L'histoire des systèmes MFA

Stéphane FOSSE
fosse.fr

19 janvier 2026

L'authentification multi-facteurs (MFA) transforme aujourd'hui notre rapport au numérique, mais ses racines remontent aux années 1960. Cette technologie, née des contraintes du partage d'ordinateurs et de l'automatisation bancaire, a évolué pour devenir le rempart essentiel contre les menaces numériques modernes. L'invention du premier mot de passe informatique en 1961 par Fernando Corbató au MIT a déclenché une course à l'innovation de six décennies, aboutissant aux passkeys et à l'authentification comportementale par intelligence artificielle de 2025.

Cette évolution s'articule autour de quatre révolutions technologiques majeures : l'informatisation des systèmes bancaires (1960-1980), l'invention des mots de passe à usage unique (1980-1995), la standardisation internet (1995-2010), et la démocratisation mobile (2010-2025). Chaque époque a apporté ses innovations techniques, motivées par des menaces sécuritaires émergentes et des contraintes technologiques spécifiques.

1 Les origines pré-informatiques et l'invention du mot de passe numérique

1.1 L'automatisation bancaire pionnière (1960-1967)

L'histoire moderne de l'authentification multi-facteurs débute avec l'invention du premier distributeur automatique de billets le 27 juin 1967 [1]. John Shepherd-Barron, ingénieur chez De La Rue Instruments, inaugure cette révolution à la succursale Barclays d'Enfield, au nord de Londres. Ce système combinait déjà deux facteurs d'authentification : un voucher papier imprégné de Carbon-14 pour la lisibilité machine et un code PIN à quatre chiffres.

Le choix du code à quatre chiffres mérite une attention particulière. Shepherd-Barron avait initialement conçu un système à six chiffres, mais sa femme Caroline lui fit remarquer qu'elle ne pourrait retenir que quatre chiffres maximum [2]. Cette anecdote illustre parfaitement l'équilibre permanent entre sécurité et expérience d'utilisation qui caractérise l'évolution des systèmes MFA, et plus généralement la sécurité.

Le premier DAB américain suit rapidement, le 2 septembre 1969, installé par Chemical Bank à Rockville Centre, Long Island [3]. Donald Wetzel, son inventeur chez Docutel, lance ce « Docuteller » avec le slogan prophétique : « Le 2 septembre, nos banques ouvriront à 9h et ne fermeront plus jamais. »

1.2 Fernando Corbató et la naissance du mot de passe informatique (1961)

Parallèlement à ces innovations bancaires, Fernando José Corbató révolutionne l'informatique au MIT en novembre 1961 avec la première démonstration du Compatible Time-Sharing System (CTSS) [4]. Face au défi du partage d'ordinateurs mainframe coûteux entre multiples utilisateurs, Corbató invente le premier système de mots de passe informatique.

« Le problème clé était que nous installions plusieurs terminaux qui devaient être utilisés par plusieurs personnes, mais chaque personne ayant son propre ensemble de fichiers privés », explique Corbató dans ses mémoires. Cette innovation, récompensée par le prix Turing en 1990, établit le concept fondamental de confidentialité numérique.

L'histoire prend une tournure inattendue dès 1962 : Allan Scherr, doctorant au MIT, devient le premier « hacker » informatique documenté en accédant illégalement aux fichiers de mots de passe pour obtenir plus de temps d'utilisation [5]. Cette première violation illustre la course permanente entre sécurité et malveillance qui motive l'évolution constante des systèmes d'authentification.

1.3 Les contraintes techniques de l'époque

Les années 1960-1970 imposent des contraintes techniques drastiques qui façonnent ces premières innovations. Les ordinateurs mainframe, d'un coût prohibitif, doivent être partagés entre dizaines d'utilisateurs. Le stockage se limite à des disques partagés non protégés, les communications s'effectuent par modems 1 200-2 400 bauds, lents et peu fiables.

Ces limitations techniques expliquent les choix d'époque : cartes perforées pour la programmation, bandes magnétiques pour le stockage, jetons physiques parfois radioactifs (Carbon-14) pour l'authentification. Le courrier postal reste même nécessaire pour le retour des jetons DAB défaillants, illustrant l'infrastructure hybride physique-numérique de cette période fondatrice.

2 L'âge d'or de l'innovation cryptographique (1970-1987)

2.1 RSA et les fondements mathématiques modernes

La révolution cryptographique de 1977 transforme radicalement le paysage sécuritaire. Durant le week-end de Pâques 1977, Ronald Rivest, incapable de dormir après une soirée, formalise en une nuit l'algorithme RSA qui changera la cryptographie mondiale [6]. Avec Adi Shamir et Leonard Adleman, il jette les bases mathématiques de la sécurité informatique moderne.

