

# Re: Offline Root Certificate Server and subordinate CA

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-03/0347.html>

---

**From:** Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

**Date:** 03/17/05

Date: Thu, 17 Mar 2005 11:39:21 -0600

Thanks for clearing that up Paul. Excellent explanation. ---- Steve

"Paul Adare" <padare@newsguy.com> wrote in message  
news:MPG.1ca3121c501b7ffa989c18@msnews.microsoft.com...  
> *In article <O01CfGrKFHA.572@tk2msfngp13.phx.gbl>, in the*  
> *microsoft.public.win2000.security news group, Steven L Umbach*  
> *<n9rou@nospam-comcast.net> says...*  
>  
>> *As*  
>> *far as the empty CDP/AIA, that depends on your particular needs for*  
>> *security*  
>> *and performance.*  
>  
> *The requirement for empty AIA and CRL distribution points for a root CA*  
> *has nothing to do with performance nor security. For the AIA, the AIA*  
> *location is used to build a certificate chain and the AIA distribution*  
> *point in an issued certificate is used to locate the certificate of the*  
> *CA that issued that certificate. To find the root CA certificate, all we*  
> *need is the AIA location from any certificate issued by the root. The*  
> *root is the top level so once we have its certificate, we don't need to*  
> *find anymore, therefore no need for an AIA distribution point in it.*  
> *As far as having an empty CDP location for the root, RFC 3280 calls for*  
> *applications to stop revocation checking one level below a self signed*  
> *certificate in the chain. Also, keep in mind that a CRL is a signed*  
> *document, so with the root CA you've got a chicken and egg situation. If*  
> *you were to revoke the root CA certificate, you then need to use the*  
> *revoked certificate to sign the CRL that contains the revocation. :-)*  
>  
>> *I have also read where it is recommended in many situations*  
>> *to increase the length of CRL life to six months for the offline CA based*  
>> *on*  
>> *the assumption that it is secured and the likelihood that it would ever*  
>> *have*  
>> *it's certificate revoked is extremely unlikely.*  
>  
> *Now you're confusing the CRL that a root CA issues (which would only*

microsoft.public.win2000.security: Re: Offline Root Certificate Server and subordinate CA

- > *ever contain certificates that it issued) with a theoretical CRL that*
- > *would contain its own certificate.*
- >
- > --
- > *Paul Adare*
- > *"On two occasions, I have been asked [by members of Parliament],*
- > *'Pray, Mr. Babbage, if you put into the machine wrong figures,*
- > *will the right answers come out?' I am not able to rightly apprehend*
- > *the kind of confusion of ideas that could provoke such a question."*
- > -- *Charles Babbage (1791–1871)*