AUTHENTIFICATION MULTIFACTEUR FORTE SMARTCARD PIV DANS UN DOMAINE WINDOWS

DESCRIPTION DU THÈME

Propriétés	Description
Intitulé long	Déploiement d'une solution d'authentification MFA forte dans un domaine Microsoft Windows.
Formation(s) concernée(s)	☐ Classes de première Sciences et technologies du management et de la gestion (STMG) ☐ Terminale STMG Système d'information de gestion (SIG) ☒ BTS Services Informatiques aux Organisations
Matière(s)	☐ Sciences de gestion ☐ SIG ☐ Bloc 1 – Support et mise à disposition de services informatiques ☒ Bloc 2 SISR – Administration des systèmes et des réseaux ☒ Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	L'objectif de ce « labo » est de mettre en place une authentification MFA forte sans mot de passe (passwordless) pour les comptes Administrateurs du domaine dans un environnement Microsoft Windows. Ce labo sera également l'occasion d'introduire la notion de tiering Microsoft ainsi que de remobiliser les savoirs et compétences autour des stratégies de groupe et de la cryptographie.
Compétences	**2.2 Installer, tester et déployer une solution d'infrastructure réseau** • Installer et configurer des éléments d'infrastructure • Tester l'intégration et l'acceptation d'une solution d'infrastructure • Déployer une solution d'infrastructure **3.3 Sécuriser les équipements et les usages des utilisateurs** • Identifier les menaces et mettre en œuvre les défenses appropriées • Gérer les accès et les privilèges appropriés • Vérifier l'efficacité de la protection
Prérequis	Les fondamentaux en matière d'administration Windows Server (AD, GPO). Les fondamentaux en matière de cryptographie (symétrique, asymétrique, fonction de hachage, autorité de certification, certificats SSL/TLS). Les fondamentaux en matière d'authentification MFA (TP Bloc 3 SIO 1 publié par le réseau CERTA sur le sujet).

Outils	Un serveur Windows 2022 ou 2025 Standard. Au minimum deux postes clients Windows 11 Pro Au minimum une Yubikey 5
Mots-clés	PKI, GPO, MFA, Certificats X509, Tiering
Durée	6 heures
Auteur·e·s	Quentin Demoulière avec la relecture et les précieux conseils de David Balny, Jérôme Bezet-Torres et Michel Vienne
Version	V1.0
Date de publication	Mars 2026

DERNIÈRES RÉVISIONS

Ce tableau contient les modifications apportées au document après sa publication uniquement.

Date	Auteur·e	Description

CONTEXTE

L'authentification est une préoccupation majeure du responsable de la sécurité du système d'information (RSSI) de l'entreprise CUB. En effet, suite à une prestation de tests d'intrusion réalisée par un prestataire nommé HackBoost, le système d'information a été compromis via l'un des comptes "Administrateurs du domaine" .

Parmi les préconisations émanant du rapport d'audit, il est suggéré de mettre en place une authentification multifacteur forte pour tous les comptes "Administrateurs du domaine". Votre responsable de la sécurité du système d'information (RSSI) vous demande de choisir une solution adaptée puis de produire un PoC (Proof of Concept) au sein de votre agence.