La création de RSA Data Security en 1982 dans l'appartement d'Adleman marque le début de l'industrie commerciale de la cryptographie. L'entreprise frôle cependant la faillite, les ordinateurs des années 1980 manquant de puissance de calcul pour exploiter efficacement ces innovations.

Le sauvetage arrive en 1986 avec Jim Bidzos, qui transforme RSA en leader mondial malgré l'opposition farouche de la NSA [6]. Les « Crypto Wars » des années 1990 opposent l'industrie technologique aux agences gouvernementales, Bidzos luttant notamment contre le projet Clipper Chip de contrôle gouvernemental du chiffrement.

2.2 L'émergence des premiers jetons d'authentification

Kenneth Weiss révolutionne l'authentification pratique en 1984 avec la fondation de Security Dynamics Technologies [6]. Son innovation majeure, le jeton SecurID, combine un dispositif de la taille d'une carte de crédit avec un écran LCD générant des codes pseudo-aléatoires toutes les 60 secondes.

Le brevet fondamental US 4 720 860, déposé en novembre 1984 et accordé en janvier 1988, décrit un « appareil pour la génération électronique et la comparaison de codes non-prédictibles utilisant des variables statiques et dynamiques » [7]. Cette innovation technique établit le principe durable de l'authentification à deux facteurs : PIN (ce que vous savez) + tokencode (ce que vous avez).

L'acquisition de RSA Data Security par Security Dynamics en 1996 pour 251 millions de dollars consacre cette révolution. RSA SecurID domine rapidement le marché avec plus de 70% des parts en 2003, produisant 25 millions de dispositifs avant 2010 [6].

3 L'invention théorique des mots de passe à usage unique (1981)

3.1 Leslie Lamport et les fondements mathématiques

Leslie B. Lamport publie « Password Authentication with Insecure Communication » en novembre 1981 dans Communications of the ACM [8]. Cette recherche fondamentale au MIT établit les bases mathématiques des One-Time Passwords modernes.

L'innovation de Lamport repose sur les fonctions de hachage à sens unique appliquées de manière répétée. Son schéma utilise une fonction f appliquée 1 000 fois à une graine initiale s, générant $f^{999}(s)$, $f^{998}(s)$, etc. Cette approche mathématique résout définitivement le problème des mots de passe statiques vulnérables aux écoutes réseau.

Lamport, récompensé par le prix Turing 2013 pour ses contributions aux systèmes distribués, pose les fondements théoriques qui permettront toutes les innovations pratiques ultérieures. Son travail inspire directement le développement du système S/KEY par Bellcore à la fin des années 1980 [9].

3.2 Les brevets fondamentaux de Kenneth Weiss

Au-delà de son rôle entrepreneurial, Kenneth Weiss accumule 22 brevets américains fondamentaux pour l'industrie MFA. Son portfolio inclut des innovations sur les systèmes de sécurité personnelle (US5361062A, 1993) et l'utilisation de jetons pour l'accès aux ressources (US5657388A, 1994) [10].

Ces brevets établissent les principes techniques durables : génération de codes temporels, synchronisation cryptographique, authentification multi-facteurs matérielle. L'influence de Weiss perdure aujourd'hui dans toutes les implémentations modernes de jetons d'authentification.

4 La standardisation internet et l'interopérabilité (1995-2010)

4.1 HOTP et TOTP : l'émergence des standards ouverts

L'initiative OATH (Open AuTHentication) de 2004 transforme un marché fragmenté en écosystème interopérable. David M'Raihi de VeriSign dirige le développement du standard HOTP, publié en décembre 2005 dans la RFC 4226 [11]. Cette innovation permet enfin l'interopérabilité entre différents fournisseurs de tokens et systèmes d'authentification.

HOTP établit un algorithme standardisé basé sur HMAC-SHA-1 avec compteur incrémental. L'extension TOTP (RFC 6238, mai 2011) remplace le compteur par un facteur temporel [12], simplifiant drastiquement l'expérience utilisateur en éliminant les problèmes de synchronisation.

Ces standards ouverts cassent le monopole des solutions propriétaires coûteuses. Les PME accèdent désormais à l'authentification forte, démocratisant une technologie précédemment réservée aux grandes entreprises.

4.2 L'évolution des codes SMS et email

Les années 1990 voient naître l'authentification par SMS et email. AT&T décrit dès 1996 un système d'autorisation basé sur l'échange de codes via des récepteurs bidirectionnels, déposant son brevet en mai 1995. Cette innovation transforme progressivement les téléphones mobiles en outils d'authentification.

