Web Cryptography Next Steps

Using the W3C WebCrypto API for document signing


inventivedesigners

BELGIQUE BELGIË BELGIEN BELGIUM

Carte E | E Kaart | E Karte | E Card

Nom / *Name*
Prénoms / *Given names*

Fiores
Gema Frédéric J

Type de carte / *Type of card*
Attestation d'enregistrement

Sexe / *Sex* **F**

N° carte / *Card No*
B 1003636 00

Valide du - au / *Valid from - until*
31.01.2001 - 31.01.2006

Signature du titulaire
Holder's signature


50 EURO
10 EURO
BCE ECB EZB EKT EKP 2002
10
BCE ECB EZB EKT EKP 2002
20

nl | fr | de | en

My eGov Login

Login using my eGov profile with the government

Log in with your eID card

To log in with your eID **insert your electronic identity card, electronic foreigner card or Kids-ID into the card reader** and click the Next button below. Enter your PIN code when prompted.

Next

Please find below other accepted ways to authenticate:

Token

In order to authenticate with your token, press the **Choose** button.

Choose

Welcome to My eGov Login

In order to authenticate yourself please provide the requested credential(s).
If you do not possess any of these credentials, please go to the Self Registration page: Self Registration page.

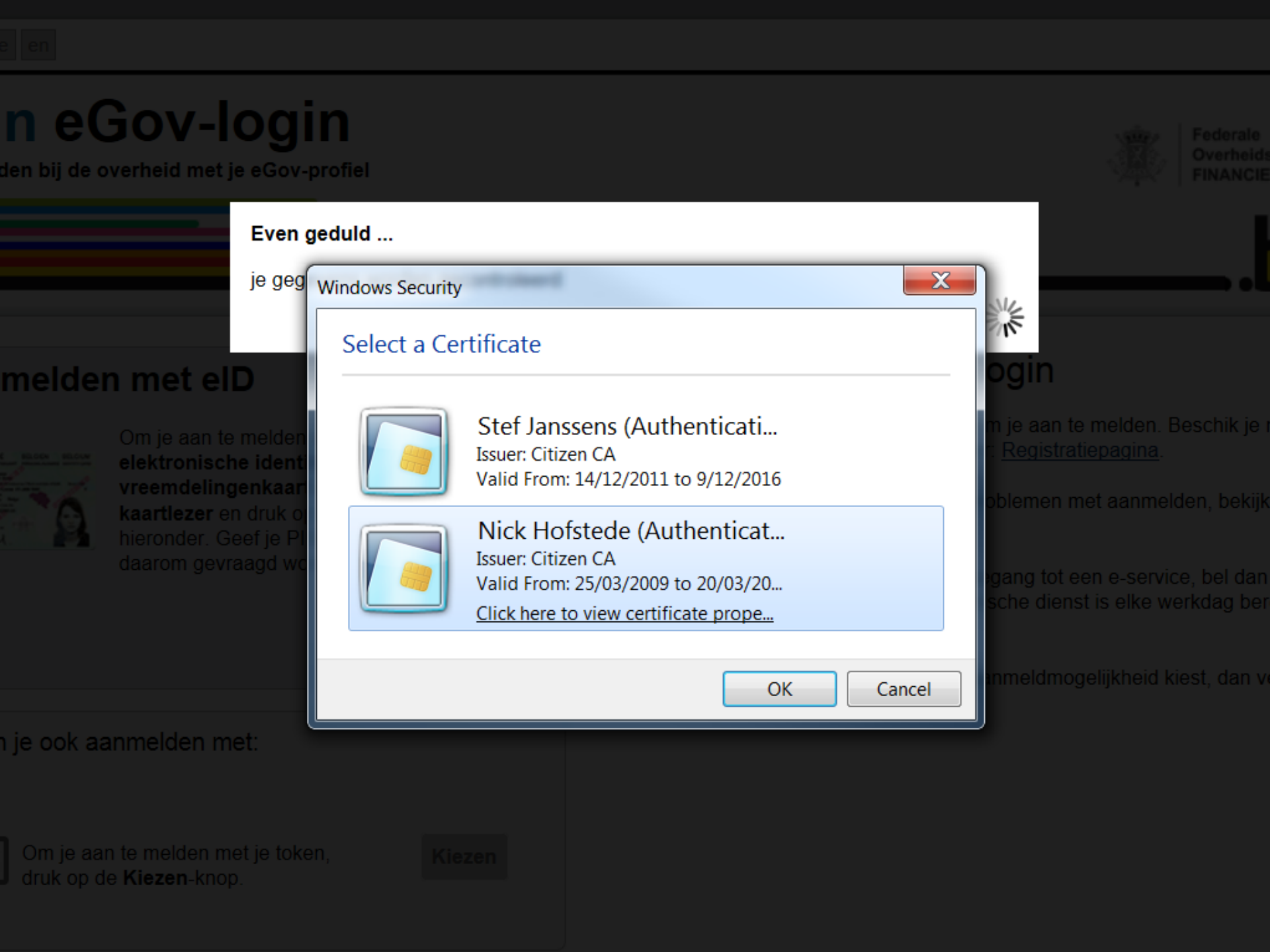
If you have any further questions or problems about the authentication please check our FAQ pages.

