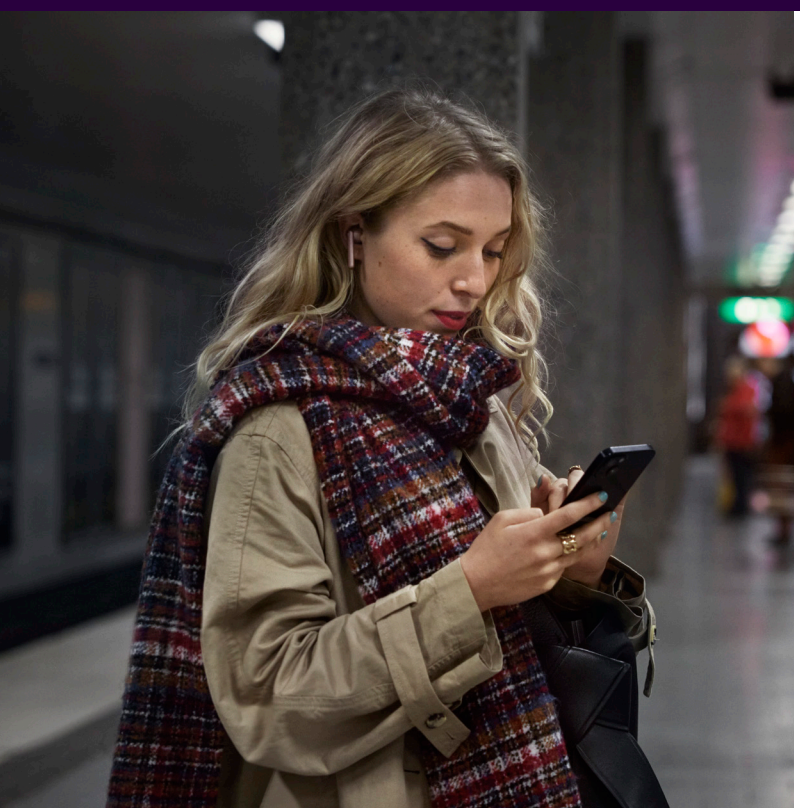
Har du koll på dina certifikat?

Secured by Telia Cygate

Mycket inom IT märks först när det slutar fungera. Certifikat är ett sådant område. De är en förutsättning för att system ska kunna identifiera varandra, kommunicera säkert och fungera som de ska, men får sällan någon uppmärksamhet så länge allt fungerar. Nu förändras förutsättningarna snabbt.

Tidigare har certifikat haft giltighetstider på över ett år. Nu kortas de successivt, och inom några år kan vi se intervall ner mot cirka 47 dagar. Det innebär att något som tidigare hanterades en gång per år behöver göras betydligt oftare, och antalet tillfällen där något kan gå fel ökar.

Hela den digitala tilliten bygger på vem som utfärdar certifikaten. I många fall ligger den kontrollen idag utanför både organisationen, landet och Europa. Det gör att vi nu ser två risker växa samtidigt: en operativ och en strukturell.



Vad är ett certifikat?

Ett digitalt certifikat är en identitet som används för att verifiera vem eller vad som kommunicerar, och för att kryptera trafiken mellan dem.

“Certifikat är lås och nycklar i den digitala världen”.

Det är certifikatet som gör att en webbplats visar ett hänglås. Men det är också ett fungerande certifikat som gör att system kan lita på varandra, att API:er fungerar och att interna tjänster kan kommunicera säkert.

Tekniskt sett är det en liten fil, men i praktiken är det en grundförutsättning för att digitala tjänster ska fungera.

