AUÐKENNI

Tæknin á bakvið PKI-IS

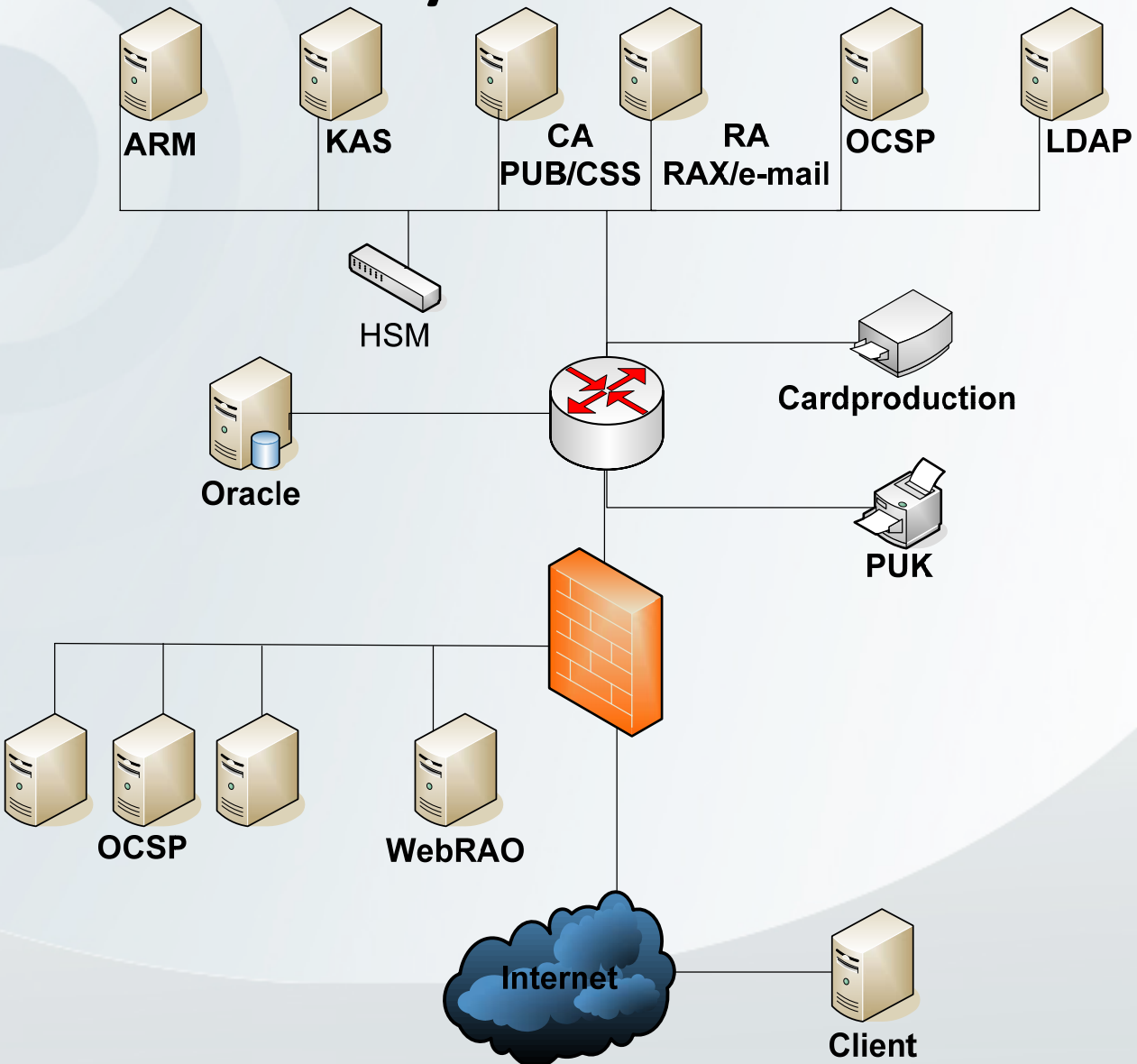
Kristinn Stefánsson , Kaupþing

Sverrir Bergþór Sverrisson, Auðkenni

Yfirlit

- Inngangur
- Kerfið og uppbygging
- Tæknin gagnvart notanda
- Uppsetningar
- Forritun

Yfirlitsmynd af kerfinu.



Tæknin gagnvart notanda

- Notandi fær í hendurnar
  - Debetkort með greiðsluvirkni og skilríkjum
  - Kortalesara (USB)
  - Notandahugbúnað (Personal).
  - Notandi velur sér PIN.
    - Auðkenningar PIN
    - Undirritunar PIN

