RememberMe with rolling tokens

Why is it that I cannot find a definition of a rolling authentication token anywhere? Let me provide my own then: *a rolling token is a security (authentication) token that can only be used for a single successful authentication. After a successful authentication, the used token is always replaced by a new one, therefore the token is said to be rolling*. There, now we can talk. I've always disliked typical rememberMe implementations for the weak security they provide and I still admire this eight year old blog post by Charles Miller. Let me quote from "Persistent Login Cookie Best Practice":

Persistent login cookies are the cookies that are stored with your browser when you click the "remember me" button on the login form. I would like to be able to say that such cookies are obselete, and we have a better way of handling user logins, but they aren't, and we don't.

The following recipe for persistent cookies requires no crypto more powerful than a good random number generator.

Premises

1. *Cookies are vulnerable. Between common browser cookie-theft vulnerabilities and cross-site scripting attacks, we must accept that cookies are not safe*
2. *Persistent login cookies are on their own sufficient authentication to access a website. They are the equivalent of both a valid username and password rolled into one*
3. *Users reuse passwords. Hence, any login cookie from which you can recover the user's password holds significantly more potential for harm than one from which you can not*
4. *Binding persistent cookies to a particular IP address makes them not particularly persistent in many common cases*
5. *A user may wish to have persistent cookies on multiple web browsers on different machines simultaneously*

With all this in mind, I've always implemented rememberMe based on rolling tokens in the various web applications I've worked on. However, I've never attempted to provide it as a reusable module until one day a few months ago while I was working on federatedaccounts it hit me: rolling tokens can be thought of as just another "remote" authentication provider that can be federated with the main account. For some months now, we've happily been using tynamo-federatedaccounts-rollingtokens in production. I added some quick documentation for it at the end of the generic tynamo-federatedaccounts guide, have (secure) fun with it!