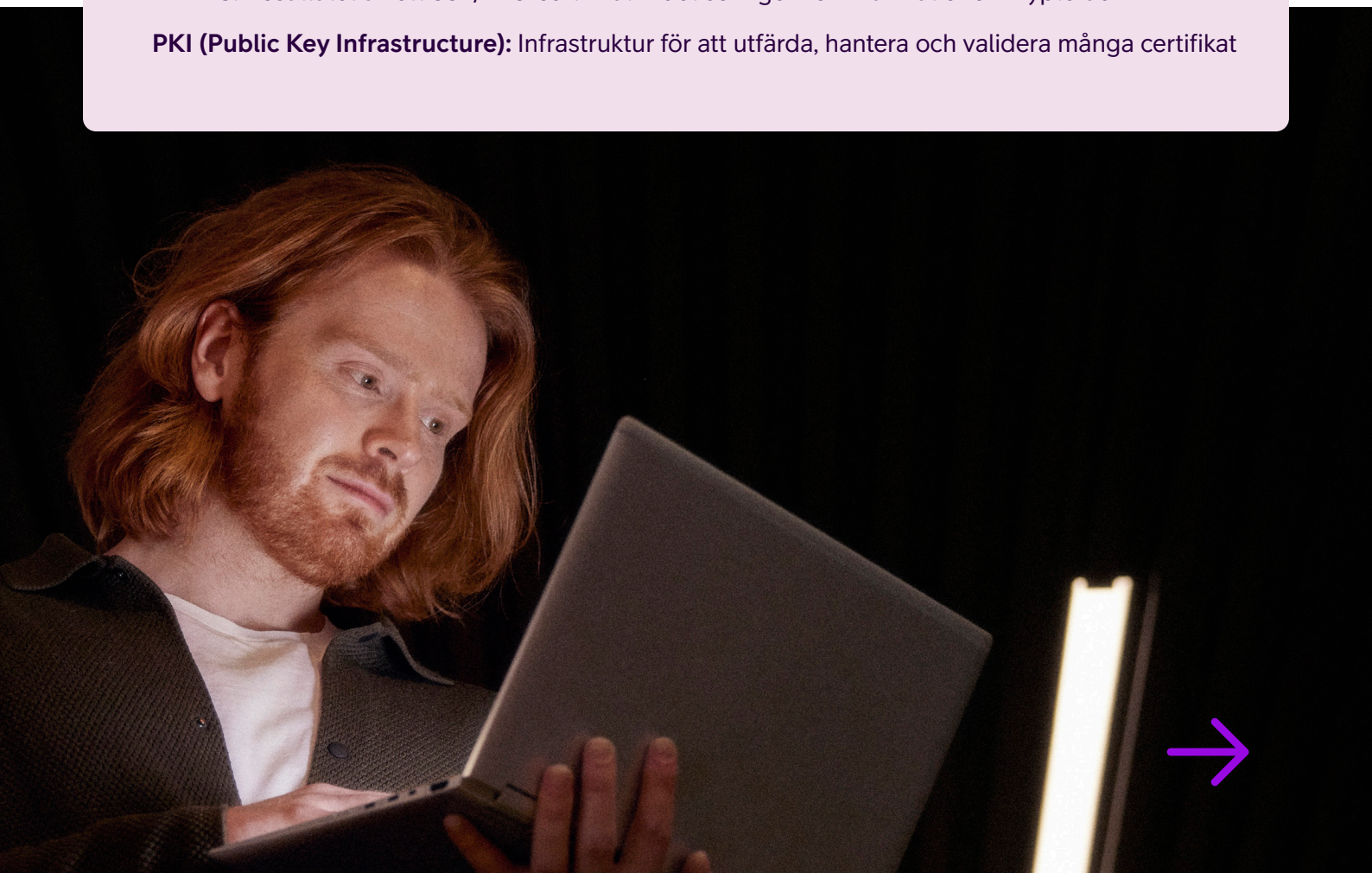
Begrepp att känna till:

Certifikat: Samlingsnamn för digitala identiteter

SSL/TLS-certifikat: Typ av certifikat för säkra webbplatser

HTTPS: Resultatet av ett SSL/TLS-certifikat – det som gör kommunikationen krypterad

PKI (Public Key Infrastructure): Infrastruktur för att utfärda, hantera och validera många certifikat



Du använder fler certifikat än du tror

Certifikat förknippas ofta med webben, men används i betydligt större omfattning i system som kommunicerar med varandra, i molntjänster och integrationer, i interna nätverk och i allt från IoT-enheter till produktionsmiljöer. Det är också här konsekvenserna blir störst när något går fel.

När ett certifikat i en webbplats går ut syns det direkt. När ett certifikat i en intern integration slutar fungera bryts i stället flöden mellan system. Data levereras inte, tjänster kan inte starta och beroenden faller utan en tydlig felbild.

> **“När certifikaten inte stämmer slutar systemen prata med varandra.”**

I mer komplexa miljöer kan hela kedjor av system påverkas. När certifikat slutar fungera bryts kommunikationen mellan system, vilket i praktiken innebär att integrationer stannar, inloggningar misslyckas och automatiserade flöden avbryts. I verksamhetskritiska miljöer kan konsekvenserna bli omfattande, från avbrott i interna processer till påverkan på produktion eller samhällstjänster.

Det handlar inte bara om funktion, utan också om förtroende. Även om problemet åtgärdas snabbt påverkar det hur tjänsten upplevs.

Ett felmeddelande eller en varning om att en sida inte är betrodd räcker för att skapa osäkerhet både hos kunder, invånare och internt i organisationen.

Nu blir manuella rutiner tyngre

I många organisationer har certifikat hanterats utan tydlig struktur. De har förnyats manuellt, ofta först när problem uppstått, vilket har fungerat eftersom giltighetstiderna varit långa och problemen uppstått sällan.

