Certifikattjänster

1.1.2024

MDB Nationell Stäm-peltjänst

Säkerhetskrav för stämpeltjäns-tens klientmiljö

1.1.2024

Dokumenthantering

Ägare	Annika Gibson
Utarbetats av	Annika gibson
Granskats av	
Godkänts av	

Versionshantering

versions nr	vad som har gjorts	datum/person
v 1.0	Dokument skapat	1.1.2024

Innehållsförteckning

MDB Nationell Stämpeltjänst

1 Inledning

1.1 Syfte

I detta dokument presenteras lägsta säkerhetskrav för en kund som begär signaturer via REST-gränssnittet hos MDB:s stämpeltjänst. I kraven ingår:

- Fysisk säkerhet
- Nätverkssäkerhet
- Maskinvarusäkerhet
- Plattformssäkerhet
- Programvarusäkerhet

Kraven definieras för att skydda stämpeltjänsten samt kundens klientmiljö och hemliga uppgifter (som privata nycklar och liknande icke-offentlig information), enheter och nätverk.

Kunden behöver sätta sig in i kraven, genomföra de säkerhetskontroller som krävs och även tillhandahålla bevis på att säkerhetskontrollerna har genomförts innan de skickar begäran om signering genom REST-gränssnittet.

1.2 Process för granskning av efterlevnad

Syftet med granskningen av efterlevnad är att säkerställa att kunden följer kraven i detta dokument och att säkerhetskontrollerna används och fungerar.

Granskningen av efterlevnad består av följande steg:

1. MDB tillhandahåller klienten detta dokument och tillhörande checklista för klientmiljö gäller säkerhetskrav
2. Kunden kontrollerar statusen på befintliga säkerhetskontroller mot det här dokumentet och genomför nödvändiga säkerhetskontroller vid behov
3. Kunden fyller i checklista för klientmiljö vad gäller säkerhetskrav och lämnar den till MDB.
4. MDB granskar den ifyllda checklistan, ger feedback och hjälper vid behov kun-den att implementera de säkerhetskontroller som saknas
5. MDB godkänner checklistan för klientmiljö vad gäller säkerhetskrav när nödvändiga säkerhetskontroller är på plats.

Checklistan innehåller följande information:

- **ID:** Hänvisning till avsnittsnummer i detta dokument

- **Krav:** Hänvisning till kravets namn
- **Använd kontroll:** Markera det krav som kunden har uppfyllt, det vill säga att kunden har uppfyllt de säkerhetskontroller som hör till kravet.
- **Beskrivning:** Kort beskrivning av genomförda säkerhetsåtgärder (eller en beskrivning av varför säkerhetsåtgärderna inte tillämpas)

1.3 Dokumentets upplägg och anteckningar

Kraven är uppdelade i ”Beskrivning”, ”Bakgrund” och ”Exempel” enligt följande principer:

- ”Beskrivning” innehåller det faktiska kravet
- ”Bakgrund” förklarar varför kravet finns
- ”Exempel” innehåller möjliga sätt att genomföra en säkerhetskontroll för att upp-fylla kravet

Dokumentet tar upp två olika typer av krav: **obligatoriska** och **frivilliga**.

- **Obligatoriska** krav är markerade med ordet ”SKA” i kravbeskrivningen.
- De delar av ett krav som är **frivilliga** och som Insta rekommenderar markeras med ordet ”BÖR” eller ”REKOMMENDERAS” i kravbeskrivningen.

2 Allmänna säkerhetskrav

2.1.1 Beskrivning

Klientmiljön (klientservrar som, från det programvarupaket som ska signeras, skapar en hashsumma och skickar till stämpeltjänsten, HSM, som lagrar viktigt material etc.) SKA endast användas till att signera koder som relaterar till åtgärder. Dessa åtgärder kan vara:

- autentisering till stämpeltjänsten
- nyckelmaterial för hosting (exempelvis autentiseringsnyckel)
- att skapa en hashsumma från det programvarupaket som ska signeras
- att skicka begäran om signering (hashsumma) till IOSS och mottagande

2.1.2 Bakgrund

Klientmiljön används i säkerhetssyfte och bör därför hållas så enkel och koncis som möjligt. Klientmiljön innehåller hemliga uppgifter som exempelvis privata nycklar för gränssnittscertifikat. Om klientmiljön används som en delad resurs för andra ändamål och processer kan den komma att påverkas och därför inte fungera som avsett.

