Infrastructure - Task #2660

Story # 1906 (Closed): Review, revise, and update architecture documentation

Deciding on a key size for D1 certs

2012-04-27 22:11 - Roger Dahl

Status:	New	**Start date:**	2012-04-27
Priority:	Normal	**Due date:**	
Assignee:	Dave Vieglais	**% Done:**	0%
Category:	Documentation	**Estimated time:**	0.00 hour
Target version:	Maintenance Backlog		
Milestone:	CCI-1.0.0	**Story Points:**	
Product Version:	*		

Description

This is not purely an arch doc, but a decision that we should make and then document.

Discussion:

Friday 03:56:58pm andy Are you sure you want to do a full 4K key? The system will be doing a lot of work to keep up with that.
Friday 04:05:32pm andy If somebody wants to get the information, there would be easier ways than hijacking the connection. Computing the encryption is still not a free process. The CPU will be spending a LOT of cycles computing the encryption instead of serving up files.
Friday 04:08:13pm andy "2048-bit keys are generally considered safe for the time being. If you want an intermediate step, though, 3072-bit keys are right smack-dab in the middle."
Friday 04:08:32pm roger Ah.
Friday 04:09:05pm andy A followup post: "Thanks. I noticed generating a 4096 bit key took a whole lot longer as well, and the final size of it was bigger as well."
Friday 04:09:17pm andy
http://stackoverflow.com/questions/8453529/are-there-any-disadvantages-to-using-a-4096-bit-encrypted-ssl-certificate
Friday 04:10:11pm andy I think that until quatum computing becomes mainstream, there aren't enough people with enough compute power to break the 2048-bit keys.

History

#1 - 2012-04-27 22:17 - Dave Vieglais

2048 bit keys are recommended in general best practice.

For example, https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.0.pdf

#2 - 2012-04-27 22:49 - Matthew Jones

The size of the certificate key won't really have an impact on throughput, because SSL only uses the asymmetric key for the initial SSL handshake, at which point a different symmetric key is used for traffic encryption because it is much faster -- the symmetric key chosen depends on how the SSL server and client are configured and what each will accept. So, although the SSL handshake will take marginally longer with a 4096 bit key (because it takes longer to encrypt and sign the challenge tokens), this is a very small amount of data and should be mostly ignorable. See: http://stackoverflow.com/questions/7426609/ssl-if-you-use-2048-bit-rsa-key-will-the-symmetric-key-that-is-negotiated-also

I would argue that our Root CA certs and Intermediate certs should be 4096 because they have very long expiration times (I made them 100 years), but the others can be anything over 2048 because they can be revoked. That said, 4096 keys should be fine on MNs too, but I think the CA makes 2048 bit keys as configured now.

#3 - 2014-10-02 17:21 - Dave Vieglais

- Target version set to Maintenance Backlog