

A use case for DNSSEC

Phishing Protection

By Guido Witmond

<http://eccentric-authentication.org>

Phishing

- Phishing is the art of deception:
 - Humans are targeted;
 - The site you're on is not what you expect!
 - It looks like your bank, but it's a fake.
 - Computers offer no protection.
- Our goal: Let the computer protect its user.

HTTPS / TLS / SSL

- We need HTTPS
 - It encrypts the connection against tampering;
 - It helps to identify the site;
 - And the green address bar gives confidence.
- We have a problem
 - Which CA to choose?

Choose a CA

- There are 160 of them
 - Each of those is good for a green bar;
 - Give 'em your money, get a certificate;
 - If one refuses, try another.
- Agony of choice isn't the problem
 - Any CA can sign any certificate for any site;
 - Criminals can get one for your bank;
 - With stolen credit cards and fake passports.

The CA problem

- Who is the CA of your bank?
 - How would you know?
 - How often do you check?
 - If the address bar is green, it's OK, isn't it?
- The core problem is this:
 - **Users won't know which is the expected CA for a given domain name.**

DNSSEC to the rescue

- Cue the music: DNSSEC to the rescue
- DANE: DNSSEC Authenticated Naming of Entities:
- **DANE specifies which is the expected CA for a given domain name.**
 - It solves a long standing problem:
The missing link between domain name and Certificate;
- It opens doors to new possibilities

DANE usage

- Site creates a DANE / TLSA record:
 - TLSA specifies the TLS-Anchor,
i.e. the CA that signs the server certificate;
 - It tells the user what to expect.
- Browser fetches the TLSA-record;
 - It verifies the DNSSEC-chain to ICANN Root;
 - It connects to the site;
 - And validates the actual server certificate against the record from the TLSA-record.

CA problem solved

- With DANE, the CA problem is solved
 - Almost for free: just publish the TLSA-record in your DNSSEC secured DNS-zone.
- Now you can choose a CA based on real criteria:
 - Their reputation; policies, support, etc.
- It protects users who opt in to check the TLSA-record and validate the DNSSEC chain.
- Others are out of luck. i.e. Diginotar'ed.

It's not enough against Phishing

- Scammers set up a DANE-protected fake site:
 - It looks just like your bank;
 - They lure you to it with a scary email;
 - To make you type your username and password.
- There lies the problem:

Users managing their own passwords.

Let's do better

- Users could deploy a password manager:
 - It manages all accounts and passwords;
 - It does the sign-up, log-in and log-out;
 - It has buttons for these operations.
- The manager remembers which accounts a user has at each site.
- The user decides what to do, i.e. sign-up, log in, log out: the manager makes it happen.

Password manager does DNSSEC

- When the user presses the 'Log In'-button:
 - The manager validates the DNSSEC chain
 - It validates the server certificate against DANE
 - It shows which accounts it has for that site;
 - And lets the user choose one;
 - Only then it presents the password at the site.
- You don't have to remember your passwords;
Nor type them in.
- Your agent does the work for you.

This makes phishing difficult

- Here's how:
 - While scammers can copy the looks of a site;
 - They can't fake the domain name;
 - They have to use their own domain name;
 - To the password manager, that is a new site:
 - It helpfully offers to create a new account and password.
- This should wake people up.
 - “Where is my password for the bank?”
 - “It was here yesterday.”

A really scared user ...

- Suppose, our user is really scared and doesn't take 'No' from the manager; they'll do anything:
 - Open the manager to get the password;
 - And happily give it to the bank scammers.
- Password Manager should not allow that
 - It should never reveal passwords to its user;
 - Best to deploy a cryptographic zero-knowledge proof.