3 Krav på fysisk säkerhet

3.1 Begränsning i fysisk åtkomst till klientmiljön

3.1.1 Beskrivning

Klientmiljön (inklusive, men inte begränsat till klientmiljö-servern och HSM) SKA skyddas från obehörig åtkomst. Det SKA finnas fysiska säkerhetskontroller som förebygger, förhindrar och upptäcker obehörig användning, tillägnande eller avslöjande av känslig information och system i klientmiljön. Detta krav BÖR också tillämpas för remote-system som administrativa distansarbetsplatser.

3.1.2 Bakgrund

Om klientmiljön är tillgänglig för ”vem som helst” utan några fysiska säkerhetsbegränsningar kan den påverkas av fientliga aktörer som avslöjar känslig information och bryter dess integritet. Kravet ställs för att säkerställa att obehöriga inte får tillgång till hårdvaran, att flyttbar media inte används och att obehörig användning upptäcks.

3.1.3 Exempel

- Lista över personal som har tillgång till systemet.
- Portar och dörrar som förhindrar åtkomst till systemen.
- 2FA används för att komma in i byggnaden
- Ingångar övervakas med videokameror och vid eventuellt säkerhetsbrott skickas automatisk notifikation
- När någon går in i eller ut ur byggnaden loggas detta automatiskt.
- Vakter kontrollerar identiteteten innan någon släpps in i byggnaden

3.2 Begränsad fysisk åtkomst till säkerhetskopierat material för klientmiljön

3.2.1 Beskrivning

Säkerhetskopierat material i klientmiljö SKA skyddas från obehörig åtkomst. Det SKA finnas fysiska säkerhetskontroller som förebygger, förhindrar och upptäcker obehörig användning eller tillägnande av säkerhetskopierat material.

3.2.2 Bakgrund

Säkerhetskopior förvaras vanligtvis på annan plats så att de finns tillgängliga om den primära byggnaden skulle förstöras. Säkerhetskopiorna innehåller lika känslig information som den klientmiljön som är i bruk, och måste därför förvaras lika säkert.

3.2.3 Exempel

- Lista över personal som har tillgång till systemet.
- Portar och dörrar som förhindrar åtkomst till systemen.
- 2FA används för att komma in i byggnaden
- Åtkomst till säkerhetskopior övervakas och loggas.

- Ingångar övervakas med videokameror och vid eventuellt säkerhetsbrott skickas automatisk notifikation
- När någon går in i eller ut ur byggnaden loggas detta automatiskt.
- Vakter kontrollerar identiteteten innan någon släpps in i byggnaden.

4 Säkerhetskrav för maskinvara

4.1 Maskinvara avsedd för klientmiljön

4.1.1 Beskrivning

System som används vid signeringsbegäran BÖR installeras på maskinvara som endast används för signering.

4.1.2 Bakgrund

klientmiljön används i säkerhetssyfte och därför bör attackvektorer hållas på minimal nivå. När klientmiljön används på avsedd maskinvara kommer säkerhetsproblem eller fel i andra operativsystems, exempelvis hög resursförbrukning, inte att påverka den.

4.1.3 Exempel

- klientmiljö-server (operativsystem och programvara) är installerad på avsedd maskinvara
- klientmiljö-server (operativsystem och programvara) är installerad på virtuell dator. Den virtuella miljön innehåller endast andra virtuella servrar som används för att signera (exempelvis säkerhetskopieringssystem, klientmiljö i viloläge, belastningsutjämning)

5 Nätverkssäkerhetskrav

5.1 Skyddad koppling mellan klientmiljön och stämpeltjänsten

5.1.1 Beskrivning

Kommunikationen mellan klientmiljön och stämpeltjänsten SKA skyddas med hjälp av branschgodkända och beprövade algoritmer för att hålla begäran om signering och svar skyddade från ändringar och avslöjanden.

5.1.2 Bakgrund

Huvudorsaken till att skydda kommunikationen mellan stämpeltjänsten och klientmiljön är att säkerställa att stämpeltjänsten är kopplad till en känd part.

