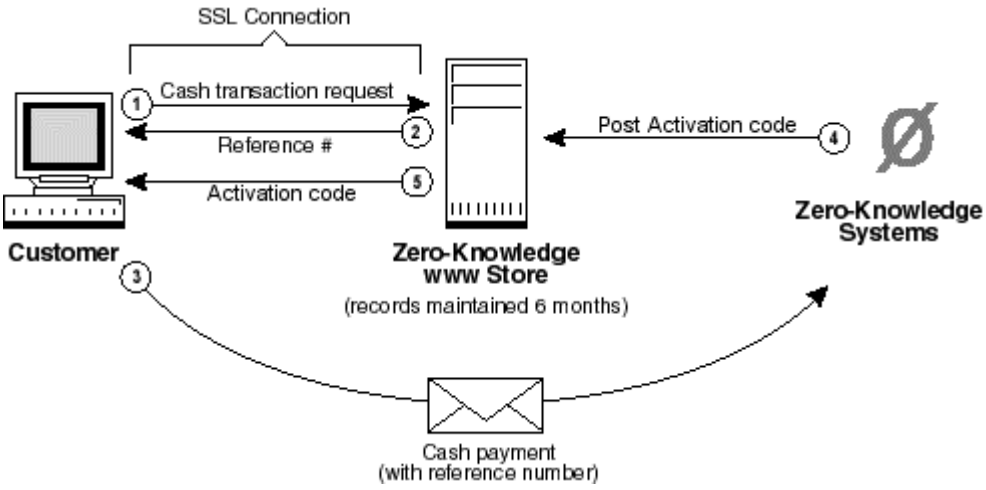

Figure 2: Standard cash transaction

Future plans include the ability to purchase activation codes in person via a cash transaction through third-party distributors, retail stores, or a trade show booth. These avenues could provide a similar level of confidence by preventing any association between the customer and the activation code.

The Untraceable Currency Subsystem

Activation codes and nym tokens form the basis of Freedom's untraceable currency system which dissociates customers' identity from the 'currency' (nym tokens) that is eventually used to create or extend a nym. This section describes its processes and components.

Activation Code Distribution

Activation codes are analogous to traveller's cheques that are purchased by a user, in the sense that they may be associated with specific transactions or specific individuals. They are randomly generated 60-bit numbers, followed by a 10-bit checksum, represented as a 14-character alphanumeric string.

Activation codes are generated offline by an activation code generator, which, at a Zero-Knowledge operator's request, creates a specified number of unique[4] activation codes. Each activation code is associated with a set of capabilities, describing its value, that is stored along with the activation code in a database:

[4] All activation codes ever generated are stored on the activation code generator to prevent the generation of duplicates.

© 2000 Zero-Knowledge Systems Inc. All rights reserved.

Activation Code Capability Code	
Fields	**Description**
Activation code Type	Activation code SKU (stock keeping unit). Every different type of activation code is assigned a particular identifier.
Token Count	Number of nym tokens associated with the activation code. For instance a premium service activation code might be redeemable for five nym tokens, while a standard activation code might only be redeemable for three.
Token Type	The type of nym tokens associated with the activation code. Different token types have different values (as described later), and activation codes may be redeemed only for the specific type of nym token described in this field.
Activation Date	The date at which the activation code becomes active in the activation code Database. This field is used primarily to ease the burden of provisioning activation codes by allowing them to be 'post-dated'.
ID	This field identifies the data as an activation code capability code.
Version	Indicates the version of the capability code.

Activation codes, in and of themselves, are worthless--it is only at a later time when they are 'activated' in the activation code database that they become negotiable. Once created, each activation code and its associated capability set are transferred by a Zero-Knowledge operator into the activation code database which maintains a record of all activation codes and their associated redemption values. Once the activation code 'Activation Date' has passed, they become negotiable and can be exchanged for nym tokens. At this point, activation codes can be securely transferred to a web-based store operating under payment policies such as those described earlier, or alternatively, to any other distribution channel.

