PKI homework

1. Obtain a certificate

- You can get a free one from StartSSL – These are generic certificates for all purposes.
- You can get a test certificate from Microsec here – You can get separate certs for encryption/authentication/signature, these chain to a non-production root and have a "Test" prefix in the common name.
- You can generate a keypair and create a self-signed CA, and use this CA to issue a certificate for yourself. Please find info for starting here or here.

2. Send me (istvan@berta.hu) a signed and encrypted mail

I will be sharing my encryption certificate.

3. Create a CA for yourself

Recommendation: Use openSSL.

1. Issue a certificate to yourself. Issue a certificate to another team member.
2. Optional: Issue a CRL and revoke the other student's certificate.
    a. Note: You will need to ensure that the CRL can be found by the software verifying the certificate. The CRL should be on the Internet, and should be referenced by the CRL Distribution Point Ext of the certificate.
3. Cross-certify another students CA.
4. Check a signature from the other student (chaining to his/her) CA via your root.
5. Optional: Revoke the cross-certificate. Check the signature again.

Send me the certificates/chains and screenshots in a zip file via e-mail.

4. Send me a PDF with visible signature (based on certificate)

- You can use Acrobat Reader for creating the signature.
- You can also use the e-Szigno software.

Optional: Send me a time stamped signature

- The Microsec test timestamping service can be accessed with these credentials.
- Feel free to use any other timestamping source. Feel free to set up your own (via OpenSSL).

This homework is due by the 29th of March (last day of Easter holiday).