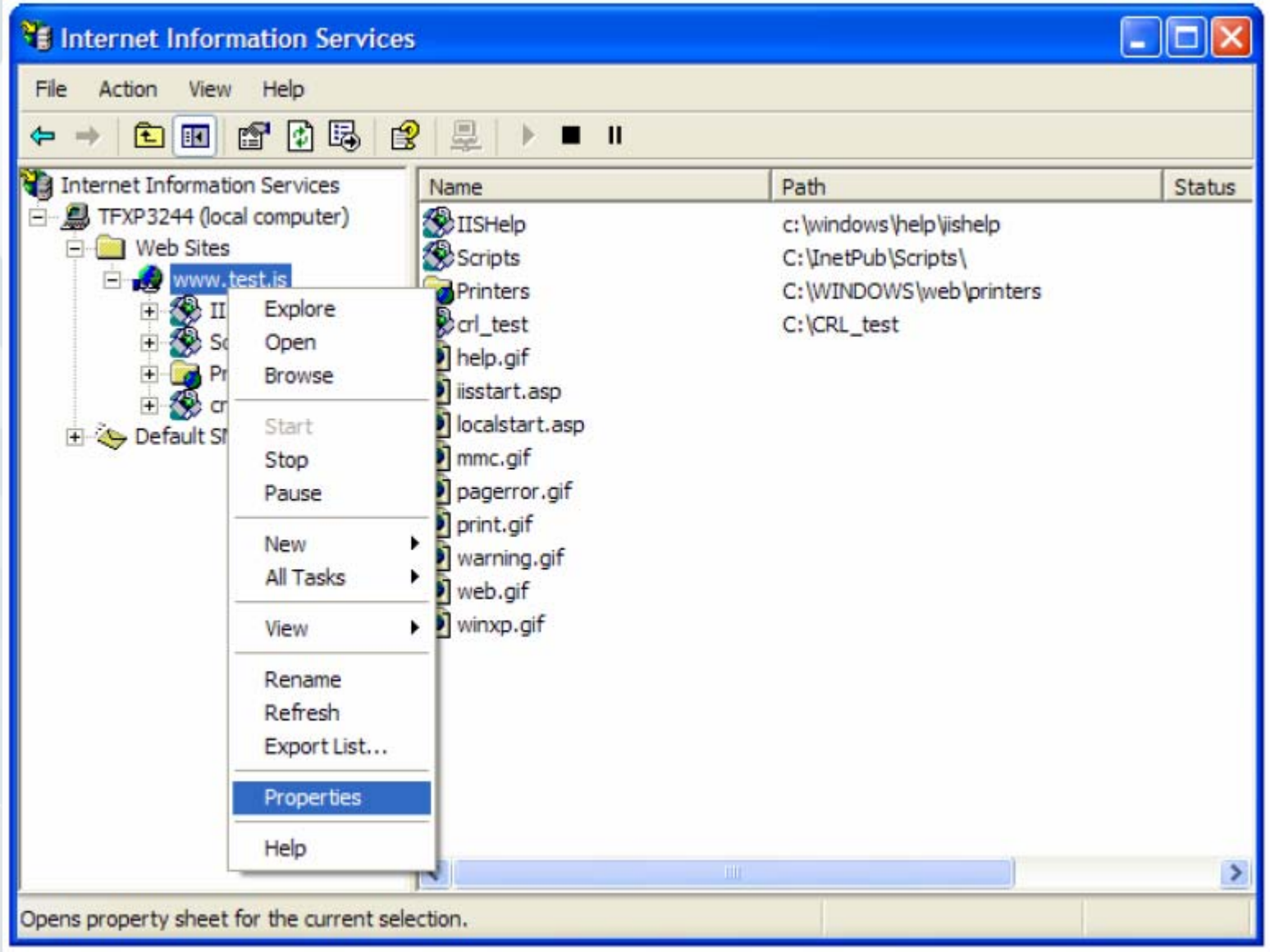
Tæknin gagnvart notanda

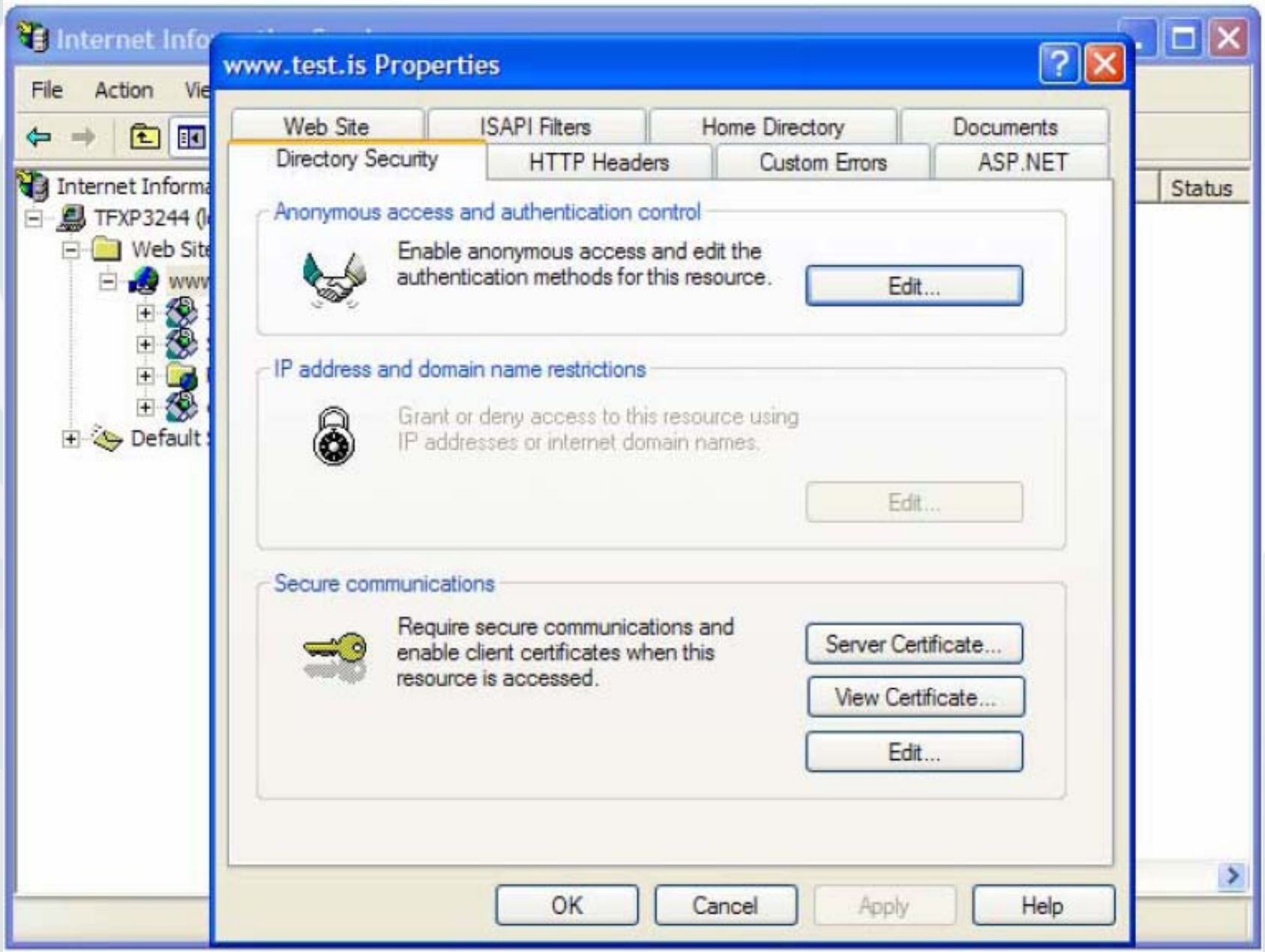
- Uppsetning á vél notanda.
  - Notandahugbúnaður settur upp – Nexus Personal.
    - Einfalt ferli
    - Útgáfur fyrir Windows og MAC.
    - Hægt að nota MAC intel útg. fyrir Linux
  - Lesari tengdur við tölvu
    - Reklar frá Windows update fyrir Windows.
    - Reklar fyrir MAC og Linux frá framleiðanda.

