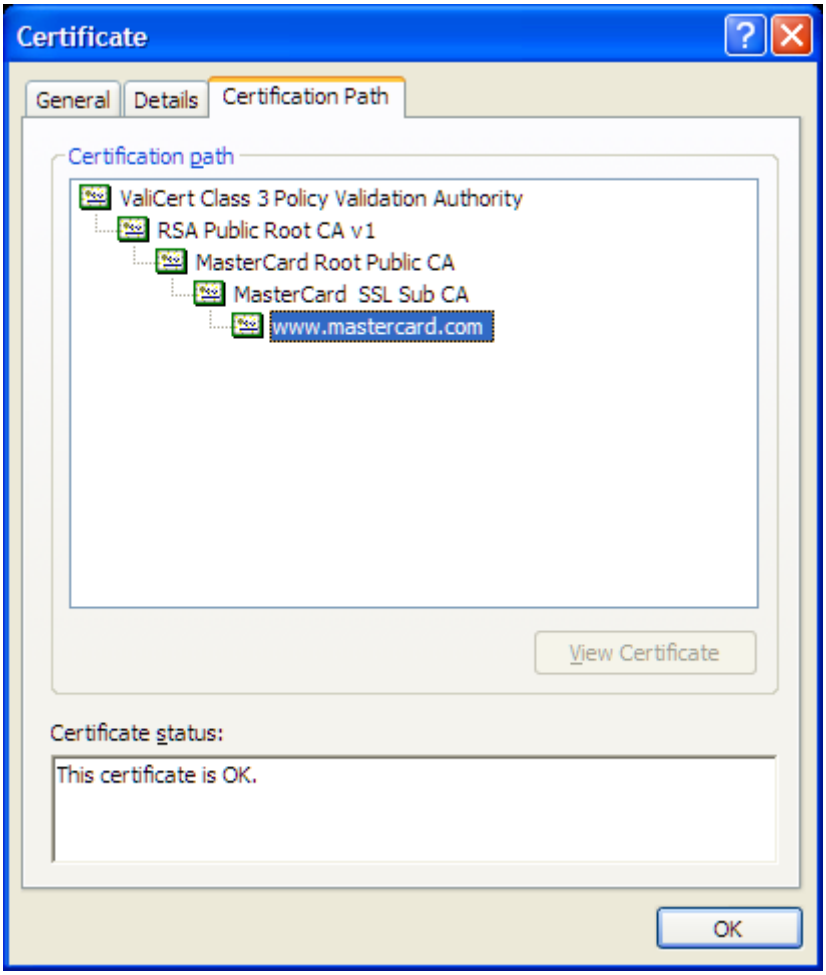
NOT yours
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Forskellen på "Chained root" og "Single root" certifikater

Denne vejledning vil prøve på at beskrive forskellen på et "Chained root" og et "Single root" udstedt certifikat. Derudover vil vi også forsøge at beskrive hvilke fordele og ulemper de to metoder at udstede certifikater har.

Begge ord bliver af certifikatudstederne anvendt som salgsfremmende ord, hvor de fremhæver fordelen ved at anvende den metode de selv anvender. Her får du muligheden for selv at bedømme og vælge hvilken model der passer dig og dine behov. Du kan også se vores anbefaling på næste side.

Følgende billede illustrerer et gyldigt certifikat, der har ikke mindre end 3 underudstedere, det er derfor et "Chained root" certifikat. Se det selv på https://www.mastercard.com



For support og hjælp til anvendelsen af denne vejledning kan du kontakte FairSSL på e-mail support@fairssl.dk eller telefon +45 77 345 678. For certifikat bestilling, certifikat sammenligninger og flere vejledninger se websitet på www.fairssl.dk.

Version 1.1 – July 2010

NOT yours
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Indholdsfortegnelse

Vores anbefaling

Vi ser ingen grund til at bekymre sig over at vælge et certifikat med den ene eller den anden model, vælg i stedet et certifikat der opfylder dine krav til pris, support og egenskaber som genudstedelsesmulighed, SGC, SAN og installationslicenser. På samtlige server produkter vi har erfaring med, kan man installere mellemcertifikaterne (”Intermediate certificates”) uden problemer, på en typisk Microsoft server tager det under 1 minut at installere et mellem certifikat, på en apache installation kræver det en ekstra linje i konfigurationen og derudover har samtlige udstedere vejledninger til næsten alle servertyper.