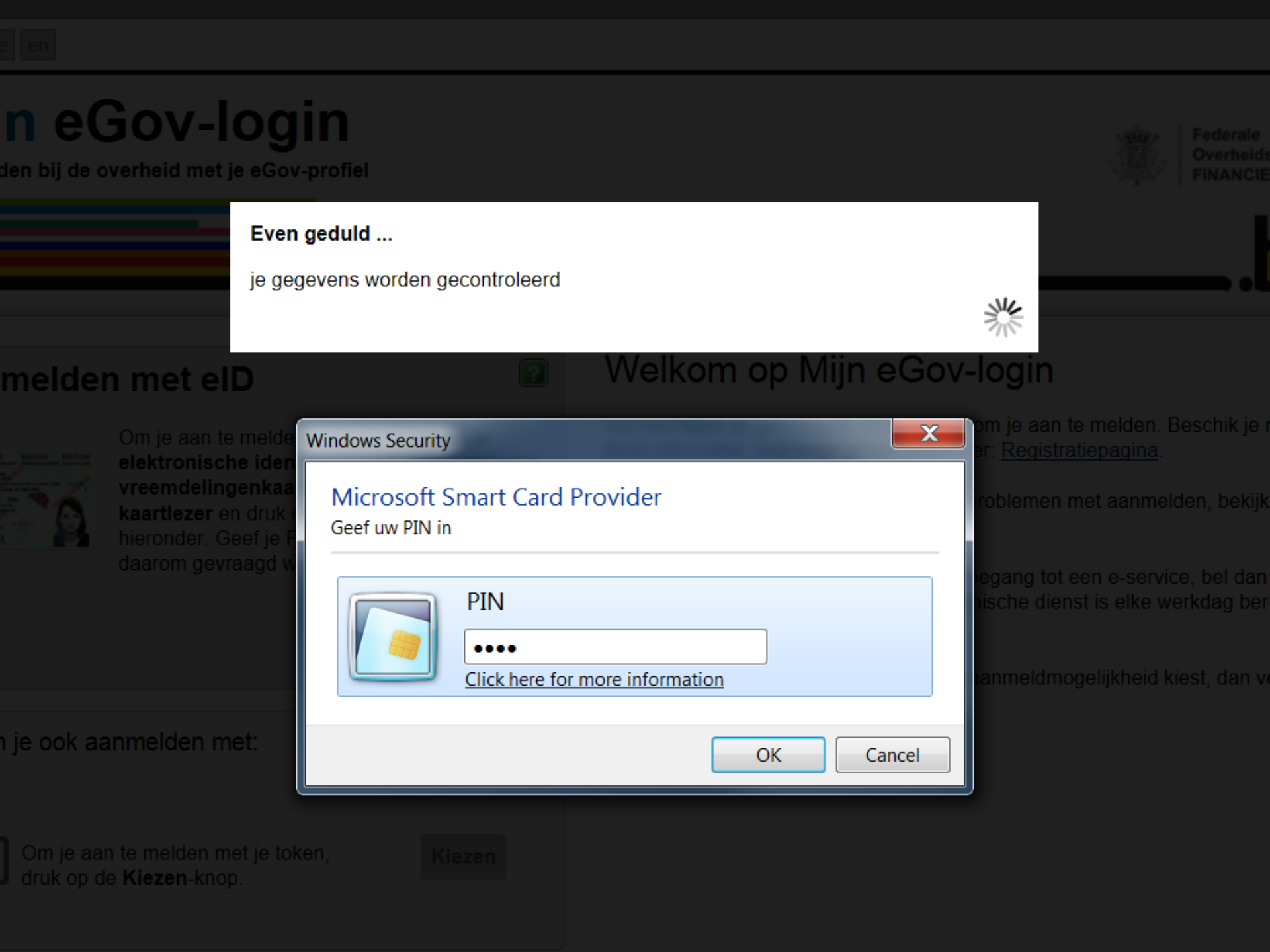
Looking for an answer about accessing an e-service? Please call 0257/257 57 (normal rate). This telephone service is at your disposal every working day from 8.00 hrs to 17.00 hrs.