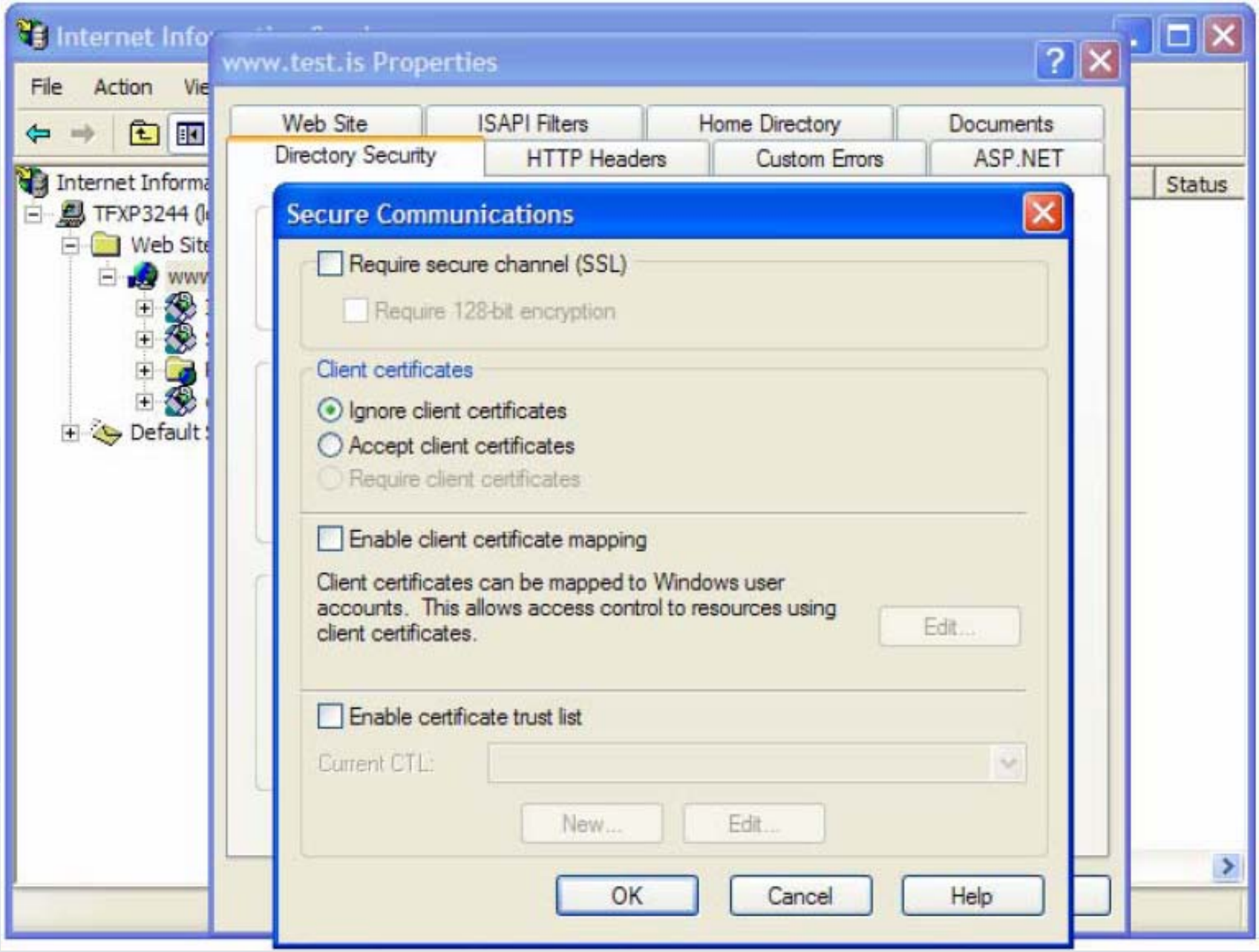
Hvernig nýti ég skilríkin?

- Netþjónn þarf SSL skilríki
- Skilríkjakeðju Íslandsrótar
  - Public rótarskilríki Íslandsrótar
  - Public milliskilríki Auðkennis
  - Public milliskilríki Fjármálaráðuneytis
- Heimila aðgang skilríkja inn á vefþjón
- „Smá“ forritun

Stillingar á Microsoft IIS.