Hvis du mener du har brug for et rod udstedt certifikat, skal du vælge et GeoTrust QuickSSL certifikat eller hvis prisen er største faktor et RapidSSL certifikat.

Vi spår at i fremtiden vil samtlige udstedere, skifte til ”Chained root” modellen, i takt med at deres rod certifikater skal fornyes og deres udstedelsesmodel skal godkendes af klient producenterne.

Opdatering: 27. juni 2010 skiftede Thawte til kun at udstede chained root SSL certifikater.
22. juli 2010 skiftede GeoTrust til kun at udstede chained root SSL certifikater.
RapidSSL har i en pressemeddelelse sagt at de også vil skifte til chained root SSL i løbet af 2010.

Årsagen til denne ændring menes at være grundet Microsofts krav om at alle rod certifikater der skal være inkluderet i deres produkter fra den 31. december 2010 skal være over 2048 bit og overholde industri standarden med en offline root CA, hvilket kræver en chained root model til udstedelse.

NOT yours
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Hvordan stoler klienten på certifikatet?

Når en klient forbinder til en server med SSL protokollen, vil klienten hente det offentlige certifikat for serveren direkte fra serveren selv. I dette certifikat er der informationer om certifikatets detaljer, inklusive navnet på serveren der tilgås, udløbsdatoen på certifikatet, hvem der har udstedt certifikatet og en verificering af udstederens certifikat.

Alle klienter kommer med indbyggede rod certifikater som klienten stoler på, klienten vil anvende denne liste til at undersøge om certifikatet er udstedt af et af disse certifikater der stoles på.

Hvis certifikatet er udstedt af en underudsteder også kaldet "Subordinate Certificate Authority", vil den også hente certifikatet for underudstederen fra serveren eller lokalt hvis den har dette installeret og undersøge underudstederens udsteder i mod listen over certifikater den stoler på.

Hvis klienten stoler på top certifikatet og den kan tilgå alle underudsteder certifikater, vil den kunne godkende alle certifikater ned til selve serverens certifikat, uden at klienten altså behøver at have installeret andet end rod certifikatet på sig i forvejen.

I eksemplet med www.mastercard.com vil klienten undersøge om certifikatet indeholder navnet www.mastercard.com eftersom det er dette navn klienten tilgår, derudover vil den undersøge hele kæden af certifikater (se forsiden), og fordi den stoler på rod certifikatet, vil alle certifikater godkendt af rod certifikatet, inkl. dens underudstedere også være stolet på. Så med andre ord, for selve klienten gør det altså ingen forskel. Klienten vil også forsøge at online godkende at certifikatet ikke er tilbagekaldt, f.eks. fordi ejeren har mistet certifikatet og udstedt et nyt.

NOT yours
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

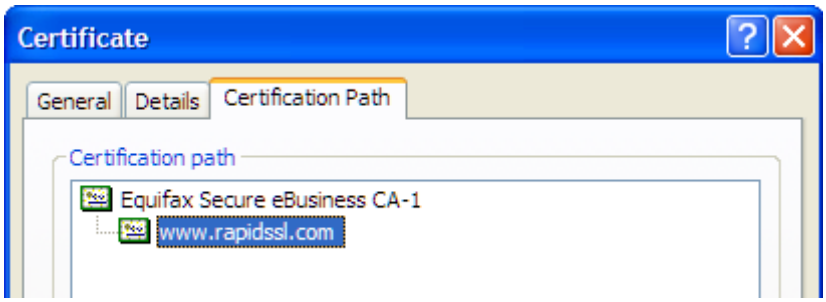
Hvad er et "Single root" certifikat?