När giltighetstiderna nu kortas, i vissa fall ner mot cirka 47 dagar, förändras förutsättningarna. Samma uppgift behöver utföras betydligt oftare, vilket gör manuell hantering svår att överblicka.

”Med 100 maskiner och cirka 10 minuter per certifikat motsvarar det omkring 17 timmars arbete per år vid årlig förnyelse. När certifikat i stället behöver förnyas ungefär var 47:e dag kan det öka till över 130 timmar per år”, säger Fredrik Månsson, Säkerhetsexpert på Telia Cygate.

Det som tidigare tog begränsad tid kan därmed börja ta en påtaglig del av arbetstiden. Samtidigt är det en repetitiv uppgift som i grunden inte kräver avancerad kompetens, men som ändå ofta hanteras av kvalificerade resurser.

När frekvensen ökar gör även risken för misstag det, eftersom varje moment innebär en potentiell felkälla när människor är inblandade.

Tillit, beroenden och suveränitet

Certifikat är grunden för digital tillit och bygger på förtroendet för den aktör som utfärdar dem. I många fall är den aktören extern och global. Det innebär ett beroende som inte alltid är synligt, men som påverkar både säkerhet och kontroll.

“Om du inte kontrollerar tilliten – kontrollerar du inte heller systemen.”

För organisationer med höga krav på säkerhet, regelefterlevnad eller samhällskritiska funktioner blir det därför allt viktigare att förstå och kunna påverka denna del av infrastrukturen.

I det sammanhanget blir valet av certifikatutfärdare avgörande. Telia är Nordens enda ETSI-certifierade utfärdare. Det innebär att våra publika TLS-certifikat uppfyller Europas högsta säkerhetskrav och att certifikat från Telia Cygate är förankrade i en nordisk infrastruktur, med kontroll över hela tillitskedjan.

Det minskar beroendet av externa aktörer och skapar bättre förutsättningar för att hantera både säkerhet och kontinuitet över tid.

Dags att ta kontroll

Certifikat behöver hanteras som en tillgång, med tydligt ägarskap och ett arbetssätt som förebygger problem.

Att ha kontroll innebär att ha:

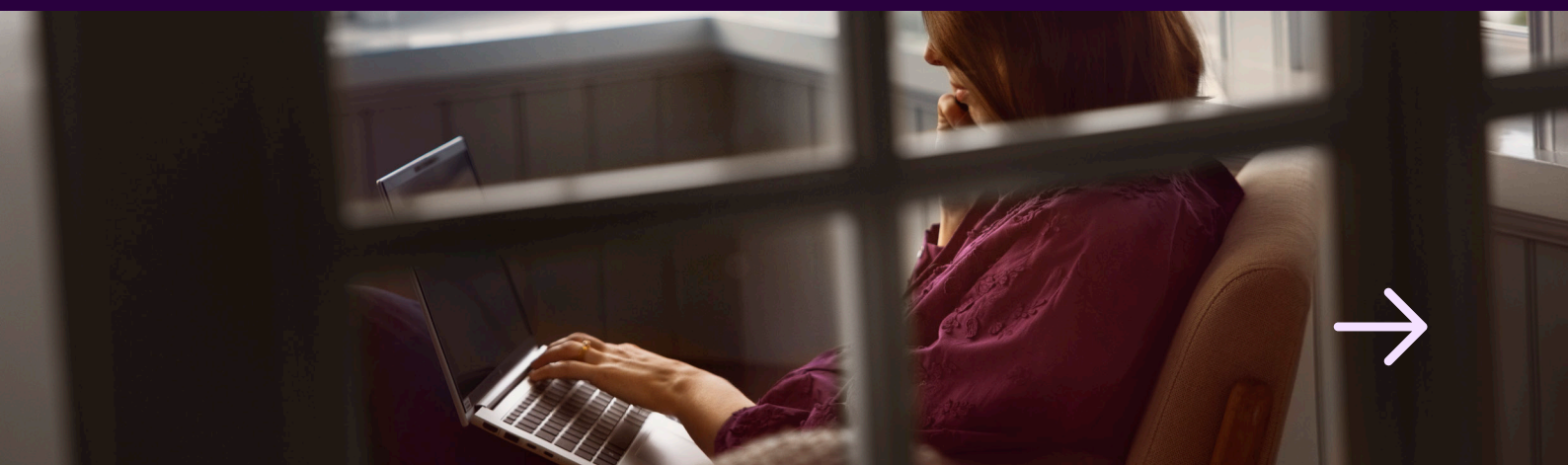
- ⟶ Överblick över vilka certifikat som finns
- ⟶ Kunskap om var de används och vad de påverkar
- ⟶ Kontroll över giltighetstider och beroenden
- ⟶ Tydliga processer för hela livscykeln