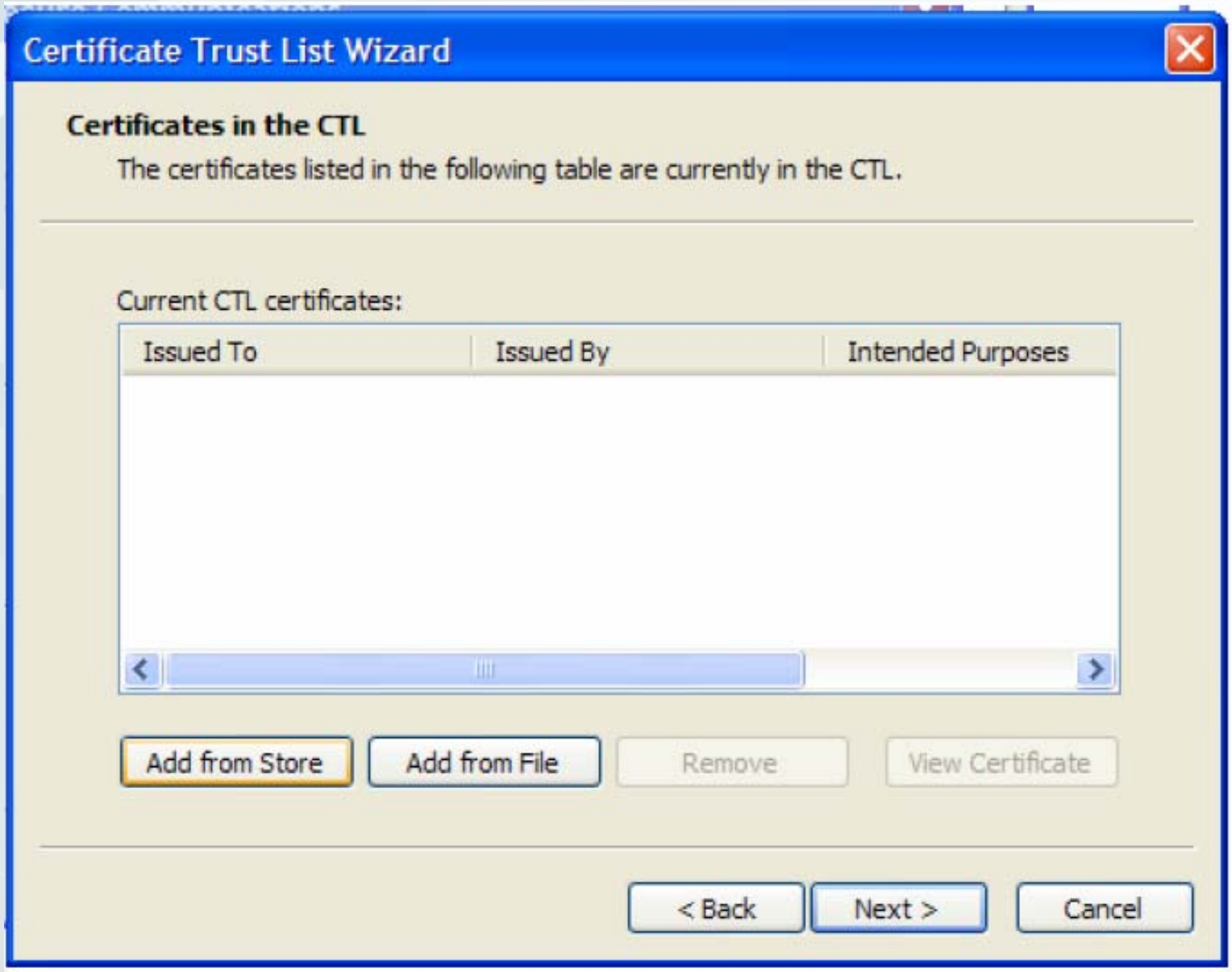


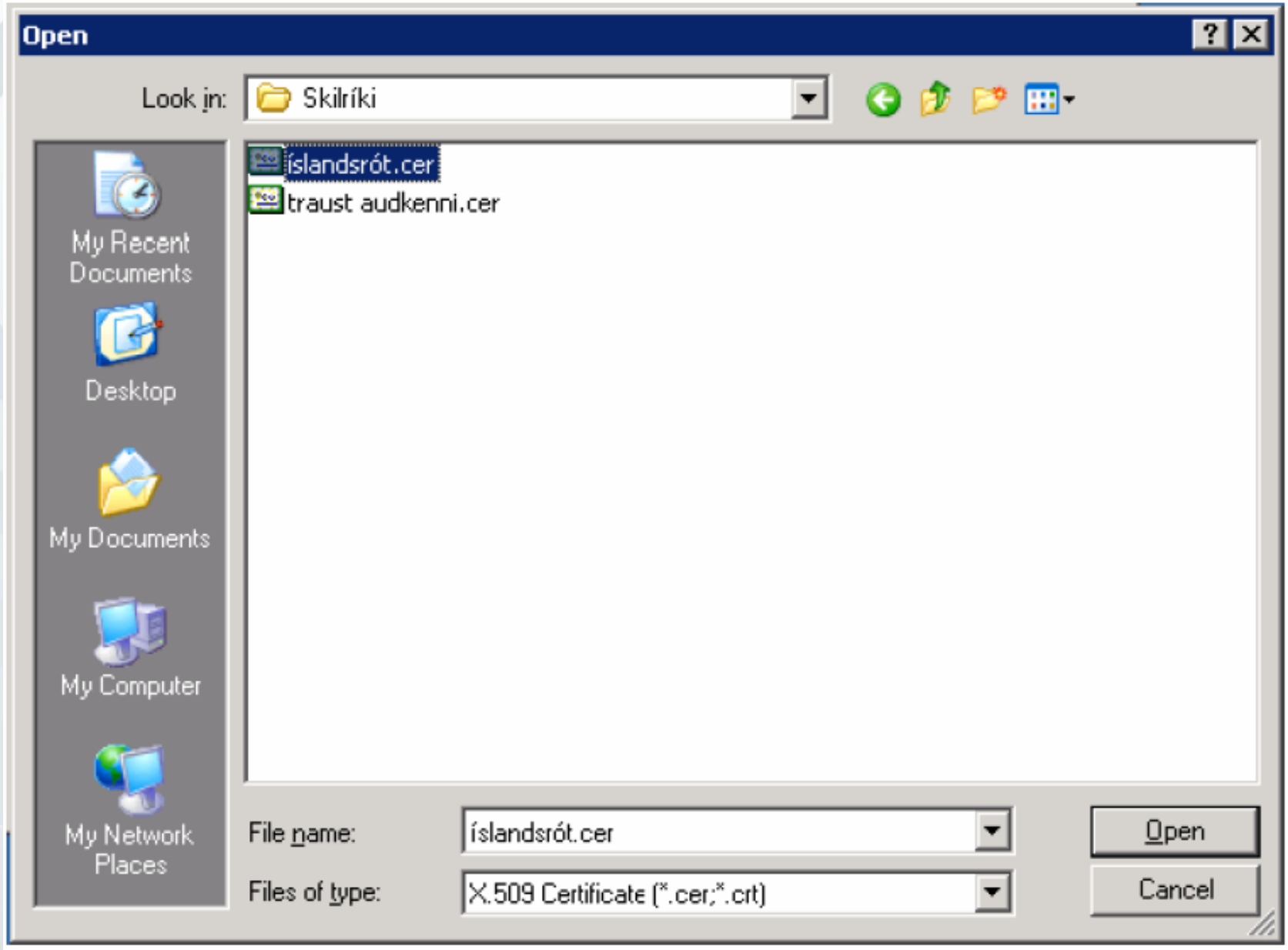

Internet Info
File
Action
Vie
Internet Informa
TFXP3244 (l
Web Site
www
Default
Status
www.test.is Properties
Web Site
ISAPI Filters
Home Directory
Documents
Directory Security
HTTP Headers
Custom Errors
ASP.NET
Anonymous access and authentication control
Enable anonymous access and edit the authentication methods for this resource.
Edit...
IP address and domain name restrictions
Grant or deny access to this resource using IP addresses or internet domain names.
Edit...
Secure communications
Require secure communications and enable client certificates when this resource is accessed.
Server Certificate...
View Certificate...
Edit...
OK
Cancel
Apply
Help