Rod certifikater også kaldet "Single root" certifikater, er certifikater der er udstedt direkte af det certifikat som er installeret på klientens liste over certifikater den stoler på. Dette gør at klienten kun behøver certifikatet fra serveren og med dennes information samlet med klientens egen information om udstedercertifikatet kan godkende certifikatet. Den vil stadig godkende certifikatets indhold som navnet der tilgås, udløbsdato og om certifikatet er tilbagekaldt.

Det er ikke muligt at få de nye Extended Validation (EV) udstedt direkte fra et rod certifikat, da industri standarden for EV certifikater kræver at den sikrere "Chained root" model anvendes, hvor rod certifikatet er offline.

Bemærk at der er forskel på certifikat udstederes anvendelse af rod certifikater, de dyrere udstedere som VeriSign anvender i virkeligheden "Chained root" modellen som er sikrere, men de har også fået installeret nogle af deres underudsteder certifikater i flere klienter. Disse certifikater bør man altid installere mellem certifikatet på, derved sikres at flere klienter kan godkende certifikatet. Nogle få udstedere anvender stadig deres rod certifikat til at udstede kundernes certifikater direkte, men det bliver langsomt mindre almindeligt.

Følgende er et eksempel på et rod certifikat der ikke anvender en underudsteder.



Hvad er fordelene?

Den primære fordel ved et rod certifikat er at man kun behøver at installere serverens eget certifikat på serveren, skulle serveren ikke have rod certifikatet installeret selv (sjældent, men kan ske på f.eks. ældre servere), skal dette også installeres så serveren selv stoler på certifikatet.

Hvad er ulemperne?

Den primære ulempe ved et rod certifikat er at det begrænser udstederens muligheder hvis rod certifikatet kompromitteres, dvs. hvis nogen får adgang til den private nøgle af et rod certifikat, vil det blive nødvendigt at lukke rod certifikatet og derved også lukke samtlige certifikater der er udstedt af dette rod certifikat.

Chancen for at et rod certifikat kompromitteres er ekstremt lille, men grundet den teoretiske mulighed vælger de fleste udstedere at anvende "Chained root" modellen. Det er også et krav for Extended Validation certifikaterne som betragtes som værende mere følsomme, at de anvender "Chained root" modellen, netop for at undgå muligheden for misbrug.

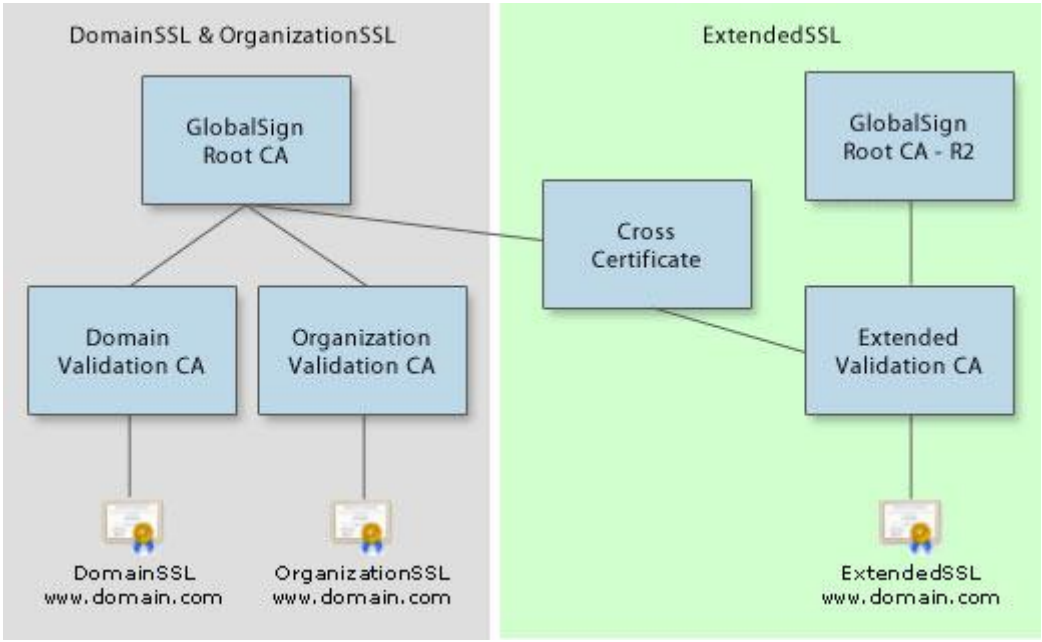
NOT yours
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Hvad er et "Chained root" certifikat?

