# Modèles de certificats avec des configurations non sécurisées

ID METSYS : 6  
ID PingCastle : [A-CertTempCustomSubject](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID PurplKnight : [Modèles de certificats qui permettent aux demandeurs de spécifier un subjectAltName](https://www.purple-knight.com/fr/security-indicators/), [Certificate templates with three or more insecure configurations](https://www.purple-knight.com/fr/security-indicators/)  
ID ANSSI : [vuln1\_vuln\_adcs\_template\_auth\_enroll\_with\_name](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#vuln_adcs_template_auth_enroll_with_name)

Charge de travail : 1 jour  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

Les configurations suivantes d'un modèle de certificat peuvent être exploitées par des adversaires :

• L'approbation du responsable est désactivée - les nouveaux certificats sont automatiquement approuvés si l'utilisateur dispose des droits d'inscription corrects.

• Aucune signature autorisée n'est requise - les CSR (Certificate Signing Requests) ne sont pas signées par un certificat autorisé existant.

• SAN (Subject Alternative Name) activé - permettant au créateur d'un modèle de certificat de spécifier le « subjectAltName » dans le CSR, ainsi ils peuvent effectuer la demande en se faisant passer pour n'importe qui, même un administrateur de domaine.

• EKU (Enhanced Key Usage) d'authentification présent - s'il est présent, l'EKU créé à partir du modèle de certificat permettra à l'utilisateur de s'authentifier avec celui-ci.

****Recommandation****

Plusieurs actions peuvent être entreprises pour rendre les modèles de certificats moins vulnérables :

• Activer l'approbation du responsable - veillez à ce que l'approbation du responsable soit activée et requise pour le certificat, et approuvez chaque demande manuellement après l'avoir examinée.

• Aucune signature autorisée n'est requise - il est recommandé de le régler sur 1, de manière que chaque demande soit signée par un certificat autorisé.

• SAN activé - évaluez si le certificat doit spécifier un « subjectAltName », et le cas échéant, désactivez cette option.

• EKU d'authentification présent - assurez-vous que le modèle de certificat est utilisé uniquement pour l'authentification. Par exemple, un certificat utilisé uniquement pour la signature de code ne doit pas être utilisé également pour l'authentification.