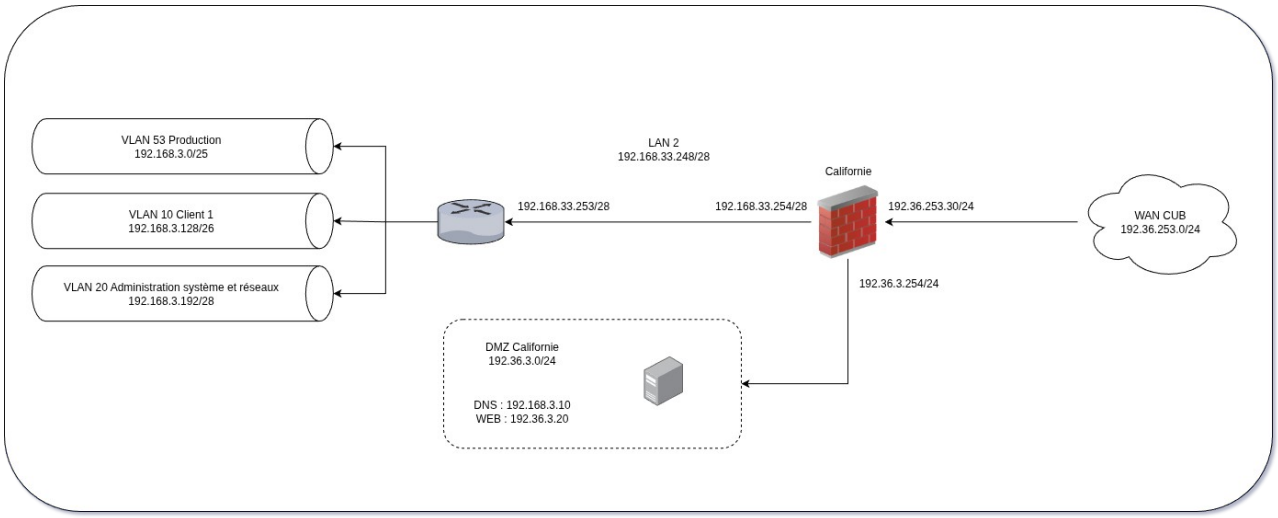

Figure 1: Schéma réseau logique d'une agence de l'entreprise CUB

a) Pourquoi l'authentification par login et mot de passe est problématique pour se connecter avec un compte "Administrateur du domaine" ?

b) Donner la définition d'une authentification multifacteur forte.

PRÉREQUIS

La fiche 1 est à mobiliser dans cette partie.

- Un serveur Windows 2022 ou 2025 contrôleur de domaine.
- Au minimum deux machines clientes Windows 11 intégrées au domaine.
- Une clé de sécurité matérielle Yubikey 5 NFC.
- Le pilote Minidriver Yubikey Smart Card installé sur les machines où l'authentification par certificat sera effective (poste d'administration et contrôleur de domaine).

⚠ Attention ! Avant de commencer l'activité, veillez à ce que le code PIN et le code PUK de la clé de sécurité pour l'authentification par certificats (SmartCard/PIV) soient changés.

c) Quelles sont les fonctions du code PIN et du code PUK ?

d) Pourquoi est-il obligatoire de les modifier avant de mettre en œuvre la nouvelle authentification ?

CHOIX DE LA SOLUTION

Après avoir pris en compte les différentes solutions techniques à votre disposition, deux solutions attirent l'attention de la DSI :

- Authentification TOTP.
- Authentification par certificat X509 et clé privée (SmartCard/PIV).stockés sur une clé de sécurité matérielle (ex : Yubikey, Nitrokey).

Lors d'une analyse de risques, plusieurs scénarios sont évoqués par votre RSSI :

Après exfiltration d'un couple login et mot de passe concernant un utilisateur, un attaquant se rend compte qu'un code à usage unique généré sur le smartphone de la victime est nécessaire pour s'authentifier sur son webmail.

e) Proposer une attaque (en dehors du vol du téléphone) lui permettant d'obtenir ce code à usage unique.

Un attaquant souhaite compromettre le compte d'un utilisateur « Administrateur du domaine » qui s'authentifie sur le contrôleur de domaine Windows à l'aide d'un certificat X509, d'une clé privée stockés sur une clé de sécurité matérielle et accessibles à l'aide d'un code PIN.

f) Comment l'attaquant peut-il obtenir l'accès au compte « Administrateur du domaine » ciblé dans cette situation ?

g) Expliquer pourquoi l'authentification TOTP est jugée moins robuste que l'authentification par certificat X509 stocké sur une clé ?

MISE EN PLACE DU POC

La fiche 6 est à mobiliser dans cette partie.

A PARAMÉTRAGE DE L'AD

Sur le prototype que vous réalisez, dans l'annuaire Active Directory présent sur le contrôleur de domaine, il vous est demandé de mettre en place l'arborescence suivante :

racineAD

|___ AdminSys (Unité d'organisation)

|____ Utilisateurs (Unité d'organisation)

|____ Ordinateurs (Unité d'organisation)

|____ Tier0 (Unité d'organisation)

|____ Tier2 (Unité d'organisation)

|____ Serveurs (Unité d'organisation)

| |____ Tier0 (Unité d'organisation)

| |____ Tier1 (Unité d'organisation)

|____ Admins

|____ Tier0 (Unité d'organisation)

|____ Tier1 (Unité d'organisation)

|____ Tier2 (Unité d'organisation)

Ensuite, vous devez créer les comptes suivants pour le même utilisateur à savoir Roger Sanchez :

- rsanchez dans l'UO Adminsys/Utilisateurs.
- sanchezadmt0 dans l'UO Adminsys/Admins/Tier0 et membre du groupe Admins du domaine ;
- sanchezadmt1 dans l'UO Adminsys/Admins/Tier1.
- sanchezadmt2 dans l'UO Adminsys/Admins/Tier2.

