AYI NEDJIMI Consultants

MFA résistant au phishing : FIDO2, Passkeys et au-delà

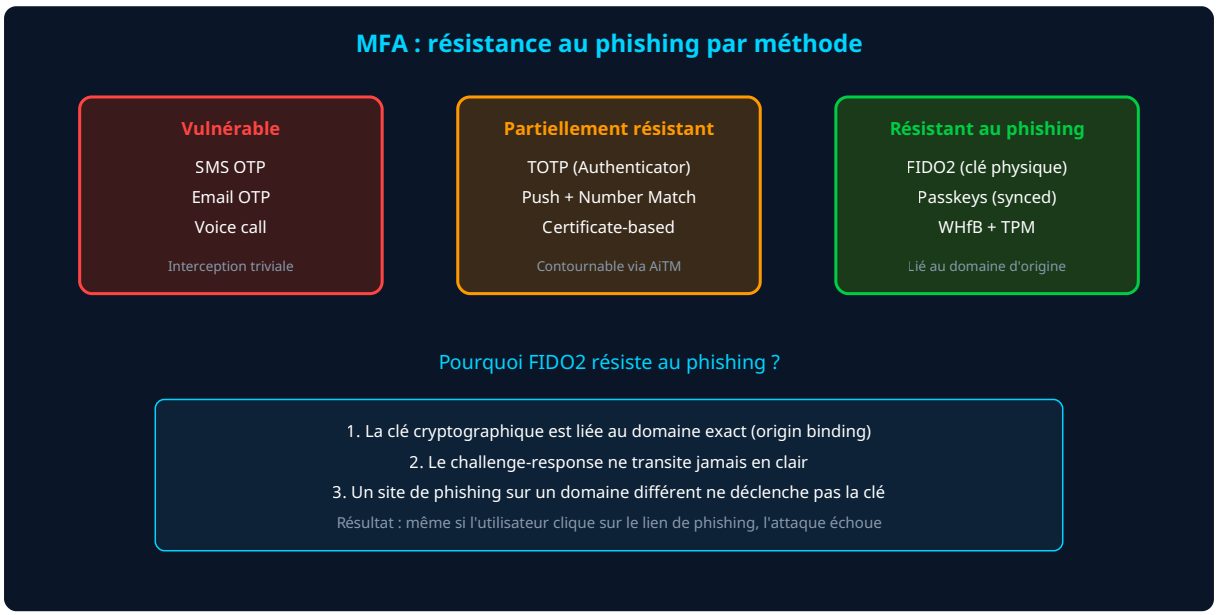
Catégorie : IAM et Gestion des Identités Lecture : 6 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

FIDO2, Passkeys, WebAuthn : guide technique pour déployer un MFA résistant au phishing et éliminer les attaques par interception de tokens et SMS.

Le MFA traditionnel ne suffit plus. Les attaques de type Adversary-in-the-Middle (AiTM) contournent les codes OTP et les notifications push avec une facilité déconcertante. En 2025, les kits de phishing comme EvilGinx et Modlishka ont rendu ces techniques accessibles à des attaquants de niveau intermédiaire. Face à cette réalité, les méthodes d'authentification résistantes au phishing deviennent une nécessité absolue. FIDO2, Passkeys, WebAuthn — ces standards redéfinissent la sécurité de l'authentification en éliminant le vecteur d'interception à sa source. Ce guide vous accompagne dans la compréhension technique de ces protocoles, le choix du matériel adapté, les stratégies de déploiement et les retours d'expérience terrain. Nous aborderons aussi les limites actuelles et les solutions de contournement pour les cas d'usage où le passwordless n'est pas encore viable. L'objectif est de vous donner les clés pour migrer progressivement vers une authentification forte qui résiste aux techniques d'attaque modernes, sans paralyser la productivité de vos équipes.