5.1.3 Exempel

- VPN (TLS / IPSec) mellan klientmiljön och stämpeltjänsten med hjälp av algoritmerna EC P-384 / AES-256 / SHA-384.

5.2 Endast klientmiljön är kopplad till stämpeltjänsten

5.2.1 Beskrivning

Endast kopplingar som klientmiljön initierar SKA skickas från klientmiljön till stämpeltjänsten. I praktiken ska klientmiljöns nätverk segmenteras/skyddas/begränsas så att endast klientmiljö-server/-servrar kan kommunicera med stämpeltjänsten via VPN-tunneln.

5.2.2 Bakgrund

Klientmiljö-servern är den enda komponenten i klientmiljön som behöver kopplas till stämpeltjänsten. Andra servrar och bärbara datorer i klientmiljön behöver inte denna anslutning och bör alltså inte kopplas till stämpeltjänsten. Kopplingen bör avbrytas i klientmiljö-nätverket.

5.3 Säker koppling till klientmiljön

5.3.1 Beskrivning

Närverket i klientmiljön SKA minimeras och skyddas mot vanliga nätverksattacker. Lägsta säkerhetskrav för nätverket i klientmiljön är:

- Åtkomst till nätverket i klientmiljön SKA skyddas så att inte fler klientmiljö-tjänster än nödvändigt utsätts för externa nätverk.
- Enheter för gränskontroll som används för att skydda närverket SKA stoppa alla tjänster som inte är nödvändiga från att ta sig in i och ut ur klientmiljön.
- Om klientmiljö-servern eller andra komponenter i klientmiljön används på distans SKA kommunikationen mellan kontaktpunkten på distans och klientmiljön säkras.
    - Distansarbetsplatser för administrativt arbete

Distanstjänst (exempelvis fabrikskund) som ber klientmiljön om certifikat.

5.3.2 Bakgrund

klientmiljön innehåller känslig information som måste skyddas. Genom att begränsa antalet attackvektorer, exempelvis från onödiga tjänster, minskar risken för fientliga intrång i systemet, samtidigt som verksamheten kan fortsätta som planerat.

5.3.3 Exempel

- Nätverket delas av en brandvägg, vilket gör att klientmiljö-enheter finns i en egen skyddad del
- Nätverket begränsas av en brandväggslösning som endast accepterar att nödvändiga system ansluts.
- IDS- och IPS-enheter finns på plats för att förhindra/avslöja vanliga nätverksattacker.

6 Operativsystemkrav

6.1 Åtkomst till klientmiljö-operativsystem begränsas av lämpliga mekanismer

6.1.1 Beskrivning

Åtkomst till klientmiljöns operativsystem SKA skyddas med lämpliga mekanismer så att endast behörig personal kan logga in till systemet. Minimikraven är följande:

- När lösenord används som hemlig inloggning SKA tillräckliga lösenordsprinciper tillämpas.
    - Ett lösenord måste vara tillräckligt långt
    - Ett lösenord måste vara komplext
- Åtkomst SKA beviljas endast efter behov.
- Åtkomst till systemet SKA övervakas genom att åtkomst till systemet loggas.
- Åtkomstbehörigheter granskas regelbundet och personal som inte längre behöver åtkomst till systemet fråntas denna (exempelvis på grund av ändrade arbetsuppgifter eller pensionsavgångar)

2FA-lösningar REKOMMENDERAS

6.1.2 Bakgrund

Klientmiljöns operativsystem kan användas för att påverka Klientmiljöns åtgärder (exempelvis avslöjande av känslig information eller framtvingande av certifikatbegäran). Därför bör så få betrodda medarbetare som möjligt ha tillgång till systemet.

6.1.3 Exempel

- Lösenord ska innehålla minst 12 tecken och ha lösenfras i stället för lösenord
- Inloggningen är baserad på Smart Card.
- Åtkomst till klientmiljön ges utifrån AD-grupper som granskas regelbundet.
- Inloggningar på klientmiljö-OS loggas och skickas vidare till externa platser med hjälp av syslog.

6.2 Antal behörigheter till klientmiljön minimeras

6.2.1 Beskrivning

Behörigheter till klientmiljön SKA hållas på miniminivå. Detta är minimikraven för att hantera behörigheter till klientmiljön.