Ready

About this website | Privacy

powered by fedict

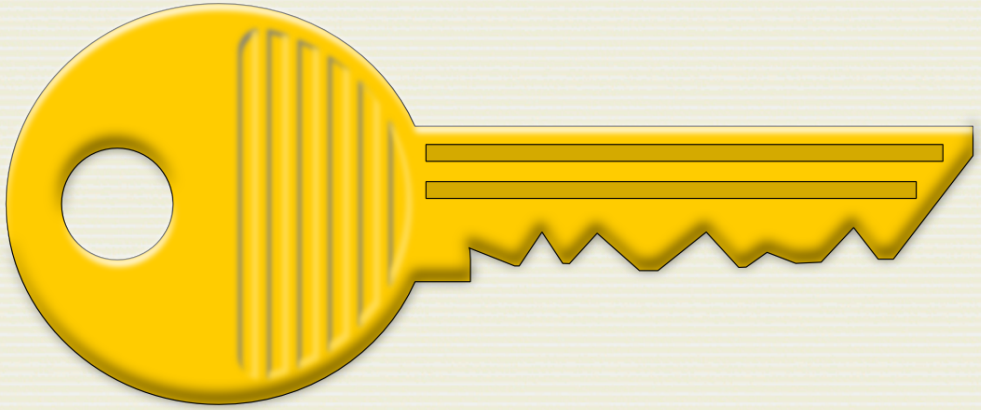

n eGov-login
den bij de overheid met je eGov-profiel
Even geduld ...
Windows Security
Select a Certificate
Stef Janssens (Authenticati...
Issuer: Citizen CA
Valid From: 14/12/2011 to 9/12/2016
Nick Hofstede (Authenticat...
Issuer: Citizen CA
Valid From: 25/03/2009 to 20/03/20...
Click here to view certificate prope...
OK
Cancel
melden met eID
Om je aan te melden
elektronische identi
vreemdelingenkaar
kaartlezer en druk o
hieronder. Geef je PI
daarom gevraagd wo
ogin
m je aan te melden. Beschik je
Registratiepagina.
blemen met aanmelden, bekijk
gang tot een e-service, bel dan
sche dienst is elke werkdag ber
nmeldmogelijkheid kiest, dan v
je ook aanmelden met:
Om je aan te melden met je token,
druk op de Kiezen-knop.
Kiezen


n eGov-login
den bij de overheid met je eGov-profiel
Even geduld ...
je gegevens worden gecontroleerd
melden met eID
Welkom op Mijn eGov-login
Windows Security
Microsoft Smart Card Provider
Geef uw PIN in
PIN
Click here for more information
OK
Cancel
je ook aanmelden met:
Om je aan te melden met je token, druk op de Kiezen-knop.
Kiezen


I Agree

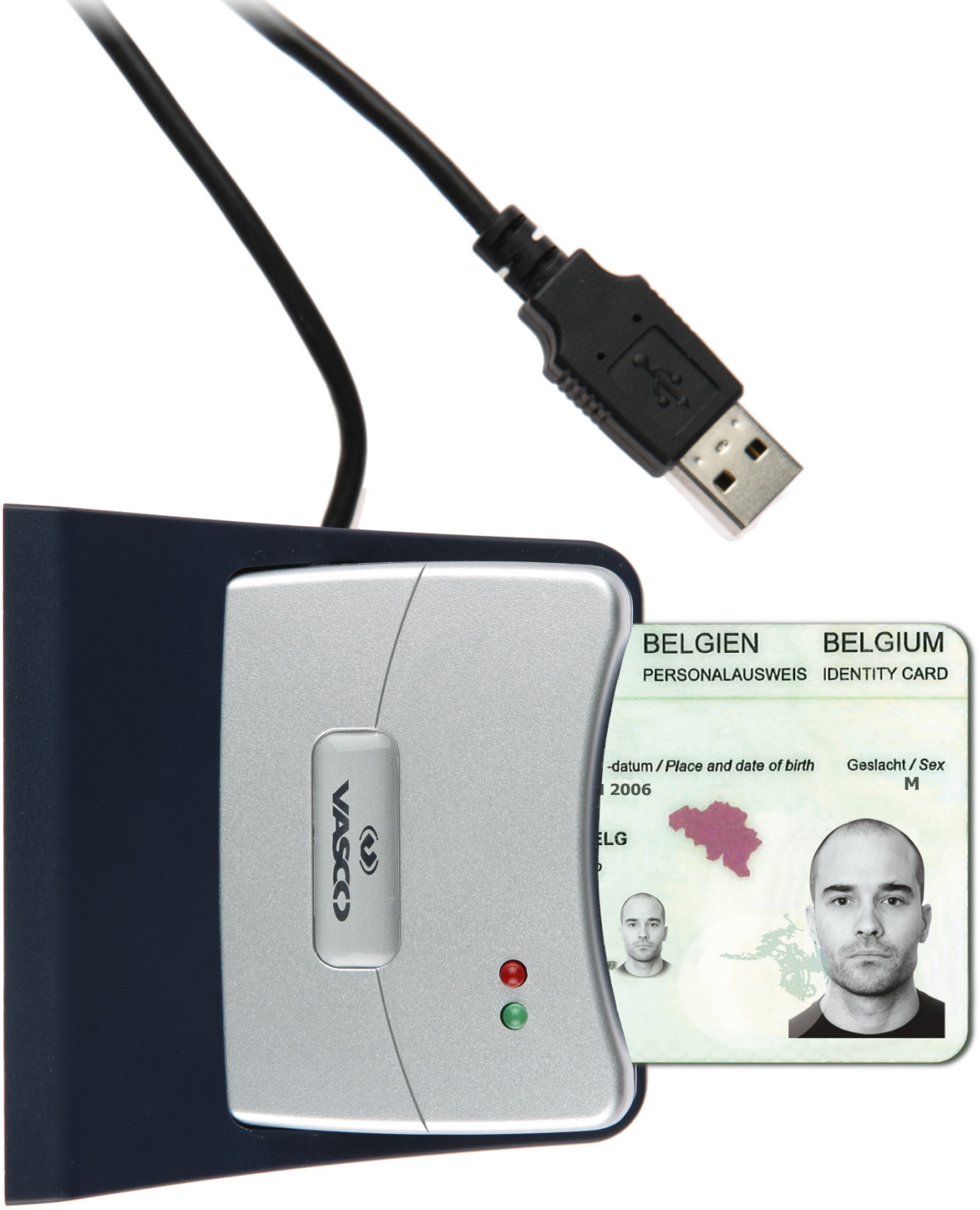

Congratulations
on 25 years of service
This certifies that
has dedicated twenty five years of service.

