The World's Most Secure Dating Site

A showcase for the Eccentric Authentication protocol.

An example on what you can gain when you **leave passwords behind**
and use Public Key Cryptography instead..

The dating site allows users to sign up with just a nickname and a public key. At registration users receive a certificate from the sites' own Local Certificate Authority. It binds the nickname and the users' public key together. In other words, it creates a verifiable identity at the site.

It gives our users:

- **Full anonymity**, we don't know who our users are; even after signing their certificate;
- **Full control over privacy**: the user decides when to reveal his real identity and to whom; If he wants to divulge his real name at all;
- Control of his online **reputation** based solely on the nickname;
- **Private communication with other members on our site**; not even we can read the messages; The user agent encrypts all private communication with the public key of the recipient before submitting to the server. Only the recipients' private key can decrypt it.

We, site operators:

- Sign each user's certificate request as long as the **nickname is unique** to us;
- Can build a **relationship** with our users, even though they are **anonymous**;
- Can ask for payment for our service; ask to deposit money tagged with the nickname; completely anonymous when using bitcoin;
- Block a user when he's misbehaving; just blacklist the certificate until it expires;
- If we would be hacked, there is **nothing to learn about our users**;
  - our users' public data is already on the web site;
  - all our users' private data is encrypted with the public keys before they submit it;
  - there are no email addresses nor password to steal;
- We run the site on commodity rented servers and can offer full privacy guarantees!

The trust comes from Eccentric Authentication:

- DANE/TLSA to distribute our servers' certificate through DNSSEC; no more MITM;
- RSA private/public key pairs and certificates; for authentication and secure messaging;
- User's nickname becomes an addressable identity: eg: *CaptainKurk @@dating.wtmnd.nl*
  - Write it on a business card, strangers can type in the name; validate the certificate and:
  - **communicate securely with total strangers** without prior key exchange.

Demo: https://dating.wtmnd.nl:10443/
Background: https://www.witmond.nl/

Contact: Guido Witmond <guido@witmond.nl> Phone: +31 10 737 1161 (UTC +1. Amsterdam)

It's not the size of the key that matters; It's how you use it.