- All personal SKA använda därför avsett inloggningskonto i stället för vanligt konto (som root).
- Alla användare (personer) SKA ha separata inloggningskonton, delade konton FÅR INTE användas för inloggning.

- Administrativa behörigheter till klientmiljö-OS SKA endast ges till administrativ personal.
- Vid behov SKA det finnas separata tjänstekonton, tjänster ska inte använda root/administrator-kontot.
- Förhöjda behörigheter (som sudo eller administrator) SKA endast användas vid behov.

6.2.2 Bakgrund

När antalet behörigheter till systemet hålls nere så minskar även risken för felaktiga konfigurationer och missbruk.

6.3 Klientmiljöns operativsystemet minimeras

6.3.1 Beskrivning

Operativsystemet SKA minimeras så att det endast innehåller nödvändiga applikationer och tjänster. Minimikraven omfattar

- Alla onödiga nätverksportar och tjänster SKA inaktiveras och tas bort från systemet.
- Tjänster och applikationer BÖR inte läggas till med hjälp av standardkonfigurationen. I stället SKA konfigurationen kontrolleras och verifieras så att extra funktioner tas bort från tjänsterna.
    - Tjänsten SSH kan innehålla osäkra konfigurationer när endast standardkonfigurationen används.
- USB-portar SKA inaktiveras om de inte har en tydlig funktion i verksamheten.

6.3.2 Bakgrund

Huvud-gateway för attacker mot klientmiljön är tjänster där klientmiljön är värd. Genom att ta bort alla onödiga portar och tjänster från systemet minimeras antalet attackvektorer, vilket försvårar genomförande av fientliga attacker.

6.4 Klientmiljöns operativsystem uppdateras regelbundet

6.4.1 Beskrivning

Operativsystem SKA regelbundet uppdateras. Särskilt säkerhetsuppdateringar BÖR installeras i systemet så snart som möjligt. Uppdateringarna BÖR hämtas från en central plats inom företaget, exempelvis WSUS eller Spacewalk.

6.4.2 Bakgrund

Att hålla systemet ordentligt uppdaterat kan bidra till att skydda välkända svagheter.

6.4.3 Exempel

- Operativsystem uppdateras varje månad eller när en större säkerhetsuppdatering finns tillgänglig.

- Operativsystemets uppdateringar hanteras centralt och aktuell uppdateringsstatus för olika operativsystem är alltid känd.

6.5 Klientmiljöns operativsystem granskas

6.5.1 Beskrivning

Åtgärder på operativsystemsnivå SKA granskas och loggas. Loggen ska innehålla minst följande:

- Inloggning till OS och utloggning från OS
- Ändringar i åtkomstkontroll
- Förhöjd behörighet från normal användare till administrativ användare
- Behörig användares aktivitet (kommandon), exempelvis installation av mjukvara
- Misslyckat / obehörigt försök till åtkomst
- Ändringar i administrativa behörigheter
    - till exempel sudoers

Användning av centraliserad loggserver via en krypterad anslutning REKOMMENDERAS, i stället för att lagra loggar på den lokala servern.

6.5.2 Bakgrund

Inhämtning av systemhändelser ger systemadministratörerna information så att de kan avgöra om det sker obehörig åtkomst till deras system.

6.5.3 Exempel

- Händelser i operativsystemet samlas in med hjälp av rsyslog. Loggar vidarebefordras till centralt logghanteringssystem.

6.6 Klientmiljöns operativsystem övervakas och skyddas mot skadliga program

6.6.1 Beskrivning

Ett lämpligt säkerhetsverktyg BÖR användas för att skydda operativsystemet från skadliga program. Dessa verktyg kan omfatta lokala antivirussystem, host-baserade skyddssystem eller nätverksbaserade system som märker att en host (server) har angripits.

6.6.2 Bakgrund

Antivirus och andra liknande HIPS-produkter förhindrar att vanliga skadliga program sprids och orsakar problem i andra delar av den säkra miljön.

6.6.3 Exempel

- Lokala operativsystem skyddas med HIPS.
- IDS-enhet på klientmiljöns nätverksaviseringar, exempelvis möjliga angrepp från skadliga program.