Nick Van den Bleeken




LAW


http://www


VASCO
BELGIEN
BELGIUM
PERSONALAUSWEIS
IDENTITY CARD
-datum / Place and date of birth
2006
Geslacht / Sex
M


Java™

Signing box

Electronic Signatures

.be

What does signing box do?

This application will allow you to electronically sign files and verify signed files, by means of your electronic identity card (eID). Using this application will create a signature on an uploaded file. Only this signature will contain information on your identity. That is, your information will not be stored any where else, except in the files you signed.

Upload your file

If you want more information about eID cards and eID readers, go to: eid.belgium.be

Signing box

Electronic Signatures

.be

1 Upload file › 2 File details ‹ › 3 Sign file

Upload a file

Choose the file you want to sign or verify:

+ Choose a file to upload

If you upload an OpenOffice document (ODF), or a Microsoft Office 2007 file (ooxml), the file itself will be signed.

In case you upload another file format, your file will be zipped, and that zipfile will be signed.

Signing box

Electronic Signatures

.be

✓ Upload file › 2 File details ‹ › 3 Sign file

File detail

This document has not been signed

Download file | Upload another file | + Add signature

Signing box

Electronic Signatures

.be

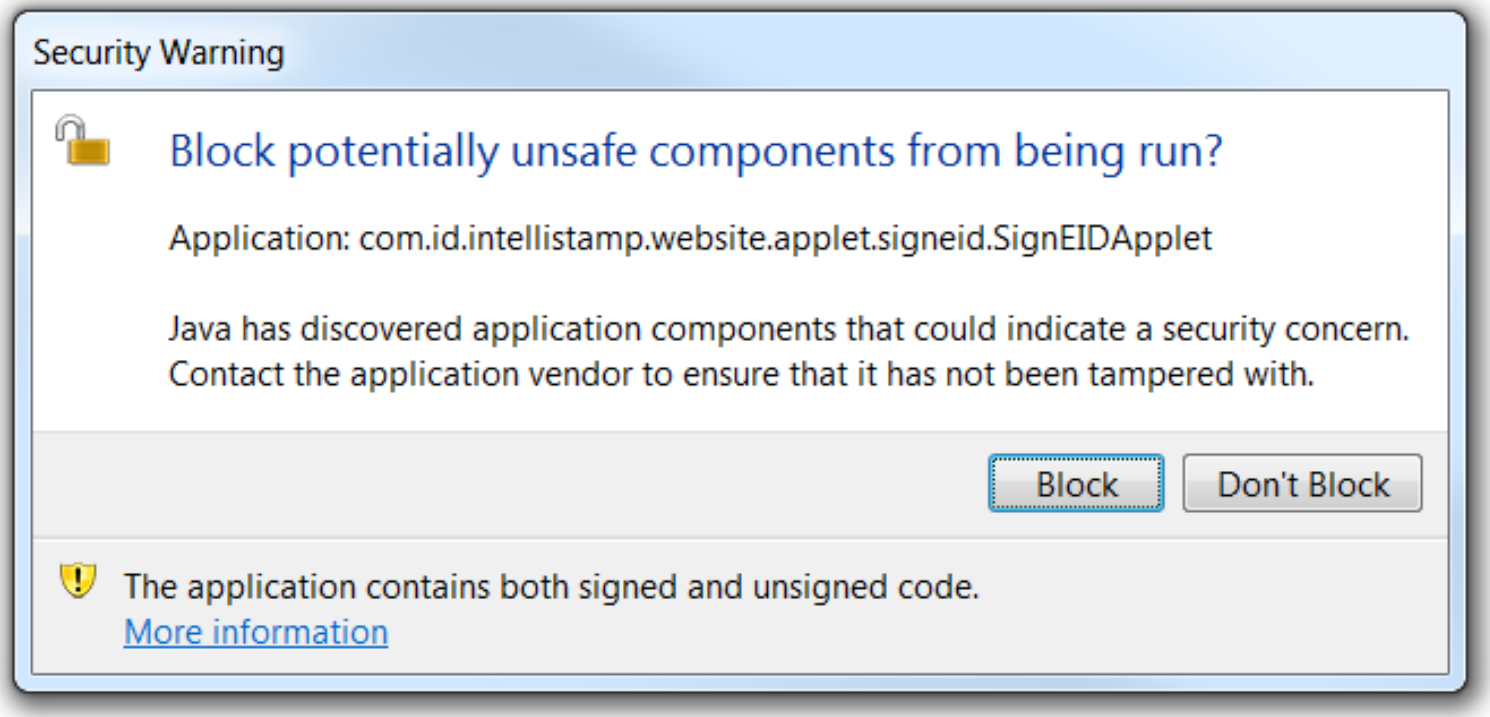
✓ Upload file › ✓ File details ‹ › 3 Sign file