L'adoption de l'email se développe parallèlement, initialement pour la réinitialisation de mots de passe avant d'évoluer vers des systèmes OTP complets au début des années 2000. Ces méthodes populaires révèlent cependant rapidement leurs failles : vulnérabilités SMS aux interceptions et SIM swapping, infrastructure non sécurisée des réseaux télécoms.

Le NIST recommande dès 2016 la dépréciation des SMS pour l'authentification, reconnaissant ces vulnérabilités structurelles. Cette prise de conscience accélère la transition vers des méthodes plus robustes.

4.3 Operation Aurora et l'adoption massive (2009-2010)

L'attaque Operation Aurora transforme définitivement l'industrie en janvier 2010 [13]. Cette cyberattaque sophistiquée contre Google et plus de 20 entreprises Fortune 100 exploite des vulnérabilités zero-day Internet Explorer et des techniques de spear-phishing avancées.

Les conséquences sont immédiates : Google lance l'authentification 2FA pour tous ses utilisateurs en 2011, déclenchant une prise de conscience industrielle de la vulnérabilité des mots de passe uniques. Cette attaque catalyse l'adoption massive MFA dans l'industrie technologique [14], établissant de nouvelles normes sécuritaires.

5 La révolution mobile et la démocratisation (2010-2025)

5.1 Google Authenticator et l'ère des applications mobiles

Google Authenticator, lancé en septembre 2010, démocratise définitivement l'authentification multi-facteurs [11]. Cette application mobile implémente les standards TOTP et HOTP ouverts, transformant les smartphones en jetons d'authentification universels.

Plus besoin de dispositifs hardware coûteux, les utilisateurs génèrent des codes OTP directement sur leurs téléphones. Google rend initialement l'application Android open source, favorisant l'adoption et l'innovation collaborative.

L'évolution vers la synchronisation cloud en avril 2023 marque une nouvelle étape, permettant la sauvegarde des codes sur les comptes Google. Cette fonctionnalité répond aux critiques d'utilisabilité tout en soulevant de nouveaux défis de sécurité.

5.2 L'écosystème concurrentiel des applications

Microsoft Authenticator, lancé sous le nom « Azure Authenticator » en juin 2015, introduit progressivement l'authentification passwordless et les notifications push [11]. Sa transition programmée vers Microsoft Edge pour l'autofill des mots de passe en juillet-août 2025 illustre l'intégration croissante des systèmes d'authentification dans les écosystèmes numériques.

Authy, développé par Twilio, se distingue par ses fonctionnalités avancées : synchronisation multi-appareils, sauvegardes chiffrées dans le cloud, support desktop (en fin de vie en 2024) [15]. Contrairement à Google Authenticator, Authy n'offre pas de fonction d'export, rendant la migration difficile et soulevant des questions de portabilité.

Duo Mobile, pionnier des notifications push dès 2011, modifie l'expérience utilisateur en permettant l'approbation d'authentification d'un simple tap [16]. Cette innovation élimine la saisie manuelle de codes, améliorant drastiquement l'utilisabilité tout en maintenant la sécurité.

5.3 La biométrie et WebAuthn

Touch ID (2013) et Face ID (2017) d'Apple font évoluer l'authentification grand public [17]. Touch ID introduit l'authentification par empreinte digitale avec l'iPhone 5S, tandis que Face ID utilise plus de 30 000 points infrarouges pour reconnaître le visage, offrant une sécurité statistiquement 20 fois supérieure.

Le standard WebAuthn/FIDO2, développé conjointement par la FIDO Alliance et le W3C, franchit une étape décisive en mars 2019 avec WebAuthn Level 1 [18]. Cette technologie permet l'authentification sans mot de passe utilisant la cryptographie à clés publiques, supportée nativement par Chrome, Firefox, Edge et Safari.

L'évolution vers l'authentification passwordless s'accélère en 2025 avec l'adoption massive des passkeys [18]. Cette approche élimine définitivement les mots de passe traditionnels, s'appuyant sur des clés cryptographiques uniques stockées localement sur les appareils.

6 Les défis sécuritaires contemporains et l'avenir de l'MFA

6.1 Menaces sophistiquées et contournements MFA

L'année 2024 révèle des menaces d'une sophistication inédite. Cisco Talos rapporte que 50% de leurs interventions impliquent des contournements MFA [19], principalement via des *fatigue attacks* (MFA bombing) et des techniques de *man-in-the-middle* (MITM).

Microsoft enregistre plus de 382 000 *fatigue attacks* MFA, exploitant la tendance humaine à approuver aveuglément les notifications répétées [20]. Ces « push bombing » représentent une vulnérabilité comportementale majeure des systèmes de notification, nécessitant des contre-mesures techniques et éducatives.