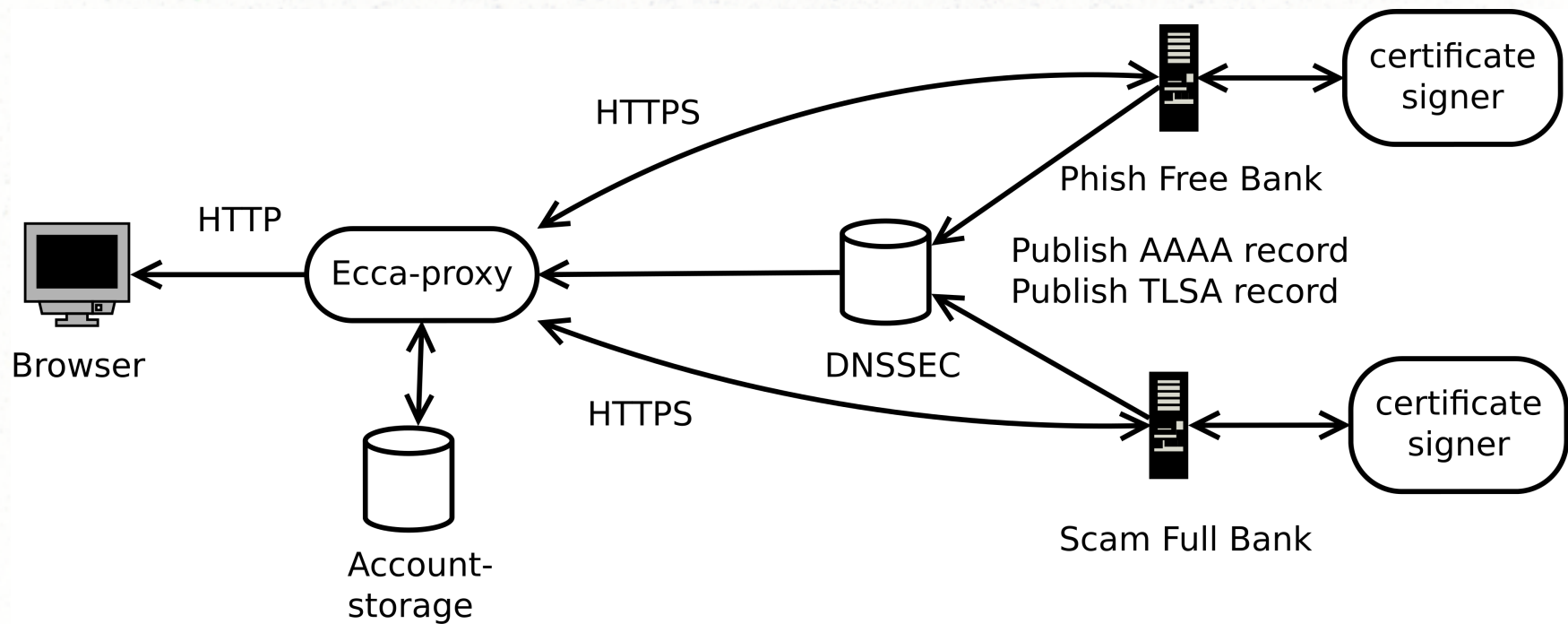
Almost there

- Users have multiple devices;
 - The password manager could use synchronising;
- Use a master password / facial scan / fingerprint to protect the password store.
- Malware is still a threat:
 - Use malware-resistant OS (Qubes, Genode, Minix)
We need these!

Demo

- Using client certificates instead of passwords
 - It's a zero knowledge proof;
 - Webservers already know how to deal with it;
 - It's easier to program too.
- We have a user agent to request certificates;
 - And a server side component to sign these.
- Each site signs their own client certificates;
 - And only accepts their own.

Demo network



http://www.ph...mnd.nl:1443/



www.phishfreebank.wtmnd.nl:1443



Wikipedia (nl)



Home

Open Account

Show Transactions

Phish-Free-Bank

Phish-Free-Bank is a bank like any other, your money is safe with us. Trust us.

Unlike every other bank: *we protect you against Phishing!*

To give you that protection we ask you to use the [ecca-proxy](#) on your computer. Please install it and enjoy our superb protection.

Background reading

Please read: [Announcing Eccentric Authentication](#).

With regards, Guido Witmond.

Feel free to mail: [guido @ witmond.nl](mailto:guido@witmond.nl).

www.phishfreebank.wtmnd.nl:1443/open-account-info

http://www.ph...-account-info



www.phishfreebank.wtmnd.nl:1443/open-account-info



Wikipedia (nl)



Home

Open Account

Show Transactions

Open account

Thank you for choosing Phish-Free-Bank.

To open the account, please create your credentials. That could be First.LastName, or just a random selected name.

You create it in your ecca-proxy. Click [here](#).

www.phishfreebank.wtmnd.nl:1443/open-account

http://ecca.h...Fopen-account +



ecca.handler/select?originalRequest=https%3A%2F

Wikipedia (nl)



401 - Eccentric Authentication required

Please select one of these identities -none-

Or create a new one

Or register anonymously:

http://ecca.h...Fopen-account



ecca.handler/select?originalRequest=https%3A%2F%2F

Wikipedia (nl)



Ecca Proxy. You are logged in www.phishfreebank.wtmnd.nl:1443 with Guido. Press here to logout:

[Log out of www.phishfreebank.wtmnd.nl:1443](#)

Click here to go to the [management page](#) of the proxy

Home

Open Account

Show Transactions

Account opened

Welcome Guido@@PhishFree.wtmnd.nl. We have opened your account.

Your account number is 12.