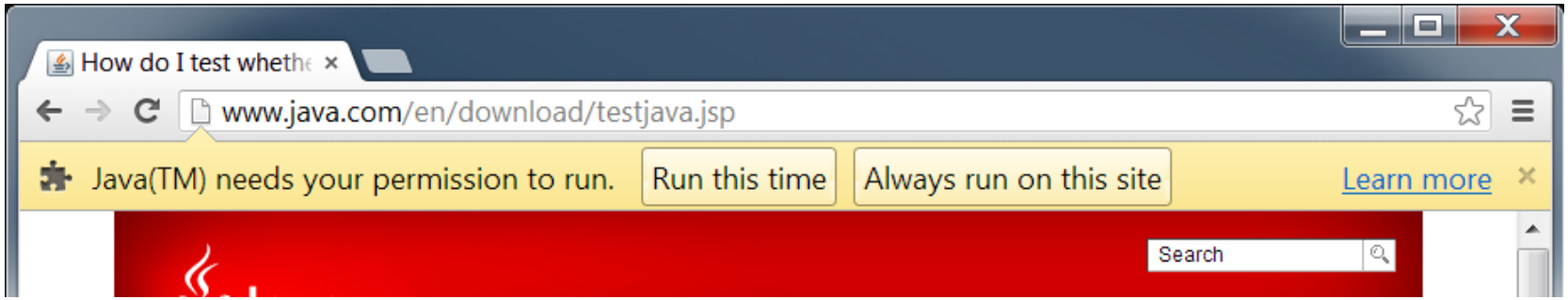
fedict @-novating government

eID Digital Signature Service

Sign document

This plugin is disabled.
Manage plugins...


Security Warning
Block potentially unsafe components from being run?
Application: com.id.intellistamp.website.applet.signeid.SignEIDApplet
Java has discovered application components that could indicate a security concern. Contact the application vendor to ensure that it has not been tampered with.
Block
Don't Block
The application contains both signed and unsigned code.
More information


How do I test whethe
www.java.com/en/download/testjava.jsp
Java(TM) needs your permission to run.
Run this time
Always run on this site
Learn more
Search

Signing box

Electronic Signatures

.be

✓ Upload file › ✓ File details ‹ › 3 Sign file

fedict e-novating government eID Digital Signature Service

View document

Please verify the content of the document you're about to sign.

Sign Cancel

Options »

Contents of this ZIP file

donut-chart.png

Signing box

Electronic Signatures

.be

✓ Upload file › ✓ File details ‹ › 3 Sign file

fedict e-novating government

eID Digital Signature Service

Sign document

Please insert your eID card...

Details >>

Signing box

Electronic Signatures

.be

✓ Upload file › ✓ File details ‹ › 3 Sign file

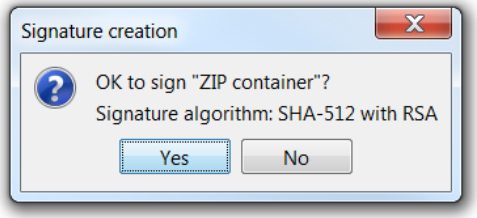
fedict e-novating government

eID Digital Signature Service

Sign document

Signing...

Details >>



Signing box

Electronic Signatures

.be

✓ Upload file › ✓ File details ‹ › 3 Sign file

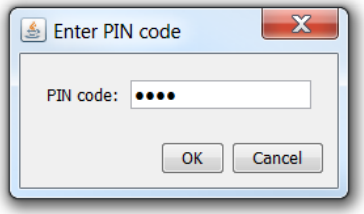
fedict e-novating government

eID Digital Signature Service

Sign document

Signing...

Details >>



Signing box

Electronic Signatures

.be

✓ Upload file › 2 File details ‹ › 3 Sign file

File detail

This file has been signed **1** time(s).

Signed by
Signer: SERIALNUMBER=79081636594, GIVENNAME=Nick, SURNAME=Hofstede, CN=Nick Hofstede (Signature), C=BE **Signing time:** Monday, June 17, 2013 6:47:40 PM CEST

Download file | Upload another file | + Add signature


IntelliStamp®


W3C®

W3C Working Draft

Web Cryptography API

W3C Last Call Working Draft *25 March 2014*

This version:
http://www.w3.org/TR/2014/WD-WebCryptoAPI-20140325/
Latest published version:
http://www.w3.org/TR/WebCryptoAPI/
Latest Editor's Draft:
http://dvcs.w3.org/hg/webcrypto-api/raw-file/tip/spec/Overview.html
Previous Version(s):
http://www.w3.org/TR/2013/WD-WebCryptoAPI-20130625/
Editors:
Ryan Sleevi, Google, Inc. <sleevi@google.com>
Mark Watson, Netflix <watsonm@netflix.com>
Participate:
Send feedback to public-webcrypto-comments@w3.org (archives), or file a bug (see existing bugs).