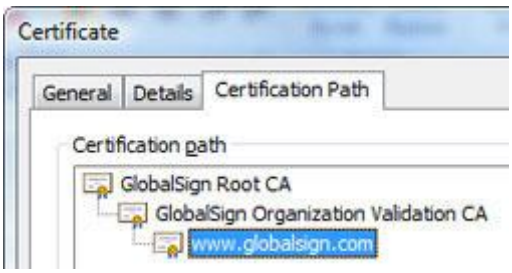
"Chained root" certifikater, er certifikater udstedt af en underudsteder, hvor klienten ikke nødvendigvis stoler på denne udsteder, men stoler på rod certifikatet der har udstedt og godkendt underudstederen.

Flere af udstederne vælger at inddele deres kunders certifikater i forskellige underudstedere, dette sikrer udstederen ved en kompromittering af en underudstederes private nøgle. Derved vil udstederen kun behøve at lukke for underudstederen og alle andre certifikater udstedt af andre underudstedere vil fortsat fungere. Derudover vil udstederen med det samme kunne oprette en ny underudsteder som vil være godkendt af alle klienter bagud fordi de altid har stolet på rod certifikatet.

Firmaer som GlobalSign og VeriSign anvender denne model for at beskytte deres rod certifikater imod misbrug og følger derved "Best Practices" standarder for "Public Key Infrastructures" ved at holde deres rod certifikat offline og utilgængeligt. Følgende illustration viser hvordan udstedercertifikaterne for GlobalSign hænger sammen.



Følgende to billeder viser hvordan klienten stoler på et Organisation SSL og et Extended SSL certifikat.

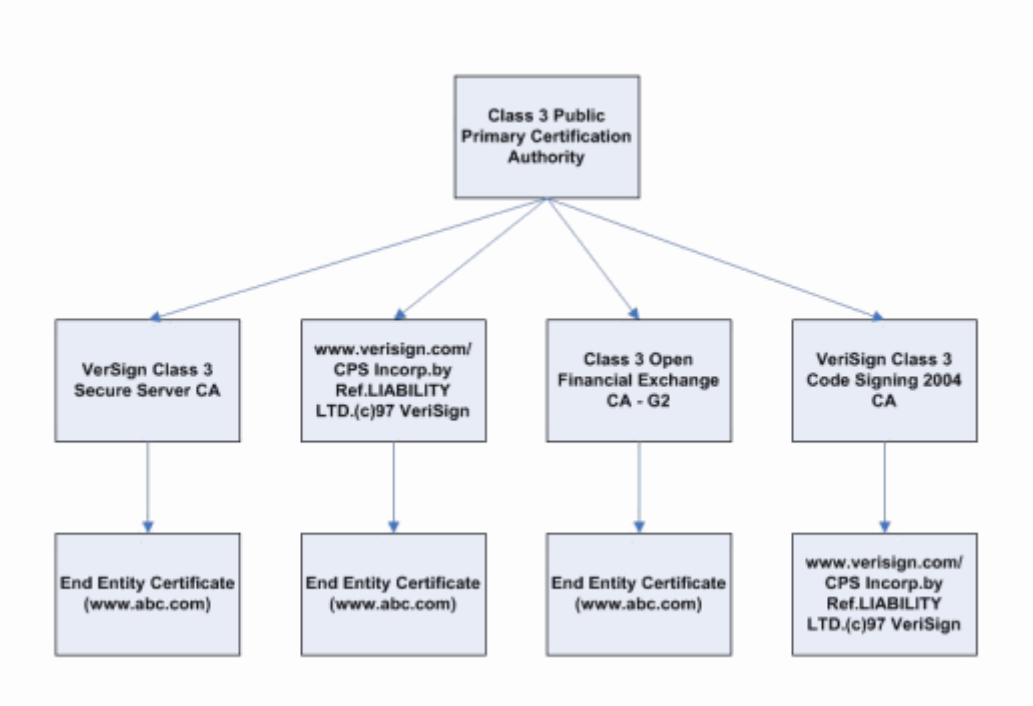


GlobalSign Organisation SSL

GlobalSign Extended Validation SSL

NOT yours
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

VeriSign har siden april 2006 anvendt ”Chained root” modellen, til alle deres SSL produkter. Deres ”Certificate Authority” (CA) struktur ser ud som følger.



