# David Wozny

Subject: MPS credentials in new MPS infra, thoughts so far

From: David@wozny.org
Sent: 27 February 2012 11:22
To:
Cc:
Subject: RE: MPS credentials in new MPS infra, thoughts so far

Gents,
I've made an attempt to show you the flavour of the SSL handshake without including any sensitive addressing information; the trace below is what we see when authenticating to the portal using an MPS card (certificate):

| Packet No | Time | Source | Dest'n | Protocol | Information |
|---|---|---|---|---|---|
| 3215 | 7.32 | Cob | Hen | SSL v2 | Client Hello |
| 3221 | 7.37 | Hen | Cob | SSL v3 | Server Hello, Certificate (#1), Certificate Request, Server Hello Done |
| 3239 | 10.06 | Cob | Hen | SSL v3 | Certificate (#2), Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message |
| 3242 | 10.12 | Hen | Cob | SSL v3 | Change Cipher Spec |
| 3243 | 10.12 | Hen | Cob | SSL v3 | Encrypted Handshake Message |

The certificates presented in remarks (#1) and (#2) are illustrated below:

| | |
|---|---|
| #1: | cn=portalxxxxxxxxxxxxxxxxxxxx.police.uk, ou=npia, o=Police, c=GB<br>cn=Authentication Issuing Authority, ou=IAM CS, o=Police, c=GB<br>cn=Police Service PKI Root Certificate Authority, o=Police, c=GB |

| | |
|---|---|
| #2 | cn=Alvin Stardust c123456, ou=met, o=Police, c=GB<br>cn=SubCA1, ou=met, o=Police, c=GB |

Hope this helps.

Kind regards, Dave

**David Wozny | Consultant**

**Mobile: +44 (0)7825 952 809**
**E-mail: david@wozny.org**

**From:** David@wozny.org
**Sent:** 25 February 2012 14:48
**To:**
**Cc:**
**Subject:** RE: MPS credentials in new MPS infra, thoughts so far

Paul,
I can confirm that only the EE certificate is present on the MPS smart card (no CA certificates).

I have done further testing using a smart card possessing a certificate issued from an MPS test PKI (i.e. unrelated to the MPS production PKI which NPIA have cross-certified with). The WireShark trace showed the start of the SSL handshake and I could see the “Certificate Request” from the server directed to the client – however, we then got a *fatal* “SSL Alert”. This suggests to me that because the client certificate (from the test PKI) doesn’t match any of the four trust anchors (see below) offered by the portal server in the “Certificate Request”, that the client cannot even present the EE certificate to the server-side during the SSL handshake. The Internet Explorer session then blows up (Page could not be displayed) – this is different behaviour than using a production MPS certificate whereby we see the entire SSL handshake complete successfully but then get the “untrusted error” from the “application”.

The DNs offered in the “Certificate Request” part of the handshake are:

- cn=National Issuing CA, OU=WestYorkshire, O=Police, C=GB
- cn=SubCA1, OU=Met, O=Police, C=GB
- cn=Police Service PKI Root Certification Authority, O=Police, C=GB
- cn=Authentication Issuing Authority, OU=IAM CS, O=Police, C=GB

Regards, Dave

**David Wozny | Consultant**

**Mobile: +44 (0)7825 952 809**
**E-mail: david@wozny.org**

**From:**
**Sent:** 25 February 2012 11:10
**To:** David@wozny.org;
**Cc:**
**Subject:** RE: MPS credentials in new MPS infra, thoughts so far

Dave/Toby/Mark,

Let me do some investigating from the DirX side to determine if there is anything we can do from our side in respect to the chain builder functionality. A quick question for the MET, can you confirm if the whole certificate chain is stored on the smartcard or is it solely the EE certificate and key pairs belonging to the user?

Regards,

Paul

**From:** David@wozny.org [mailto:David@wozny.org]
**Sent:** 23 February 2012 20:00
**To:**
**Cc:**
**Subject:** RE: MPS credentials in new MPS infra, thoughts so far

Hi Toby,
We will perform a test from a server that has no CA certificates in its stores (and therefore only the client certificate will be posted in the SSL handshake) to see if that confirms our suspicions. I agree with all the assertions you make with regard the behaviour we are seeing – all entirely plausible. I am hesitant (like yourself) though to suggest any ways forward until we have conclusive proof that we have nailed the source of the problem.

However, we do know that the MPS CA certificates are required in the certificate stores on all the MPS machines for them to do natural intra-MPS certificate authentication such as smart card logon to Windows and Citrix, etc. so I think we can rule that out now as a possible approach. Furthermore, it is probably unrealistic to expect the crypto stack on an MPS machine when building a chain from an EE certificate to pick a CA certificate other than its own natural issuer in favour of a cross-certificate - again, if it did so it would very likely be problematic for intra-MPS certificate authentication.

I think we'll be in a stronger position tomorrow to get to the bottom of this.  I am extremely grateful for your assistance, you've really helped enormously.

Kind regards, Dave

**David Wozny | Consultant**

**Mobile: +44 (0)7825 952 809**