Abstract

This specification describes a JavaScript API for performing basic cryptographic operations in web applications, such as hashing, signature generation and verification, and encryption and decryption.

```
var algorithmSign = {
    name: "RSASSA-PKCS1-v1_5",
    params: {hash: "SHA-256" }
};

var data = convertToArrayBufferView("hello World!");

window.crypto.subtle.sign(algorithmSign, key.privateKey,
    data).then(
        console.log.bind(console, "Signature: "),
        console.log.bind(console, "Unable to sign: "));
```

W3C Working Draft

WebCrypto Key Discovery

W3C Working Draft 22 August 2013

This version:
http://www.w3.org/TR/2013/WD-webcrypto-key-discovery-20130822/
Latest published version:
http://www.w3.org/TR/webcrypto-key-discovery/
Latest editor's draft:
http://dvcs.w3.org/hg/webcrypto-keydiscovery/raw-file/tip/Overview.html
Previous version:
http://www.w3.org/TR/2013/WD-webcrypto-key-discovery-20130108/
Editor:
Mark Watson, Netflix, watsonm@netflix.com

Abstract

This specification describes a JavaScript API for discovering named, origin-specific pre-provisioned cryptographic keys for use with the Web Cryptography API. Pre-provisioned keys are keys which have been made available to the UA by means other than the generation, derivation, importation functions of the Web Cryptography API. Origin-specific keys are keys that are available only to a specified origin. Named keys are identified by a name assumed to be known to the origin in question and provisioned with the key itself.

Named

Origin-specific

Pre-provisioned

Named

~~Origin-specific~~

Pre-provisioned

Named

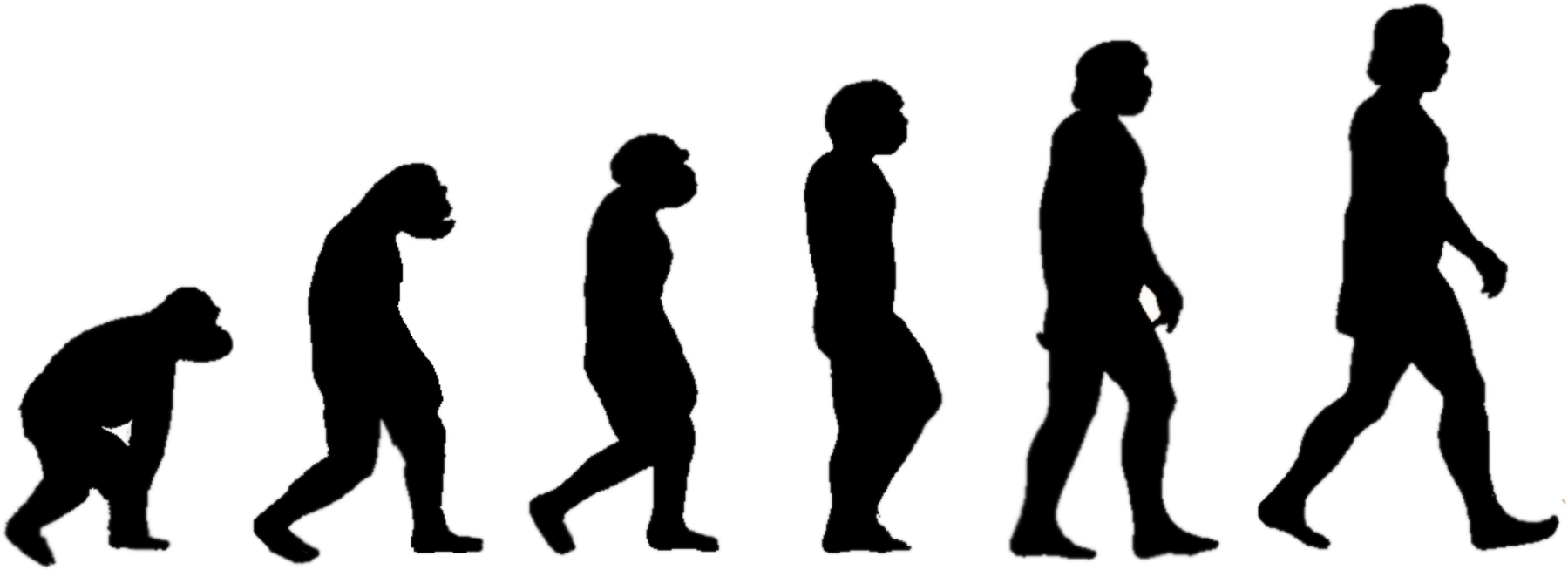
~~Origin-specific~~

~~Pre-provisioned~~

~~Named~~

~~Origin-specific~~

~~Pre-provisioned~~



Certificate based discovery

```
var c = window.crypto.subtle;
c.createX500Principal("CN=eID Citizen CA, C=BE").then(
  function(issuer) {
    c.selectX509Certificate({
      authorities : [issuer],
      privateKeyValid: true,
      reason: “Select a certificate to sign your document"
    }).then(
      function(cert) {
        var key = cert.privateKey;
        var data = convertPlainTextToArrayBufferView("Foo");
        c.sign(key.algorithm, key, data).then(
          console.log.bind(console, "Signature: "));
)})})
```

Signing box

Electronic Signatures

.be

What does signing box do?