Hvad er fordelene?

Den primære fordel med et ”Chained root” udstedt certifikat er at klienten stoler lige så meget på det som et ”Single root” certifikat, men sikkerheden for udsteder certifikatet og derved også serverens certifikat, er højere. Typisk vil certifikat udstedere der ikke har brugt en masse penge på at få næsten alle deres underudsteder certifikater installeret i alle klienter (som VeriSign), være billigere at købe.

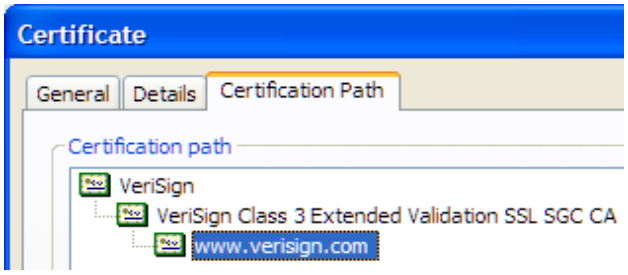
Hvad er ulemperne?

Der skal installeres alle underudsteder (”Intermediate root Certificate Authority”) certifikater på serveren, hvor certifikatet skal anvendes. Dette er for at klienten selv kan hente dette, samtidigt med selve certifikatet. På en typisk server tager det under et minuts tid at installere.

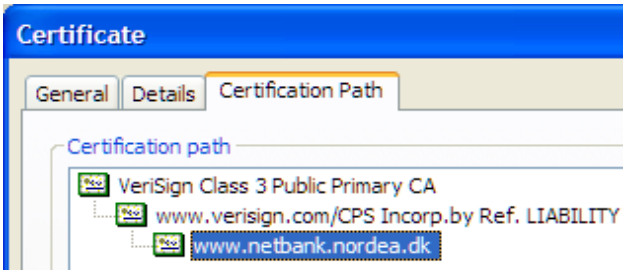
NOT yours
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Sammenlign udstedere

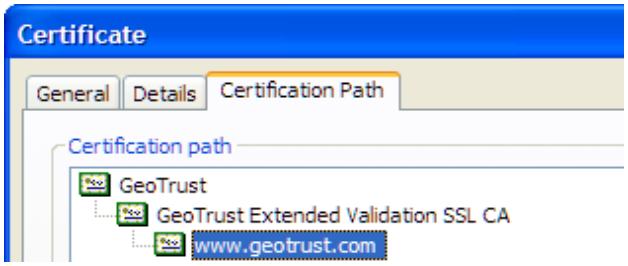
Herunder har vi samlet nogle eksempler på hvordan certifikater er udstedt, bemærk at det er meget få certifikater der er udstedt af rod certifikatet direkte.



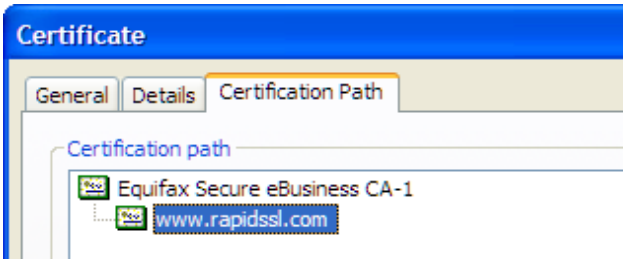
VeriSign anvender et EV certifikat og bliver derfor nødt til at anvende et chained certifikat.