Le SIM swapping reste une menace persistante, exploitant les vulnérabilités des infrastructures télécoms. 28% des utilisateurs MFA demeurent ciblés par ces attaques de détournement de numéro, soulignant les limites des méthodes basées sur SMS.

6.2 L'intelligence artificielle et l'authentification comportementale

L'avenir de l'MFA s'oriente vers l'intelligence artificielle et l'authentification comportementale. Les systèmes 2025 analysent les patterns de frappe, de navigation et les comportements uniques pour une vérification continue pendant toute la session, dépassant la simple authentification à la connexion [21].

Cette approche promet de résoudre les vulnérabilités actuelles en créant des profils comportementaux uniques difficiles à reproduire. L'authentification devient invisible et continue, s'adaptant dynamiquement aux patterns individuels sans interrompre l'expérience utilisateur.

6.3 Tendances réglementaires et adoption industrielle

L'Executive Order 14028 américain impose l'MFA résistant au phishing pour toutes les agences fédérales d'ici fin 2024. Cette évolution réglementaire accélère l'adoption de technologies FIDO2 et d'authentification biométrique [22], établissant de nouveaux standards industriels.

L'adoption varie drastiquement selon la taille des organisations : 87% pour les grandes entreprises (>10 000 employés) contre seulement 27% pour les très petites entreprises (<25 employés) [23]. Cette disparité représente un enjeu de cybersécurité, les petites structures restant vulnérables aux attaques sophistiquées.

7 Conclusion

L'histoire des systèmes MFA révèle une évolution fascinante depuis les vouchers papier de 1967 jusqu'aux passkeys et à l'authentification comportementale de 2025. Cette progression de six décennies illustre l'adaptation constante aux menaces émergentes et aux contraintes technologiques de chaque époque.

Les personnalités visionnaires – Fernando Corbató, John Shepherd-Barron, Leslie Lamport, Kenneth Weiss, Jim Bidzos – ont posé les fondements techniques et conceptuels durables. Leurs innovations, motivées par des

besoins pratiques immédiats, ont créé un écosystème sécuritaire désormais indispensable à notre civilisation numérique.

L'avenir s'annonce passionnant, ou angoissant, avec l'intégration de l'intelligence artificielle, l'authentification comportementale continue, et les identités décentralisées. Le marché MFA, estimé à 17,76 milliards USD en 2025 avec une croissance annuelle de 18%, témoigne de l'importance critique de ces technologies dans notre infrastructure numérique.

Cette histoire démontre que l'innovation sécuritaire naît toujours de la confrontation entre contraintes techniques, menaces émergentes et besoins utilisateurs.

Références

[1] S. Magazine, The ATM is Dead. Long Live the ATM! 2024.

[2] A. Marketplace, Timeline: The ATM's history, 2024.

[3] IBM, The ATM, 2024.

[4] M. News, Professor Emeritus Fernando Corbató, MIT computing pioneer, dies at 93, 2019.

[5] FusionAuth, History of Passwords: How the First Password Was Hacked, 2024.

[6] FundingUniverse, History of RSA Security Inc. 2024.

[7] K. P. Weiss et R. C. Merkle, US Patent 4,720,860: Method and apparatus for positively identifying an individual, 1988.

[8] InfoWorld, Lamport's one-time password algorithm (or, don't talk to complete strangers!) 2024.

[9] IETF, RFC 1760 - The S/KEY One-Time Password System, 1995.

[10] K. P. Weiss, US Patent 5,361,062: Personal security system, 1993.

[11] P. A. Networks, What is the Evolution of Multifactor Authentication, 2024.

[12] IETF, RFC 6238: TOTP, 2011.

[13] C. on Foreign Relations, Connect the Dots on State-Sponsored Cyber Incidents - Operation Aurora, 2024.

[14] Google, Transparency in the shadowy world of cyberattacks, 2010.

[15] T. Times, Twilio Ends Support for Authy Desktop Application: What Happened to the Users? 2024.

[16] D. Security, Two-Factor Authentication Methods - Duo Push, 2024.

[17] AbubakarRajput, Touch ID and Face ID: Biometric Security in Your Pocket, 2024.

[18] W. A. Guide, Guide to Web Authentication, 2024.

[19] Descope, MFA Bypass Explained & How to Prevent It, 2024.

[20] Hoxhunt, MFA Fatigue Attacks: Ultimate Prevention Guide 2024, 2024.

[21] CyberNexa, MFA in 2025: Trends and Predictions for the Future, 2025.

[22] H. G. Blog, What Is Multi-Factor Authentication? MFA Defined: Then, Now, and Tomorrow, 2024.

[23] JumpCloud, 2025 Multi-Factor Authentication (MFA) Statistics & Trends to Know, 2025.