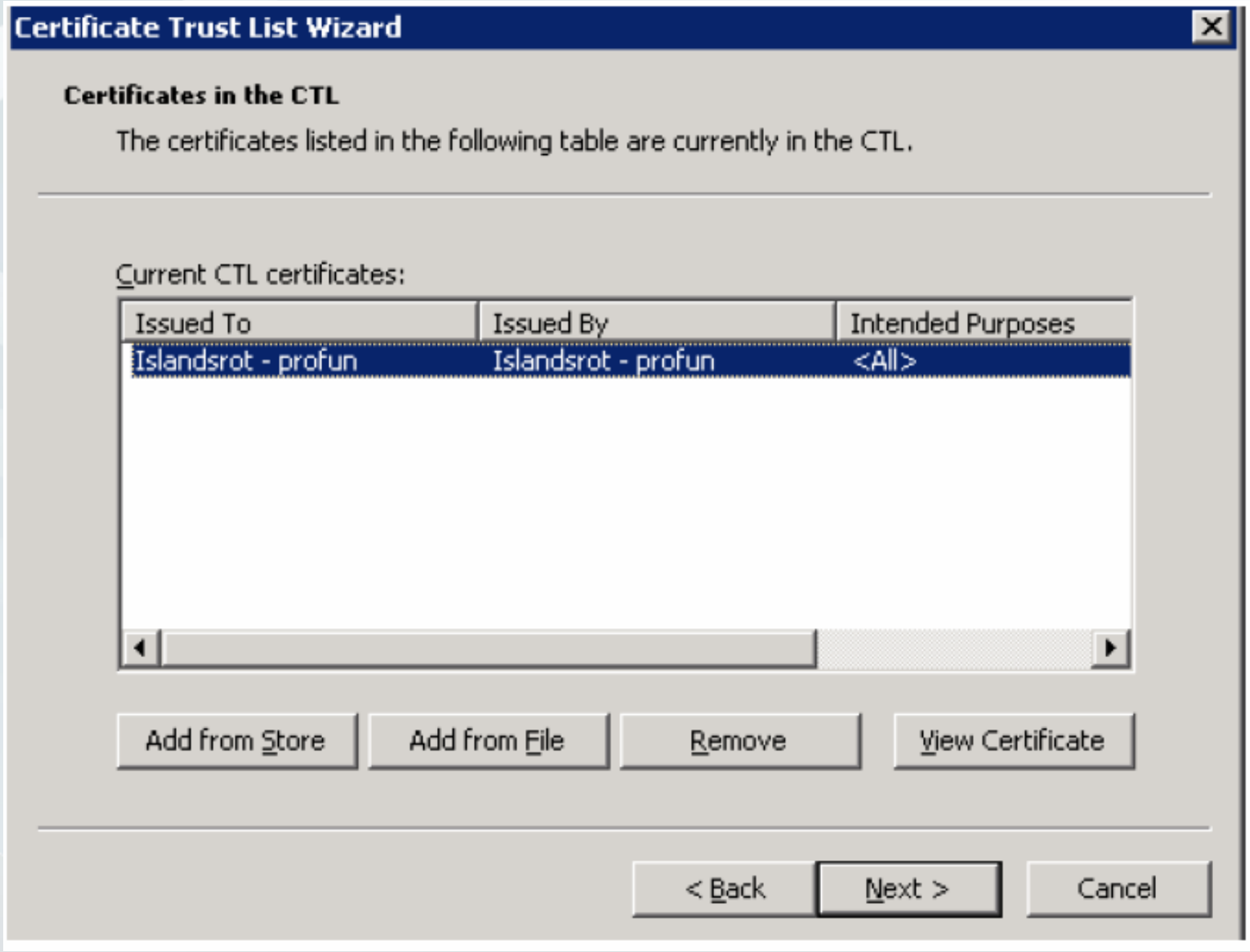

Internet Info
File
Action
Vie
Internet Informa
TFXP3244 (
Web Site
Default
Status
www.test.is Properties
Web Site
ISAPI Filters
Home Directory
Documents
Directory Security
HTTP Headers
Custom Errors
ASP.NET
Secure Communications
Require secure channel (SSL)
Require 128-bit encryption
Client certificates
Ignore client certificates
Accept client certificates
Require client certificates
Enable client certificate mapping
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.
Edit...
Enable certificate trust list
Current CTL:
New...
Edit...
OK
Cancel
Help