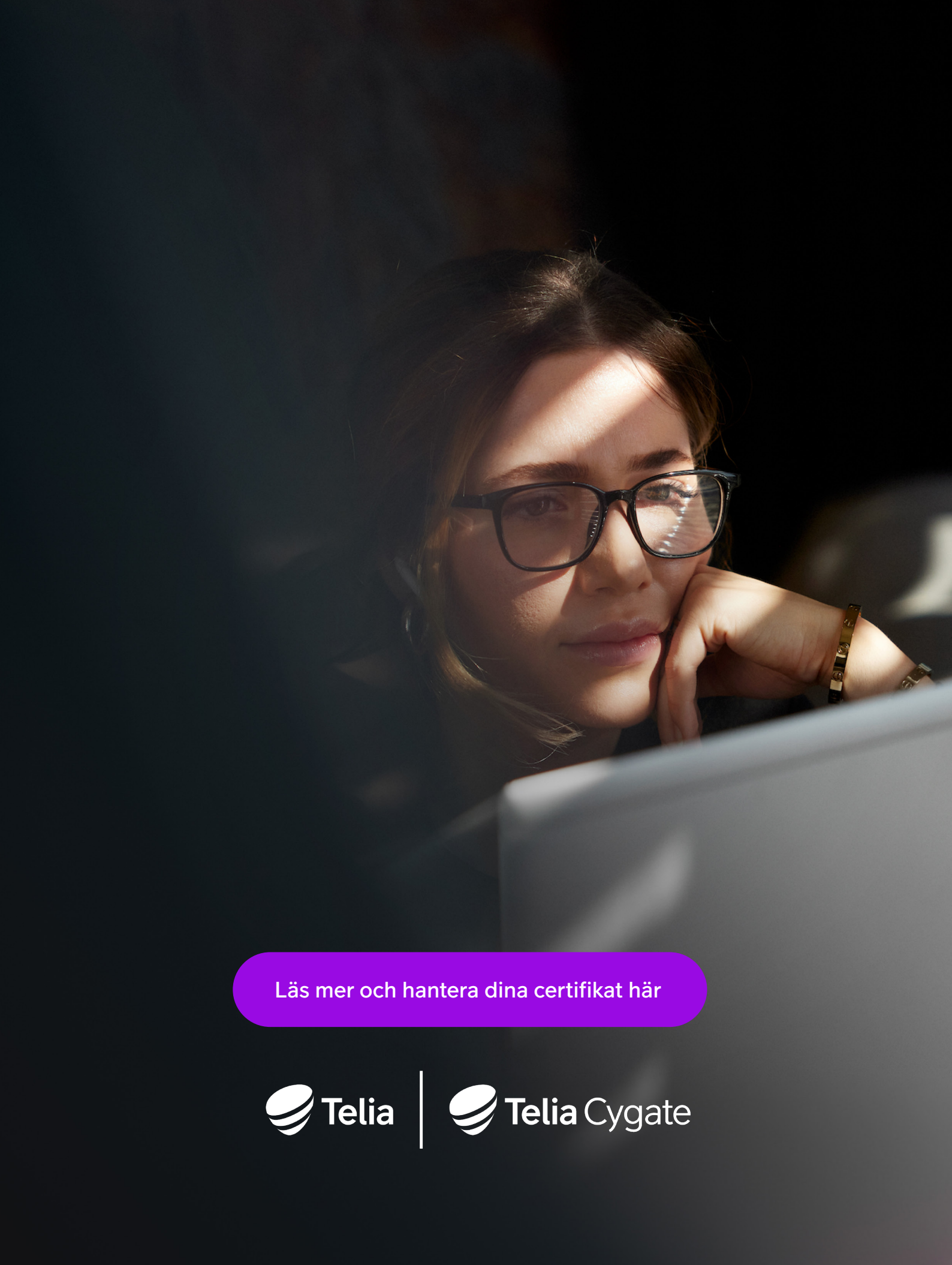
För många organisationer börjar arbetet med att skapa denna överblick. Därefter behöver hanteringen gå från manuell och ad hoc till strukturerad och automatiserad. Automatisering gör det möjligt att hantera förnyelser utan manuella moment, vilket minskar risken för fel och skapar stabilitet över tid.

“Certifikat har blivit en driftfråga.”

Telia Cygates certifikatfabrik är ett exempel på en sådan förmåga. Genom att automatisera utfärdande, förnyelse och hantering av certifikat skapas en stabil grund för digital tillit där certifikaten fungerar som de ska, utan att bli en återkommande operativ risk.

Samtidigt erbjuder Telia en flexibel pay-per-use-modell, där du bara betalar för de certifikat som faktiskt används. Det gör det möjligt att anpassa hanteringen efter behov, utan förskottsbetalning eller låsta volymer.




Läs mer och hantera dina certifikat här
Telia
Telia Cygate