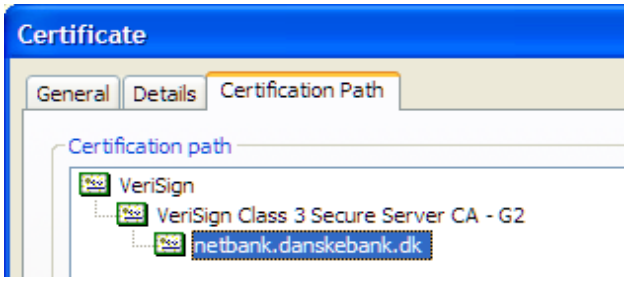
Nordea's netbank anvender et chained VeriSign certifikat.



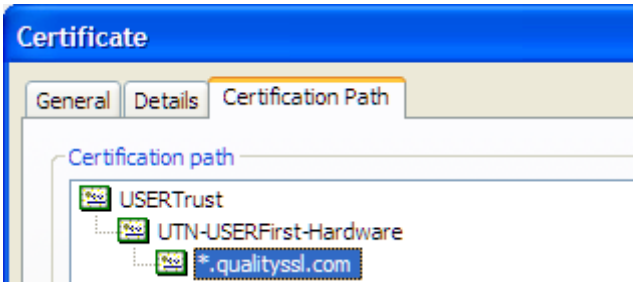
GeoTrust anvender et EV certifikat og bliver derfor nødt til at anvendet et chained certifikat.



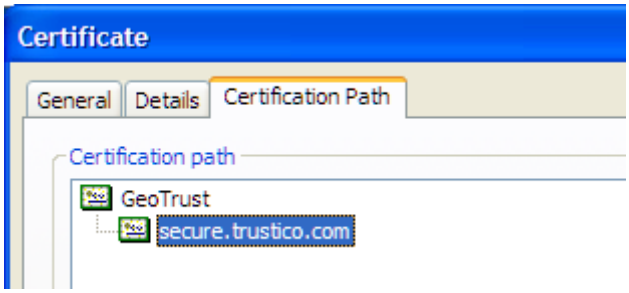
RapidSSL anvender rod certifikatet direkte uden en underudsteder.



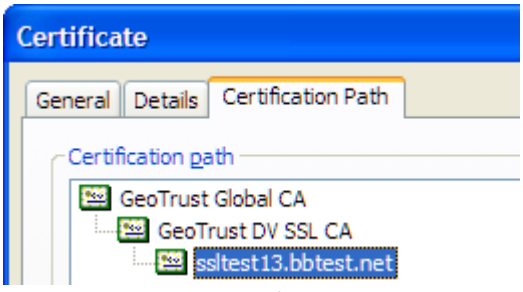
Danske Bank anvender et rod certifikat, fordi både rod og mellemcertifikatet er installeret i klienten.



QualitySSL er selv en underudsteder til en anden udsteder og ejer derfor ikke selv deres rod certifikat.



Dette eksempel er på et GeoTrust QuickSSL Premium certifikat. *(fra før den 22. juli 2010)*



Dette er et eksempel på et GeoTrust QuickSSL certifikat. *(fra efter den 22. juli 2010)*

NOT yours
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Extended Validation udstedere

Samtlige udstedere af EV certifikater, anvender en ”Chained root” model, grundet det højere krav til sikkerhed.

”Chained root” certifikat udstedere

Næsten samtlige certifikat udstedere anvender i dag ”Chained root” modellen, nogle har dog fået installeret nogle underudsteder certifikater i nogle klienter, men underudsteder certifikatet bør stadig installeres på serveren, for at sikre fuld kompatibilitet med samtlige klienter.

Følgende certifikat udstedere anvender ”Chained root” modellen.

- VeriSign
- GlobalSign
- AlphaSSL
- DigiCert
- Comodo
- GoDaddy
- QualitySSL (bemærk ejer ikke sin egen CA)
- Thawte (skiftede 27. juni 2010)
- GeoTrust (skiftede 22. juli 2010)

”Single root” certifikat udstedere

Følgende certifikat udstedere anvender ”Single root” modellen, bemærk at de ikke beskytter roden med ”Chained root” modellen.

- RapidSSL (skifter i løbet af 2010)