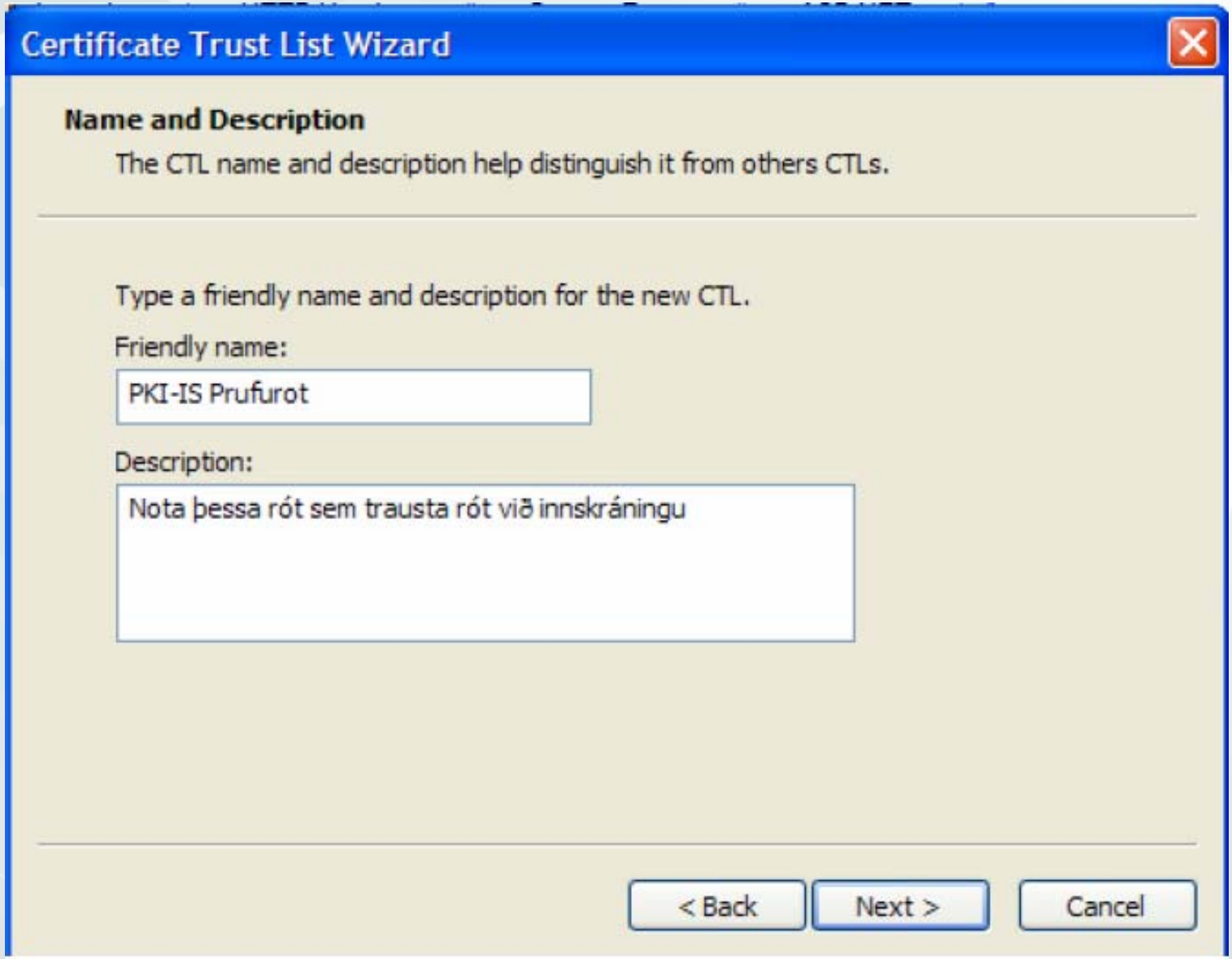

Internet Info
File
Action
Vie
Internet Informa
TFXP3244 (l
Web Site
www
Default
Status
www.test.is Properties
Web Site
ISAPI Filters
Home Directory
Documents
Directory Security
HTTP Headers
Custom Errors
ASP.NET
Secure Communications
Require secure channel (SSL)
Require 128-bit encryption
Client certificates
Ignore client certificates
Accept client certificates
Require client certificates
Enable client certificate mapping
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.
Edit...
Enable certificate trust list
Current CTL:
New...
Edit...
OK
Cancel
Help

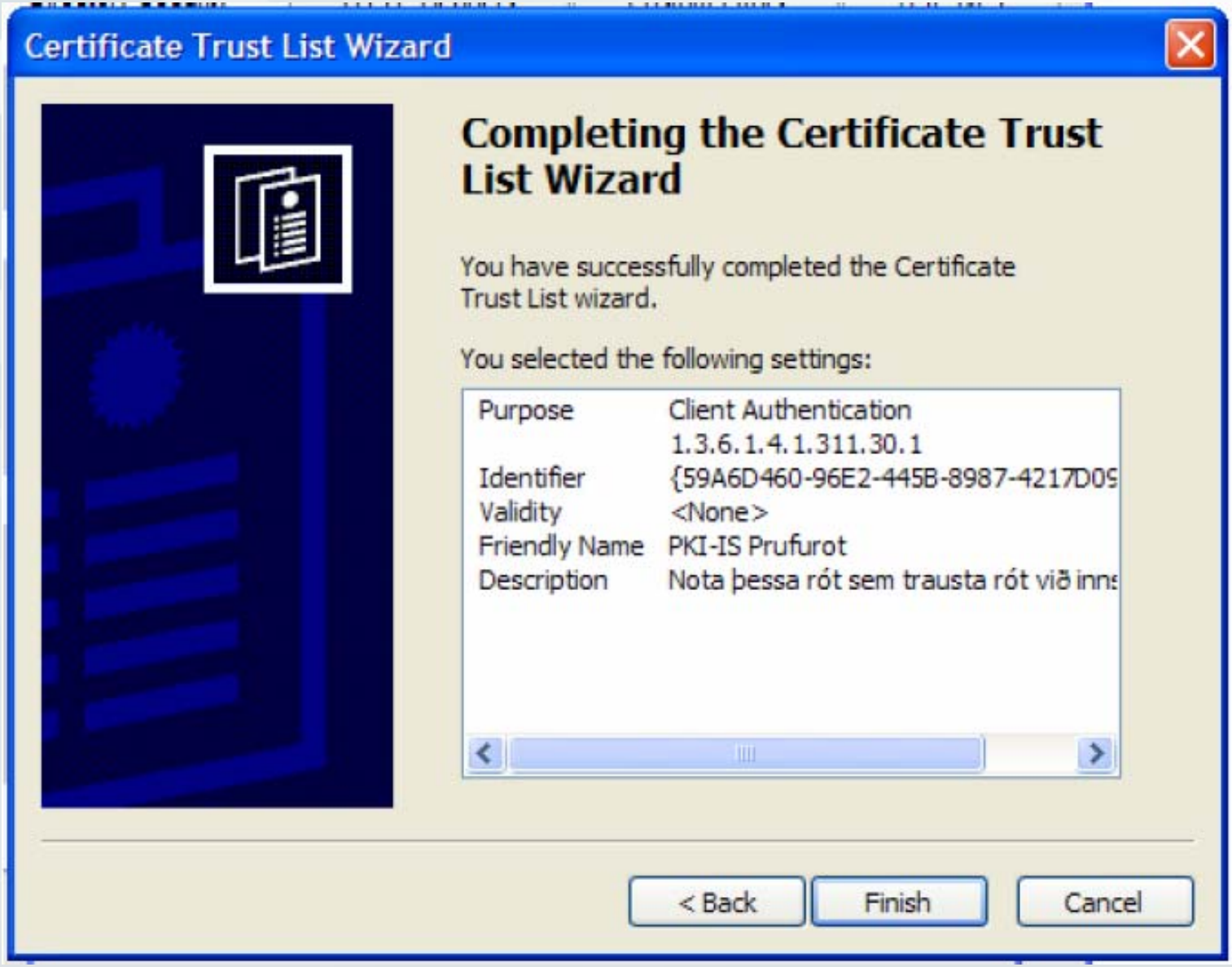

Certificate Trust List Wizard
Welcome to the Certificate Trust List Wizard
This wizard helps you create a new certificate trust list or modify an existing certificate trust list.
A certificate trust list (CTL) is a signed list of root certification authority (CA) certificates that have been judged reputable by an administrator.
To continue, click Next.
< Back
Next >
Cancel