Le compte sanchezadmt0 devra faire partie du groupe "Administrateurs du domaine"

g) Pourquoi le RSSI vous a-t-il conseillé de créer 4 comptes distincts (utilisateur standard, admin tier 2, admin tier 1 et admin tiers 0) pour le même collaborateur Roger Sanchez, Administrateur Système de l'entreprise ?

> **NB :** L'objet de cette activité n'est pas d'aborder en détail le concept de sécurité "Tiering" développé par Microsoft. Néanmoins, y faire référence semble indispensable.

Parmi les 2 clients Windows 11, l'un est considéré comme un poste d'administration. Il est donc nécessaire de le placer dans l'UO Adminsys/Ordinateurs/Tiers0. Le second est considéré comme un poste utilisateur pour les AdminSys. Il faudra le déplacer dans l'UO Adminsys/Ordinateurs/Tiers2.

h) Expliquer ce qu'est un poste d'administration et pourquoi est-il placé dans cette unité d'organisation.

> **Important !** Ne déplacez jamais les contrôleurs de domaine dans l'UO Adminsys/Serveurs/Tiers0. Même si cela est tentant, ils doivent absolument rester dans l'UO Contrôleurs de domaine. On placera dans cette UO les serveurs les plus critiques type PKI, serveurs de sauvegarde, hyperviseurs, etc.

B MISE EN PLACE D'UNE AUTORITÉ DE CERTIFICATION INTERNE (PKI)

La fiche 2 est à mobiliser dans cette partie.

Dans ce prototype, l'autorité de certification interne sera installée sur le serveur contrôleur de domaine.

> **Attention !** En production, il est recommandé d'installer le rôle AD CS (PKI) sur un serveur dédié et renforcé pour des raisons de sécurité.

i) Quelle est la fonction d'une PKI ?

j) Quel est l'intérêt de disposer d'une PKI interne plutôt que de certificats auto-signés dans une organisation ?

Installer et configurer la PKI interne.

> **Attention !** Lors des différentes phases de test, le choix d'utiliser l'algorithme de chiffrement ECDSA pour la génération de la clé privée a posé problème. Nous recommandons, dans le cadre de l'activité, le choix de RSA bien qu'il soit considéré comme moins robuste.

k) Lors de la création de la clé privée de la PKI, est-il préférable de choisir la fonction de hachage SHA1 ou SHA256 ? Votre réponse devra notamment fournir une définition du concept de collision.

C PARAMÉTRAGE DE LA PKI INTERNE POUR L'AUTHENTIFICATION PAR CERTIFICATS ET CLÉ MATÉRIELLE

La fiche 3 est à mobiliser dans cette partie.

Activez l'authentification par carte à puce pour la PKI nouvellement installée.

D MISE EN PLACE DES STRATÉGIES DE GROUPE

La fiche 4 est à mobiliser dans cette partie.

À l'aide de la fiche 4 sur les GPO :

- Autorisez l'usage de certificats générés à partir d'algorithme de chiffrement à courbes elliptiques (ECC) pour l'ordinateur d'Administration.
- Forcez le verrouillage de session si la clé de sécurité matérielle est retirée de l'ordinateur d'Administration après authentification .
- Autorisez l'auto-inscription pour le compte sanchezadmt0 et l'ordinateur d'Administration.
- Le compte sanchezadmt0 n'est autorisé à se connecter que sur l'ordinateur d'Administration.
- Forcez l'authentification SmartCard/PIV pour empêcher toute authentification par mot de passe pour le compte sanchezadmt0.
- Interdire la connexion avec le compte sanchezadmt0 sur le poste client standard.
- Interdire la connexion avec des utilisateurs non admin du domaine sur le poste d'administration.

> **NB :** Les bonnes pratiques Microsoft, recommande de dissocier les stratégies de groupe appliquées aux ordinateurs et aux utilisateurs. Vous veillerez à respecter cette recommandation lors de l'implémentation de ces dernières.

l) Déterminer le nombre de stratégies de groupe à créer et où elles devront être positionnées (domaine, unité d'organisation).

RÉALISATION DE LA RECETTE

Les fiches 5 et 6 sont à mobiliser dans cette partie.

Vérifiez que la nouvelle politique d'authentification demandée est opérationnelle :

- Authentification pour le compte sanchezadmt0 uniquement avec un certificat installé sur une clé de sécurité matérielle depuis l'ordinateur d'administration.

m) Expliquer techniquement de façon synthétique comment fonctionne cette authentification par certificat et clé de sécurité matérielle.

n) Pourquoi la nouvelle authentification est une authentification multifacteur forte.