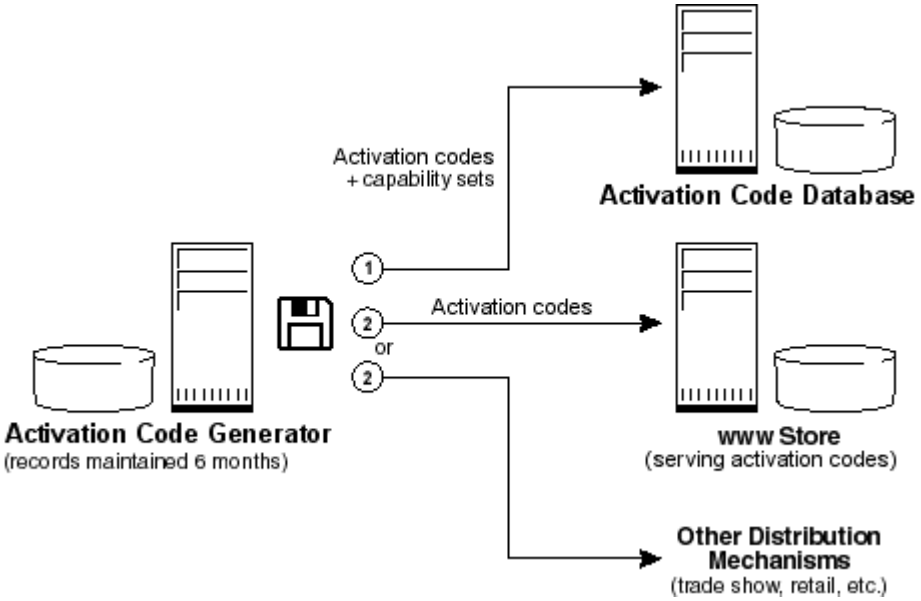

Figure 3: Activation code distribution

© 2000 Zero-Knowledge Systems Inc. All rights reserved.

Nym Token Distribution

Once an activation code is active, it can be redeemed for nym tokens via the Freedom client. These tokens are analogous to untraceable currency, albeit currency whose purchasing power is limited to Freedom nyms. The nym tokens are represented as 256 byte large binary data blocks that embed the following key information:

Token Structure	
Token Parameter	**Description**
Token Type	The Token type field determines the capabilities that are imbued to a nym by the token when it is used to create or extend a nym. The number of token types is strictly limited so as to prevent correlation between nym properties and a particular set of customers.
Token Number	This is a 128-byte random number that identifies the nym token. It uniquely identifies tokens so as to prevent them from being used on multiple occasions.
Owner	This identifies the token server that created the nym token.
Signature	This is the signature for the particular nym token, based on the token server's private key. It is used to verify the authenticity of a token when a customer attempts to use it to purchase a nym.
ID	This parameter is used to identify the datablock as a token.
Version	Indicates the version of the token datablock.
Size	Total number of bytes.
Reserved	Reserved for future use.

Once a user has been allocated an activation code, redeeming it is simply a matter of running the Freedom client and choosing to redeem[5] an activation code. This results in the creation of an unauthenticated anonymous route[6] between the client and the token server (responsible for token distribution), which in response to a command from the client, validates the submitted activation code against the activation code database and updates the database to indicate that the activation code has been used.

The token server then submits nym tokens to the Freedom client in the quantity and of the type associated with that activation code. Every token is based on a random token number, uncorrelated to any other. In addition, the token server does not record token transactions--token integrity verification is based completely on the token's digital signature, so there is no possibility for an attacker to map tokens to activation codes. Finally, because all interaction between the Freedom client and the token server is over an anonymous route, no part of the transaction can be observed by a third-party, and no one, including Zero-Knowledge, is able to verify the source IP address of the Freedom

[5] For standard nyms, activation code redemption occurs automatically.

[6] This is a connection in which the source IP address is hidden, and all communications are encrypted. For details, see the Freedom white papers: *Freedom Architecture* and *Freedom Architecture and Protocols*.

© 2000 Zero-Knowledge Systems Inc. All rights reserved.

client. These mechanisms combine to eliminate direct correlation between identity and tokens.

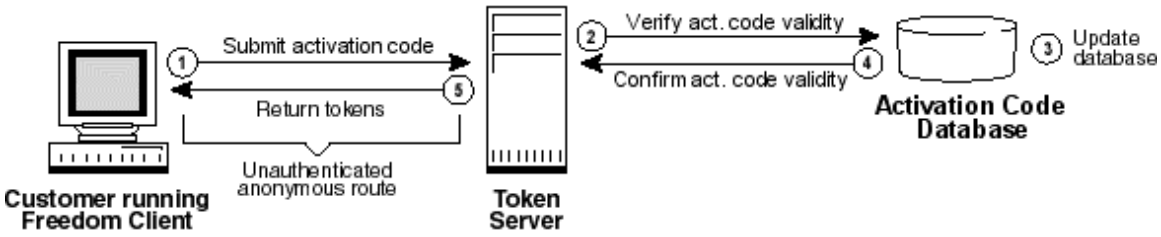

Figure 4: Nym token distribution

Nym Purchase System

The Nym Purchase System is the final step of the anonymous transaction, resulting in the creation or extension of a nym.