Points clés à retenir

- Les attaques **AiTM** contournent les MFA classiques (SMS, OTP, push) en interceptant les tokens de session
- **FIDO2/WebAuthn** est le seul standard MFA véritablement résistant au phishing
- Les **Passkeys** démocratisent FIDO2 en supprimant le besoin de clé physique dédiée
- Le déploiement se fait en mode hybride : FIDO2 pour les admins, Passkeys pour les utilisateurs, fallback conditionnel
- Microsoft, Google et Apple supportent nativement les Passkeys depuis 2024



Anatomie d'une attaque AiTM contre le MFA classique

Pour comprendre pourquoi FIDO2 est nécessaire, il faut d'abord comprendre comment les attaques AiTM contournent le MFA classique. L'attaquant déploie un reverse proxy (EvilGinx, Muraena) qui se positionne entre la victime et le site légitime. La victime accède à une page de phishing qui ressemble au portail Microsoft 365. Elle entre son identifiant, son mot de passe, puis son code MFA. Le proxy transmet tout en temps réel au vrai site, récupère le token de session authentifié et le redirige vers l'attaquant. Résultat : l'attaquant a un accès complet au compte, **MFA contourné**.

Cette technique fonctionne contre le SMS OTP, le TOTP (Google Authenticator, Microsoft Authenticator), les push notifications et même le number matching. Le point commun : ces méthodes ne vérifient pas que la requête provient bien du domaine légitime. Seules les méthodes basées sur la cryptographie à clé publique liée au domaine résistent. Les attaques par mot de passe deviennent encore plus dangereuses quand le MFA classique est le seul rempart.

FIDO2 et WebAuthn : comment ça fonctionne

Le standard *FIDO2* repose sur deux composants : **WebAuthn** (l'API navigateur) et **CTAP2** (le protocole de communication avec l'authenticator). Lors de l'enregistrement, le navigateur génère une paire de clés cryptographiques liée au domaine exact (origin). La clé privée reste sur l'authenticator (clé USB, TPM du terminal, enclave sécurisée du smartphone). Seule la clé publique est envoyée au serveur.

Lors de l'authentification, le serveur envoie un challenge aléatoire. Le navigateur vérifie que le domaine correspond à celui de l'enregistrement (origin binding), puis transmet le challenge à l'authenticator qui le signe avec la clé privée. La signature est vérifiée côté serveur avec la clé publique. Un site de phishing sur `micros0ft-login.com` ne déclenchera jamais la clé enregistrée pour `login.microsoftonline.com`. C'est cette liaison cryptographique au domaine qui rend FIDO2 fondamental dans une architecture Zero Trust.

Passkeys : la démocratisation du passwordless

Les *Passkeys* sont l'évolution grand public de FIDO2. La différence principale : les Passkeys peuvent être synchronisées entre les appareils d'un même écosystème (iCloud Keychain pour Apple, Google Password Manager pour Android/Chrome, Windows Hello pour Microsoft). Cette synchronisation résout le problème majeur de FIDO2 pur : la perte ou l'oubli de la clé physique. Un utilisateur qui perd son iPhone peut restaurer ses Passkeys sur un nouvel appareil via sa sauvegarde iCloud.

En entreprise, cette synchronisation pose une question de gouvernance : qui contrôle les clés ? La FIDO Alliance a défini deux types de Passkeys. Les **device-bound passkeys** (non synchronisées) restent sur l'appareil physique — c'est l'équivalent d'une clé FIDO2 classique. Les **synced passkeys** se répliquent dans le cloud du fournisseur. Pour les populations à risque (administrateurs, dirigeants), les device-bound passkeys sur clé physique YubiKey restent la recommandation. Pour les utilisateurs standards, les synced passkeys offrent un excellent compromis sécurité/ergonomie.

Stratégie de déploiement en entreprise

Le déploiement du MFA phishing-resistant suit une logique de segmentation par risque. Les comptes à **privilèges élevés** (admins IT, comptes de service critiques) migrent en premier vers des clés FIDO2 physiques (YubiKey 5 NFC, Feitian BioPass). Budget : 50 à 70€ par clé, deux clés par utilisateur (principale + backup). Les comptes gérés par le PAM intègrent la clé FIDO2 dans le workflow d'authentification au bastion.

Les utilisateurs standards migrent vers les Passkeys synchronisées sur leurs terminaux professionnels gérés par **Intune** ou un autre MDM. La migration se fait en mode opt-in d'abord (campagne de communication, portail d'enregistrement self-service) puis en mode enforcement progressif. Prévoyez une phase de cohabitation de 3 à 6 mois où les anciennes méthodes MFA restent disponibles comme fallback conditionnel (accès limité, session restreinte).