This application will allow you to electronically sign files and verify signed files, by means of your electronic identity card (eID). Using this application will create a signature on an uploaded file. Only this signature will contain information on your identity. That is, your information will not be stored any where else, except in the files you signed.

Upload your file

If you want more information about eID cards and eID readers, go to: eid.belgium.be

Signing box

Electronic Signatures

.be

1 Upload file › 2 File details ‹ › 3 Sign file

Upload a file

Choose the file you want to sign or verify:

+ Choose a file to upload

If you upload an OpenOffice document (ODF), or a Microsoft Office 2007 file (ooxml), the file itself will be signed.

In case you upload another file format, your file will be zipped, and that zipfile will be signed.

Signing box

Electronic Signatures

.be

✓ Upload file › 2 File details ‹ › 3 Sign file

File detail

This document has not been signed

Download file | Upload another file | + Add signature

Signing box

Electronic Signatures

.be

✓ Upload file › ✓ File details ‹ › 3 Sign file

fedict e-novating government eID Digital Signature Service

View document

Please verify the content of the document you're about to sign.

Sign Cancel

Options »

Contents of this ZIP file

donut-chart.png

```
var c = window.crypto.subtle;
c.createX500Principal("CN=eID Citizen CA, C=BE").then(
  function(issuer) {
    c.selectX509Certificate({
      authorities : [issuer],
      privateKeyValid: true,
      reason: “Select a certificate to sign your document"
    }).then(
      function(cert) {
        var key = cert.privateKey;
        var data = convertPlainTextToArrayBufferView("Foo");
        c.sign(key.algorithm, key, data).then(
          console.log.bind(console, "Signature: "));
})})})
```

This application needs access to your key store to run. Select keys Learn more

Signing box

Electronic Signatures

.be

✓ Upload file › ✓ File details ‹ › 3 Sign file

fedict e-novating government eID Digital Signature Service

View document

Please verify the content of the document you're about to sign.

Sign Cancel

Options »

Contents of this ZIP file

donut-chart.png

nl fr en de

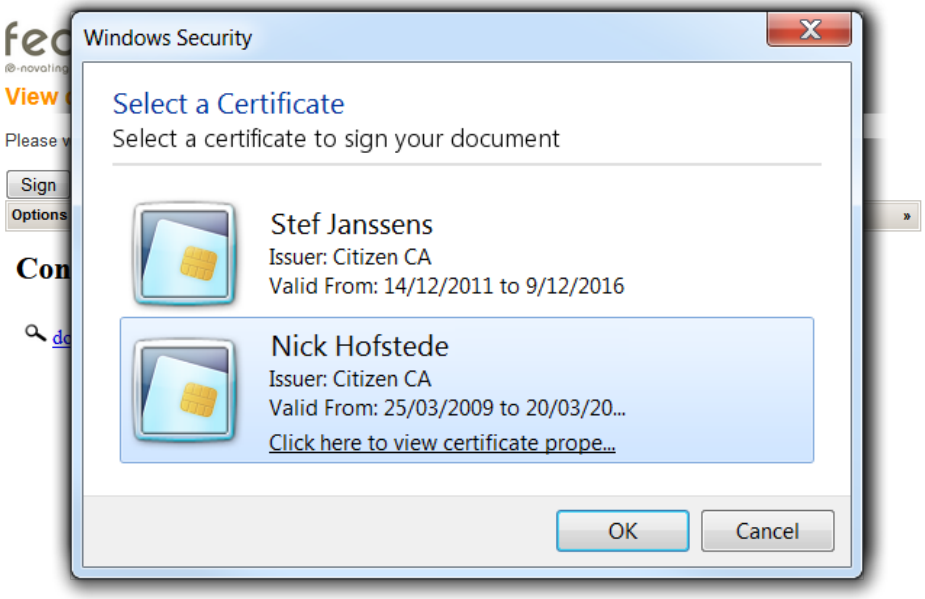
Other information and services of the government. www.belgium.be .be

Signing box

Electronic Signatures

.be

Upload file › File details ‹ › 3 Sign file



```
var c = window.crypto.subtle;
c.createX500Principal("CN=eID Citizen CA, C=BE").then(
  function(issuer) {
    c.selectX509Certificate({
      authorities : [issuer],
      privateKeyValid: true,
      reason: “Select a certificate to sign your document"
    }).then(
      function(cert) {
        var key = cert.privateKey;
        var data = convertPlainTextToArrayBufferView("Foo");
        c.sign(key.algorithm, key, data).then(
          console.log.bind(console, "Signature: "));
)})})
```

Signing box

Electronic Signatures

.be

Upload file › File details ‹ › 3 Sign file

fedict

e-novating government

eID Digital Signature Service

Sign docu

Signing

Details >>

```
var c = window.crypto.subtle;
c.createX500Principal("CN=eID Citizen CA, C=BE").then(
  function(issuer) {
    c.selectX509Certificate({
      authorities : [issuer],
      privateKeyValid: true,
      reason: “Select a certificate to sign your document"
    }).then(
      function(cert) {
        var key = cert.privateKey;
        var data = convertPlainTextToArrayBufferView("Foo");
        c.sign(key.algorithm, key, data).then(
          console.log.bind(console, "Signature: "));
})})})
```

Signing box

Electronic Signatures

.be

✓ Upload file › 2 File details ‹ › 3 Sign file

File detail

This file has been signed **1** time(s).