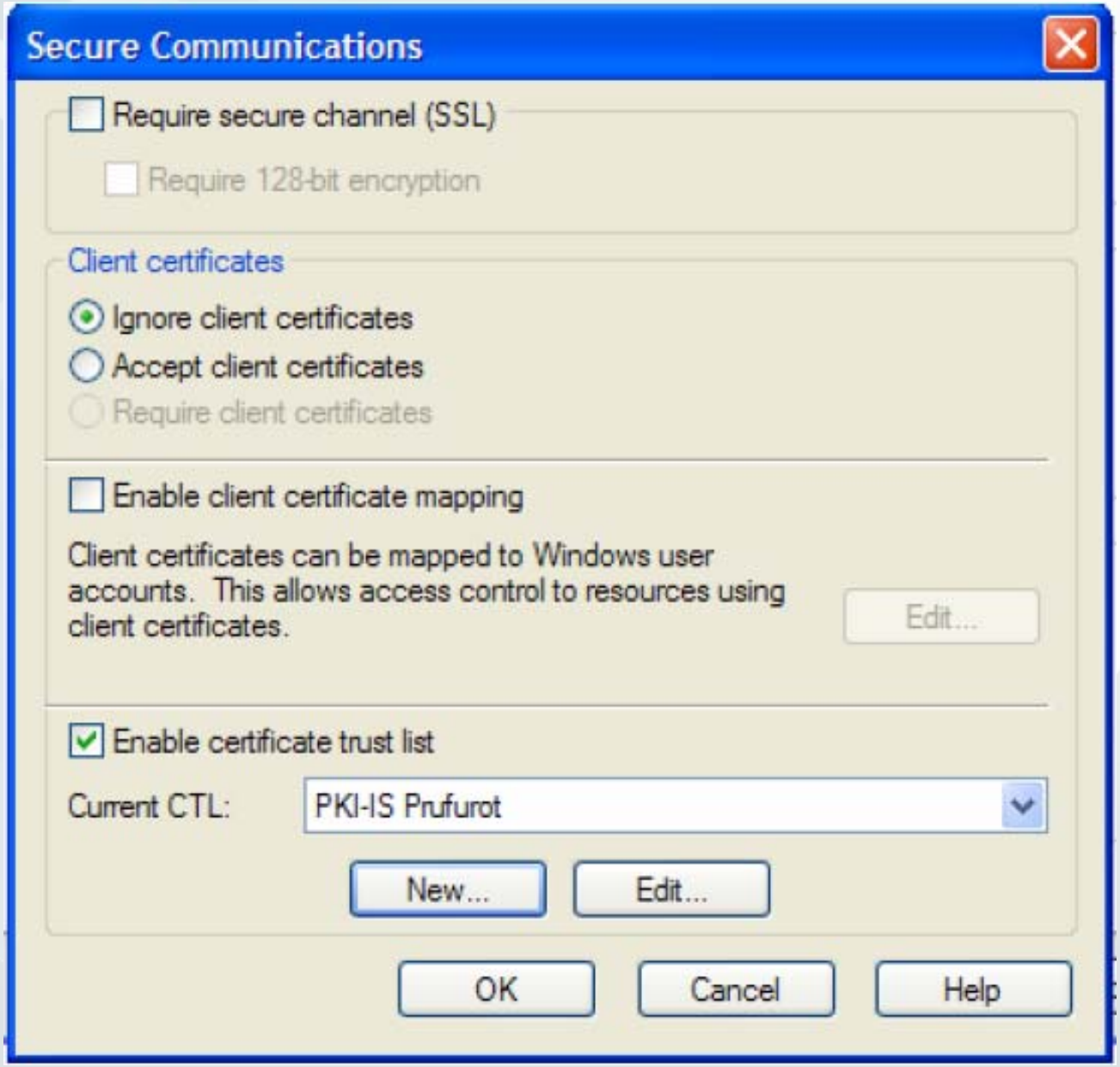

Certificate Trust List Wizard
Certificates in the CTL
The certificates listed in the following table are currently in the CTL.
Current CTL certificates:
Issued To
Issued By
Intended Purposes
Add from Store
Add from File
Remove
View Certificate
< Back
Next >
Cancel

