From: Ranko Stamatovic [ranko.stamatovic@dominionvoting.com]
Sent: 4/4/2018 1:06:10 PM
To: Paul Chavez-Casanova [paul.chavez-casanova@dominionvoting.com]; Ivan Bulut [ivan.bulut@dominionvoting.com]
CC: Martijn Punt [martijn.punt@dominionvoting.com]; Ruzica Matic [ruzica.matic@dominionvoting.com]; Dave Anderson [dave.anderson@dominionvoting.com]
Subject: RE: RTM - Listener certificate signing

When we talk about certificates in general – Dominion is not the certificate issuer. Actually, we can create certificate, but – level of trust can be problematic… Different people (users) have different perspective what certificate means and how it should be obtained.

One more thing – when we are sending election results through Internet (from tabulators or RTM), this is not closed system any more.

Therefore, my general approach to this problem is:

- do not assume anything regarding who/how/when certificate should be created/obtained,
- do not assume anything regarding the name of the certificate
- Our system should be able to:
  - import any provided certificate (but first to check validity), or/and
  - Create certificate on simple and intuitive way. Furthermore, implement logic that the same certificate is be copied to exact location where, EMS will pick it up, when prepare definition files for tabulators/RTM…

Ranko

From: Paul Chavez-Casanova
Sent: Wednesday, April 4, 2018 7:10 AM
To: Ranko Stamatovic <ranko.stamatovic@dominionvoting.com>; Ivan Bulut <ivan.bulut@dominionvoting.com>
Cc: Martijn Punt <martijn.punt@dominionvoting.com>; Ruzica Matic <ruzica.matic@dominionvoting.com>; Dave Anderson <dave.anderson@dominionvoting.com>
Subject: RE: RTM - Listener certificate signing

Hey guys:

I understand your concern, I was initially concerned about the hard-coding of that name too.

However, let me assure you that changing that name is not needed (at least not frequently). The purpose of the certificate is to identify the server, in the same way that a passport identifies someone.

When you renew your passport, your name ***doesn't change*** – it's the same thing for the Listener. The Listener will always be the Listener, no matter how many times you renew its certificate. This is why we don't need to worry about this.

Additionally, nobody in the field uses certificates from a third party: obtaining one per election would simply be too expensive and cumbersome. Plus, they are really overkill for our purposes – in our closed system there's no need for third-party trust. Finally, if somebody ever wanted to do this, they could simply ask the third party to create the cert with the rightful name of the system: "Listener".

It's still good that you guys made this configurable in app.config. This would make it easy to change things if there was some reason to rename the system in the future, e.g., if we wanted to do a full name like "DVS ImageCast Listener". For this reason, I can see that we should consider making this configurable on our side too, but we can cross that bridge when we get to it.

Anyway, thanks for bringing this up, and let me know if you have any other questions.

Paul.

From: Ranko Stamatovic
Sent: Tuesday, April 3, 2018 6:52 AM
To: Ivan Bulut <ivan.bulut@dominionvoting.com>; Paul Chavez-Casanova <paul.chavez-casanova@dominionvoting.com>
Cc: Martijn Punt <martijn.punt@dominionvoting.com>; Ruzica Matic <ruzica.matic@dominionvoting.com>
Subject: RE: RTM - Listener certificate signing

Hey Paul,

According to Eric, Chicago will change Listener certificate for each elections. This is why we started this discussion.

If I understood correctly, Listener will work only if there is installed valid certificate with "CN=Listener". Correct?
Our logic on the RTM client, when we looking for the certificate from the store is the same as above (we look for the certificate with attribute "CN=Listener"). We did not hardcode word "Listener" in the code, but in the app config.

For 5.8 (5.6A) we probably be OK, since we have only one elections to do, but for next release we need to have clan and simple to logic (both on Listener server and RTM client side) regarding certificates. We should be open to any use case – whether to create own or import third party certificate.

Ranko

From: Ivan Bulut
Sent: Tuesday, March 27, 2018 4:34 PM
To: Paul Chavez-Casanova <paul.chavez-casanova@dominionvoting.com>
Cc: Ranko Stamatovic <ranko.stamatovic@dominionvoting.com>; Martijn Punt <martijn.punt@dominionvoting.com>; Ruzica Matic <ruzica.matic@dominionvoting.com>
Subject: RE: RTM - Listener certificate signing

HI Paul,
Your answer pretty much explains what I was asking.

I've talked to Ranko and we would need to change how this is implemented with TcpClient.dll. As a EMS user I would want to have an option to use any certificate I want. The one acquired from Dominion as well as the one acquired from any other authority vendor.

Here is the ticket:
http://jirabg.dominionvoting.com/browse/ICL-231

Thank you
Ivan

From: Paul Chavez-Casanova
Sent: Friday, March 23, 2018 5:37 PM
To: Ivan Bulut <ivan.bulut@dominionvoting.com>
Subject: RE: RTM - Listener certificate signing

Hey Ivan,

I don't know who added that bit about a third-party cert, but doing something like that would be unnecessary and as far as I know, nobody does that. But yeah, if you were to do that, you'd need to ask the vendor to create the certificate with that subject name for things to work.

Your question about the TcpClient is pretty broad… can you narrow that down to the specifics you're interested in? E.g., do you mean how the cert is read?

Paul.

From: Ivan Bulut
Sent: Friday, March 23, 2018 9:55 AM
To: Paul Chavez-Casanova <paul.chavez-casanova@dominionvoting.com>
Cc: Ranko Stamatovic <ranko.stamatovic@dominionvoting.com>; Martijn Punt <martijn.punt@dominionvoting.com>
Subject: RE: RTM - Listener certificate signing

Hi Paul,
It's written in the manual that the certificate can be issued by a third party vendor. We said that we are hardcoding word "CN=Listener" on both RTM and Listener.
Can you provide more details on how does the TcpClient.dll works on Listener /RTM.

Thank you
Ivan