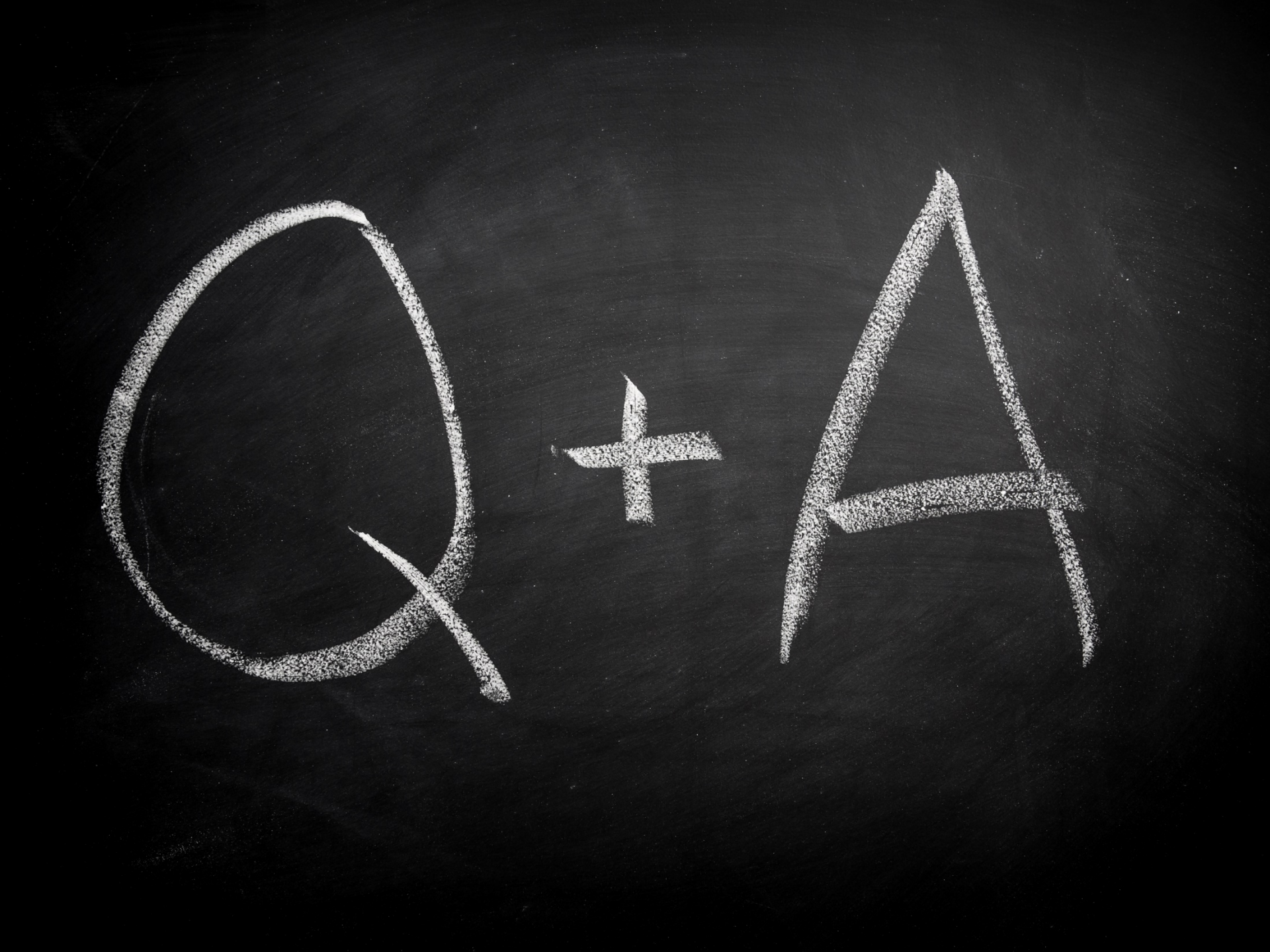
Signed by
Signer: SERIALNUMBER=79081636594, GIVENNAME=Nick, SURNAME=Hofstede, CN=Nick Hofstede (Signature), C=BE **Signing time:** Monday, June 17, 2013 6:47:40 PM CEST

Download file | Upload another file | + Add signature


Java™


ΑΘΛΗΤΙΚΗ ΕΝΩΣΗ ΑΣΤΥΝΟΜΙΚΩΝ ΕΛΛΑΔΟΣ


Thank You


Q+A