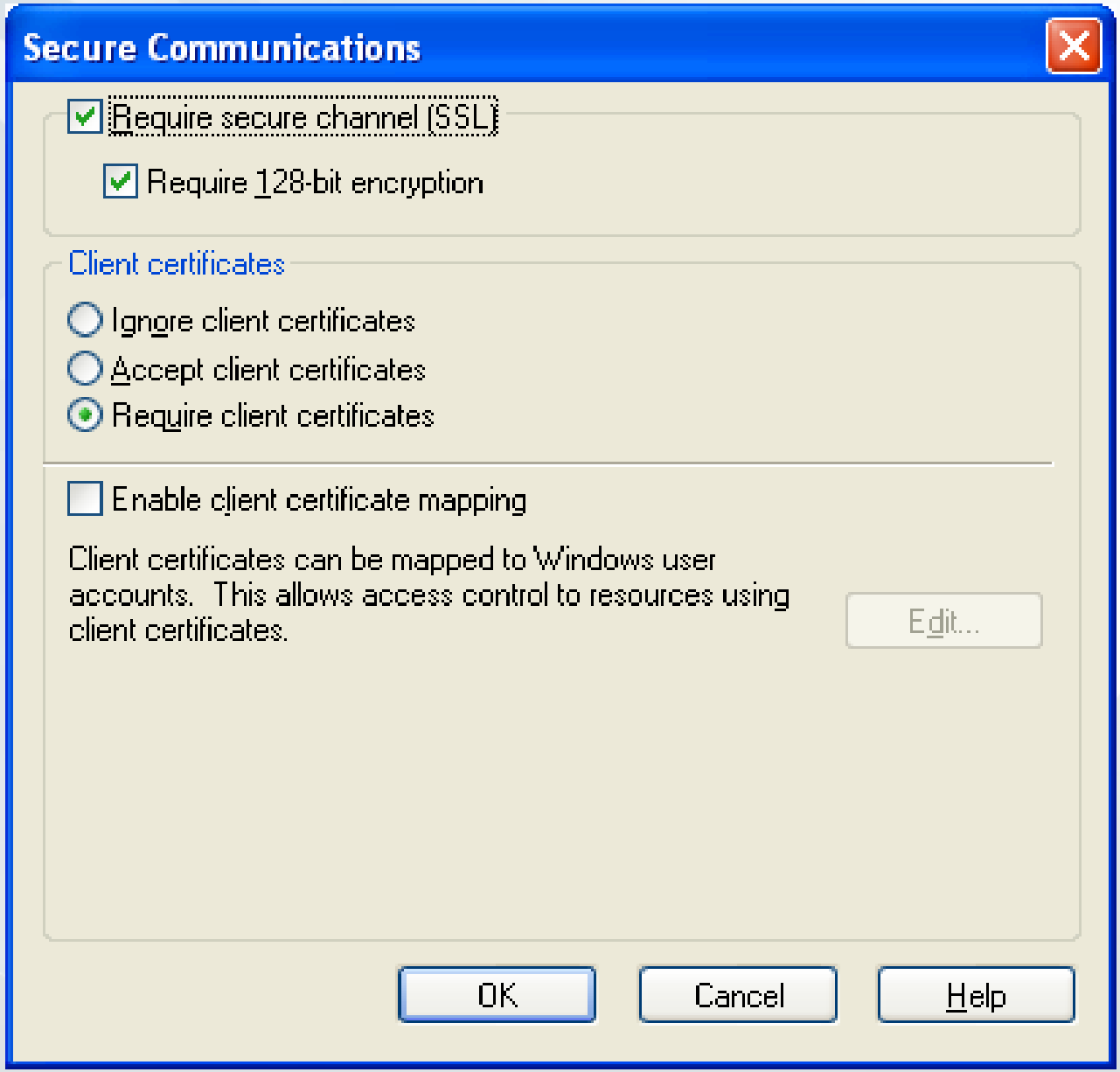

Open
Look in:
Skilríki
íslandsrót.cer
traust audkenni.cer
My Recent Documents
Desktop
My Documents
My Computer
My Network Places
File name:
íslandsrót.cer
Files of type:
X.509 Certificate (*.cer;*.crt)
Open
Cancel


Certificate Trust List Wizard
Certificates in the CTL
The certificates listed in the following table are currently in the CTL.
Current CTL certificates:
Issued To
Issued By
Intended Purposes
Islandsrot - profun
Islandsrot - profun
<All>
Add from Store
Add from File
Remove
View Certificate
< Back
Next >
Cancel


Certificate Trust List Wizard
Name and Description
The CTL name and description help distinguish it from others CTLs.
Type a friendly name and description for the new CTL.
Friendly name:
PKI-IS Prufurot
Description:
Nota þessa rót sem trausta rót við innskráningu
< Back
Next >
Cancel


Certificate Trust List Wizard
Completing the Certificate Trust List Wizard
You have successfully completed the Certificate Trust List wizard.
You selected the following settings:
Purpose
Client Authentication
1.3.6.1.4.1.311.30.1
Identifier
{59A6D460-96E2-445B-8987-4217D0
Validity
<None>
Friendly Name
PKI-IS Prufurot
Description
Nota þessa rót sem trausta rót við inn
< Back
Finish
Cancel


Secure Communications
Require secure channel (SSL)
Require 128-bit encryption
Client certificates
Ignore client certificates
Accept client certificates
Require client certificates
Enable client certificate mapping
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.
Edit...
Enable certificate trust list
Current CTL:
PKI-IS Prufurot
New...
Edit...
OK
Cancel
Help


Secure Communications
Require secure channel (SSL)
Require 128-bit encryption
Client certificates
Ignore client certificates
Accept client certificates
Require client certificates
Enable client certificate mapping
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.
Edit...
OK
Cancel
Help

```
string kennitala = null;
// The certificate is contained int the Http request data.
HttpClientCertificate currentCertificate
  = HttpContext.Current.Request.ClientCertificate;
// Most of the common certificate fields ara available as properties on
// the certificate object
string certificateSubject = currentCertificate.Subject;
// A subject string contains the personal Id number (kennitala):
// CN = Ingólfur Árnason, Serial Number = 0101508478, OU = Prófun,
// OU = Auðkenning, OU = Einkaskilríki, C = IS
string[] foo = certificateSubject.Split(",".ToCharArray());
foreach( string s in foo )
{
  string[] parameters = s.Trim().Split("=".ToCharArray());
   // Because of differences in the underlying Windows Crypto API, the
   // SerialNumber is not always translated but appears as the raw
   // certificate attribute
   if( parameters.Length == 2 && (
   parameters[0].ToLower().Equals("serialnumber" )
   ||
   parameters[0].ToLower().Equals("oid.2.5.4.5")))
   {
        kennitala = parameters[1].Substring(0, 10);
        break;
   }
}
return kennitala;
```

```
using System;
using System.Collections.Generic;
using System.Text;
using System.Web;

namespace PkiLoginApplication
{
  public static class CertificateUtility
  {
    public static string GetKennitala()
    {
      string kennitala = null;
      HttpClientCertificate currentCertificate
         = HttpContext.Current.Request.ClientCertificate;
      string certificateSubject = currentCertificate.Subject;
      string[] foo = certificateSubject.Split(",".ToCharArray());
      foreach( string s in foo )
      {
        string[] parameters = s.Trim().Split("=".ToCharArray());
        if( parameters.Length == 2 && (parameters[0].ToLower().Equals("serialnumber" )
            ||
           parameters[0].ToLower().Equals("oid.2.5.4.5")))
        {
          kennitala = parameters[1].Substring(0, 10);
          break;
        }
      }
      return kennitala;
    }
  }
}
```

Milliskilríki í notkun

- Pilot skilríki
  - Notað í prófunum
  - Sömu kröfur gerðar til vottunar
- Íslandsrót
  - Auðkenni mun sjá um útgáfu skilríkja á debetkort
  - Vottun fer fram um leið og kortið er sótt

Hvernig get ég tekið þátt?

- Hægt er að sækja um skilríki hjá Auðkenni.
- Senda þarf nafn og kennitölu á pkipilot@audkenni.is
- Í prófunarfasanum fá einstaklingar skilríki, hugbúnað , leiðbeiningar um uppsetningu og lesara.

- pkipilot@audkenni.is