When a user's Freedom client receives a nym token, the redemption value of the token depends on its token type. This redemption value is determined by a configuration file that is maintained by Zero-Knowledge on what is known as the nym server. This configuration file sets the following descriptors for each token type:

Nym Server Token Type Descriptors	
Token Type Descriptor	**Description of Resultant Nym Capability.**
Duration	The lifespan of a nym.
Grace Period	The period after nym expiry for which the nym is reserved for its original owner.
Nym Type	The access level available to the nym into the Freedom Network.
E-mail Domain	The e-mail domain to be given to the nym.
E-mail Limit	The maximum number of recipients to which e-mail can be sent per day.
Creation Flags	Describes whether the token can be used to create and/or upgrade a nym.
Maximum Life	The maximum Life of a nym at any point in time.
Cross Post Limit	The maximum number of newsgroup cross posts.

When a user attempts to convert nym tokens into nyms, the Freedom client establishes an unauthenticated anonymous route over the Freedom network to the nym server so as to conceal and anonymize communication. A command is issued by the client and the token is submitted to the nym server which then authenticates or rejects the token's signature, verifies that the token hasn't previously been used, and, if valid, creates a nym with properties based on the token type, storing its attributes in the nym database[7]. Once

[7] The nym database is described in the Freedom white paper: *Freedom System 2.0 Architecture* .

© 2000 Zero-Knowledge Systems Inc. All rights reserved.

the nym has been created, a hash of the token is added to the spent token database, which is used to prevent tokens from being used on multiple occasions.

And thus, a nym is born.

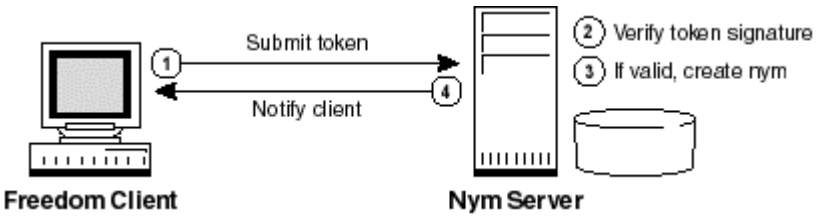

Figure 5: Nym creation or extension

Trust No One

Freedom's untraceable currency system prevents association between a nym purchaser and the nym purchased. However, as with any system there is the potential for compromise through various attacks. For those who wish to reduce this possibility, this section describes potential attacks, and where possible, methods to mitigate them.

Several minor weaknesses relate to the security of the cash payment system. First, Zero-Knowledge must be trusted to not monitor/store customers' IP addresses since that could potentially lead to the determination of a purchaser's identity. To mitigate this risk, customers can access the site via a public Internet terminal. A second risk to this system is that although cash-based transactions transfer no user information, they are vulnerable to physical interception and analysis.

For example, an attacker (or Zero-Knowledge for that matter) could intercept envelopes, and perform DNA or fingerprint analysis on an envelope to determine the identity of individuals purchasing Freedom. This can be mitigated through careful handling of the envelope. Both of these attacks simply reduce the added protection of a cash transaction, but do not compromise the user's privacy, since they can't associate the identity with any particular nym. They effectively reduce the level of security closer to that of purchasing an activation code with a credit card.

Another system deficiency is that users must trust Zero-Knowledge to not record any association between activation codes and nym tokens, due to the fact that the system uses untraceable processes rather than blinding cryptographic mechanisms. This document should assuage those concerns through its description of the token server and the fact that it creates tokens randomly, providing them directly to the Freedom client without ever recording any specific token information until after a token has been redeemed. In addition, purchasing Freedom from a venue such as a retail store or trade show floor would eliminate this concern by limiting any association between purchaser and activation code.

© 2000 Zero-Knowledge Systems Inc. All rights reserved.

The most significant weakness of the system is that it can be vulnerable to correlational analysis targeted at associating activation code downloads with nym creation. For example, if an attacker were able to determine that a user purchased 'something' at the Freedom premium services price from Zero-Knowledge on a particular date, and a warrant were issued to examine the date that a particular nym was created in Zero-Knowledge's nym database, it would be possible to correlate the two. This is especially true if there are a limited number of nyms created on any particular date, and if activation code redemption and nym creation/extension coincide with the date the activation code was purchased. To mitigate this risk, it is recommended that users not create or extend a nym on the date an activation code is purchased.

Conclusion

To summarize, premium nym creation or extension on the Freedom Network is designed to be untraceable, brought about by the mechanisms described in this document. As with all components of the Freedom Network, continual refinement of process and components will result in continually improved privacy. For example, Zero-Knowledge is actively investigating the use of alternative mechanisms such as anonymous private e-cash. We welcome your suggestions and ideas for the improvement of this system.

© 2000 Zero-Knowledge Systems Inc. All rights reserved.