We have deposited our welcome bonus of 25 Florins into your account. Aren't we generous?

With regards, ~~Sharks~~Management of PhishFreeBank.

http://ecca.h...Fopen-account



ecca.handler/select?originalRequest=https%3A%2F%2F



Wikipedia (nl)



Ecca Proxy. You are logged in [www.phishfreebank.wtmnd.nl:1443](#) with Guido. Press here to logout:

[Log out of www.phishfreebank.wtmnd.nl:1443](#)

Click here to go to the [management page](#) of the proxy

Home

Open Account

Show Transactions

Transactions

Customer: Guido@@PhishFree.wtmnd.nl

Account number: 12

Recent transactions

Date	From	To	Comment	Amount
2014-06-22 14:55	1	12	Welcome bonus	25

http://ecca.ha...-transactions



ecca.handler/select?originalRequest=https%3A%2F%2F



Wikipedia (nl)



401 - Eccentric Authentication required

Please select one of these identities [Guido](#)

Or create a new one

[Register this name](#)

Or register anonymously: [Anonymous](#)

http://ecca.ha...-transactions



ecca.handler/select?originalRequest=https%3A%2F%2F



Wikipedia (nl)



Ecca Proxy. You are logged in [www.phishfreebank.wtmnd.nl:1443](#) with Guido. Press here to logout:

[Log out of www.phishfreebank.wtmnd.nl:1443](#)

Click here to go to the [management page](#) of the proxy

Home

Open Account

Show Transactions

Transactions

Customer: Guido@@PhishFree.wtmnd.nl

Account number: 12

Recent transactions

Date	From	To	Comment	Amount
2014-06-22 14:55	1	12	Welcome bonus	25
2014-06-22 15:00	12	1	Banking fee	-10
2014-06-24	12	2	Rent	-100

The fatal email

- From: customer-support@phishfreebank

Dear Customer,

- We have a transaction waiting, please log in to allow or prevent the 1.500,- florins from being deducted.
- Click here: phishfreebank
(scamfullbank.wtmnd.nl)

http://www.sc...tmnd.nl:1666/



www.scamfullbank.wtmnd.nl:1666



W Wikipedia (nl)



Home

Open Account

Show Transactions

Phish-Free-Bank

Phish-Free-Bank is a bank like any other, your money is safe with us. Trust us.

Unlike every other bank: *we protect you against Phishing!*

To give you that protection we ask you to use the [ecca-proxy](#) on your computer. Please install it and enjoy our superb protection.

Background reading

Please read: [Announcing Eccentric Authentication](#).

With regards, Guido Witmond.

Feel free to mail: [guido @ witmond.nl](mailto:guido@witmond.nl).

http://ecca.ha...-transactions



ecca.handler/select?originalRequest=https%3A%2F%2F



Wikipedia (nl)



401 - Eccentric Authentication required

Please select one of these identities -none-

Or create a new one

Register this name

Or register anonymously:

Anonymous

http://ecca.ha...-transactions



ecca.handler/select?originalRequest=https%3A%2F%2F



Wikipedia (nl)



401 - Eccentric Authentication required

Please select one of these identities -none-

Or create a new one

Or register anonymously:

http://ecca.ha...-transactions



ecca.handler/select?originalRequest=https%3A%2F%2F



Wikipedia (nl)



Ecca Proxy. You are logged in [www.scamfullbank.wtmnd.nl:1666](#) with Guido. Press here to logout:

[Log out of www.scamfullbank.wtmnd.nl:1666](#)

Click here to go to the [management page](#) of the proxy

Home

Open Account

Show Transactions

Transactions

Customer: Guido@@ScamFull.wtmnd.nl

Account number: 2

Recent transactions

Date	From	To	Comment	Amount
2014-06-21 10:46	1	2	Welcome bonus	25



Manage your Eccentric Authentication logins

Current logins

These are your current logins.

Host	Account	Action
www.scamfullbank.wtmnd.nl:1666	Guido	Log out of www.scamfullbank.wtmnd.nl:1666

All your accounts at hosts

These are all your accounts we have private keys for.

You can log in to any. Just click on the host name to get there anonymously.

You'll get to choose the account when the sites asks for one.

Host	Accounts	Show full certificate
www.phishfreebank.wtmnd.nl:1443	Guido	show Guido
www.scamfullbank.wtmnd.nl:1666	Guido	show Guido

Conclusion

- DNSSEC is good!
- It paved the way for DANE;
 - Together, these form a killer app.
- With a different way of account management,
 - Get rid of remote passwords;
 - Let the computer manage accounts:
- Phishing can be reduced tremendously
 - The computer distinguishes friend from foe.

Questions

- Questions ...?