Population	Méthode recommandée	Budget/utilisateur	Délai déploiement
Admins IT / Global Admins	YubiKey 5 FIDO2 (x2)	100-140€	2-4 semaines
Dirigeants / VIP	YubiKey 5 NFC + Passkey	70-100€	4-6 semaines
Utilisateurs bureau	Windows Hello + Passkey	0€ (intégré)	2-3 mois
Utilisateurs mobiles	Passkey iOS/Android	0€ (intégré)	2-3 mois
Sous-traitants / externes	TOTP + accès restreint	0€	1-2 semaines

Configuration Entra ID pour FIDO2 et Passkeys

La configuration FIDO2 dans Entra ID se fait en trois étapes. D'abord, activez la méthode d'authentification FIDO2 dans le portail Entra (Authentication methods > FIDO2 security key). Restreignez les modèles de clé autorisés par AAGUID pour n'accepter que les clés certifiées (YubiKey, Feitian, Thales). Ensuite, créez une politique d'accès conditionnel exigeant un **authentication strength** de type « Phishing-resistant MFA » pour les applications sensibles.

La fonctionnalité **Authentication Strengths** (GA depuis 2023) permet de créer des profils personnalisés. Pour les accès admin : exigez FIDO2 uniquement. Pour les accès utilisateur standard : acceptez FIDO2 ou Passkeys ou Windows Hello for Business. Pour les accès externes : configurez un accès conditionnel avec MFA standard et session restreinte. La documentation Microsoft détaille chaque combinaison possible.

Gestion des cas d'usage problématiques

Certains scénarios résistent encore au passwordless. Les environnements hybrides avec Entra Connect nécessitent une double configuration (on-premise + cloud) pour le FIDO2. Les applications legacy qui n'implémentent pas WebAuthn requièrent un fallback vers des méthodes moins robustes — dans ce cas, limitez l'accès à ces applications via des politiques d'accès conditionnel restrictives (terminal conforme obligatoire, plage IP restreinte).

Les comptes de service ne peuvent pas utiliser FIDO2 par définition (pas d'interaction humaine). Pour ces comptes, la gestion des secrets via un vault avec rotation automatique reste l'approche appropriée. Les salles de réunion partagées, les kiosques et les postes en libre-service nécessitent des approches spécifiques : badge NFC + PIN, QR code temporaire ou authentification déléguée via un terminal personnel.

Questions fréquentes sur le MFA résistant au phishing

Que se passe-t-il si un utilisateur perd sa clé FIDO2 ?

C'est pourquoi chaque utilisateur doit disposer de deux clés : une principale et une de secours stockée en lieu sûr. En cas de perte des deux clés, un processus de récupération avec vérification d'identité renforcée (en personne ou visioconférence avec pièce d'identité) permet de réenregistrer de nouvelles clés. Ce processus doit être documenté et testé avant le déploiement. Les Passkeys synchronisées réduisent ce risque puisqu'elles sont sauvegardées dans le cloud.

FIDO2 fonctionne-t-il avec les applications on-premise ?

Oui, via plusieurs mécanismes. Les applications web on-premise qui supportent SAML ou OIDC peuvent utiliser FIDO2 via Entra ID comme IdP fédéré. Pour RDP, Windows Hello for Business avec clé FIDO2 permet une authentification passwordless sur les serveurs on-premise. Les applications legacy sans support SAML/OIDC nécessitent un reverse proxy ou un portail SSO qui gère la conversion d'authentification.

Quel est le coût total d'un déploiement FIDO2 pour 1000 utilisateurs ?

Pour 1000 utilisateurs avec un mix clés physiques (200 admins/VIP) et Passkeys logicielles (800 utilisateurs), comptez environ 25 000 à 35 000€. Ce budget inclut les clés physiques (200 x 2 clés x 60€ = 24 000€), la configuration Entra ID (intégrée aux licences E3/E5), la conduite du changement et la formation (5 000 à 10 000€). Le ROI se mesure en incidents de phishing évités : une seule compromission de compte admin coûte en moyenne 150 000€ à remédier.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et feuille de route

Le MFA résistant au phishing n'est plus un luxe réservé aux grandes entreprises. Les Passkeys démocratisent cette technologie en la rendant accessible sans matériel dédié. Votre feuille de route : déployez FIDO2 sur les comptes à privilèges dans les 30 jours, lancez le pilote Passkeys pour les utilisateurs standards dans les 90 jours, généralisez dans les 6 mois. Chaque compte migré vers le passwordless est un vecteur de phishing en moins. La direction est claire, les outils sont prêts — il ne manque que votre décision de lancer le projet.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr