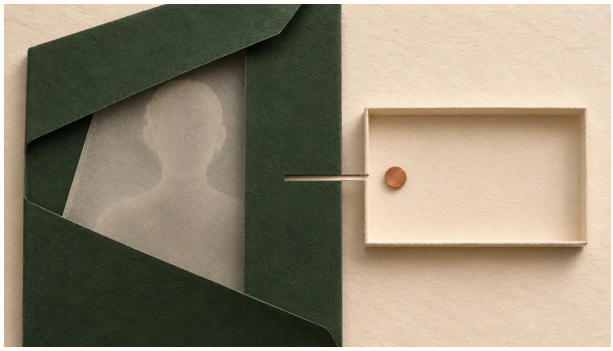


مقالة رأي وتحليل

التاريخ التحريري: ٨ أكتوبر ٢٠٢٦

أثبت من أنت، من دون أن تخبرني من أنت

حين تكفي حقيقة أصغر

في كاليفورنيا، يمكن لرخصة قيادة رقمية أن تقول لصاحب المتجر أقل مما تقوله البطاقة البلاستيكية، وأن تكون أنفع بسبب ذلك. يقدّم حاملها إلى جهاز تحقق إلكتروني ما يثبت بلوغه سنًا معينة؛ وقد يتلقى الطرف الذي يفحص الاعتماد تأكيدًا بتجاوز الحد العمري المطلوب، بينما تتطلب معاملات أخرى بيانات تعريفية أكثر. وتوضح إدارة المركبات في الولاية أن استعمال الرخصة الرقمية ما زال محصورًا في أماكن وخدمات مختارة. ليست المفاجأة أن الرخصة انتقلت من المحفظة إلى الهاتف. المفاجأة أن سؤالًا اعتدنا الإجابة عنه بكشف الاسم والصورة والعنوان وتاريخ الميلاد يمكن أن يُجاب عنه بحقيقة أصغر بكثير: هذا الشخص مؤهل من حيث السن.1

قد تبدو الخطوة تصغيرًا لوثيقة كبيرة، لكنها في الحقيقة إعادة رسم لحدود المعرفة. ما الذي يحتاج صاحب المتجر إلى معرفته فعلًا؟ ليس اسم الزبون، ولا يوم ميلاده، ولا رقم رخصته، ولا عنوان سكن لا علاقة له بالشراء. يحتاج إلى قرار تتوافر له درجة ثقة قانونية وتقنية مقبولة: هل بلغ الشخص السن التي تحددها القاعدة؟ كان التصميم القديم يسلّم الموظف ملفًا شخصيًا شبه كامل، ثم يعوّل على أن يتجاهل معظمه. أما التصميم الجديد فيحاول أن يجعل ما يستطيع النظام رؤيته مساويًا لما أُذن له بمعرفته. هنا لا نحمي البيانات بعد جمعها فحسب؛ بل نسأل لماذا دخلت الباب أصلًا.

هنا يتغير معنى كلمة «الهوية». فهي في الأنظمة الرقمية المعاصرة تؤدي أعمالًا مختلفة جمعناها، من فرط الاعتياد، تحت اسم واحد. حين يريد شخص فتح حساب مصرفي خاضع لمتطلبات معرفة العميل (Know Your Customer, KYC)، قد يكون إثبات الاسم الحقيقي والتحقق منه مطلوبين. وحين يدخل امتحانًا رسميًا، قد تحتاج الجهة إلى التأكد من أنه

الشخص المسجل بعينه. لكن من يريد إثبات أنه طالب في جامعة معترف بها، أو أنه يقيم في منطقة يحق لسكانها الاستفادة من خدمة، أو أنه أكمل التدريب الإلزامي قبل دخول منشأة، لا يلزم أن تكون الحقيقة المطلوبة هي نسخة شاملة من سيرته الشخصية. الفرق ليس بين «الهوية» و«إخفاء الهوية» دائمًا؛ بل بين معرفة الشخص ومعرفة صفة محددة فيه.

من البطاقة إلى الاعتماد

في يوليو 2025 قدمت المفوضية الأوروبية مخططًا تقنيًا للتحقق من السن يتيح للدول والخدمات الرقمية بناء تطبيقات تعتمد إثبات الأهلية العمرية دون كشف معلومات تعريفية غير لازمة. بدأ اختبار المخطط وتكييفه مع دول ومنصات ومستخدمين في ذلك الشهر. ثم صدرت نسخة ثانية في أكتوبر تضمنت طرقًا للاعتماد على جواز السفر وبطاقة الهوية، وذكرت المفوضية إدراج تقنيات برهان المعرفة الصفرية في الحل. وبحلول أبريل 2026 قالت إن التطبيق أصبح جاهزًا من الناحية التقنية وإن إتاحته للمواطنين ستأتي لاحقًا. وسمت الدنمارك وفرنسا واليونان وإيطاليا وإسبانيا ضمن الدول التي تعمل على تكييفه. هذه وقائع تطوير واختبار وخطة نشر، وليست دليلًا على أن جميع الأوروبيين كانوا يستخدمونه بالفعل عند كتابة هذه المقالة.2

يكشف المخطط الأوروبي عن طموح أعمق من تحسين نافذة تسجيل الدخول. فعند إصدار إثبات السن تعتمد الجهة المصدرة على مصدر موثوق، مثل هوية وطنية أو جواز سفر أو وسيلة تحقق أخرى معتمدة. ثم يفترض التصميم أن ينفصل استعمال هذا الإثبات عن الجهة التي أصدرته، بحيث لا يتلقى المصدر إشعارًا بكل موقع يزوره صاحبه. الخدمة الرقمية، من جهتها، تطلب إثبات الحد العمري، ويتلقى نظامها نتيجة تُمكّنها من السماح بالدخول أو رفضه. جرى فصل لحظتين اعتدنا دمجهما: لحظة التأكد من صحة أصل المعلومة، ولحظة استعمال قدر محدد منها. وقد يبدو الفصل إجراءً تقنيًا دقيقًا، لكنه يحول دون نشوء سجل مركزي لحياة الإنسان من مجرد محاولاته إثبات أهلية عادية.2

في مايو 2025 اعتمد اتحاد شبكة الويب العالمية (W3C) الإصدار الثاني من نموذج بيانات الاعتمادات القابلة للتحقق (Verifiable Credentials Data Model 2.0). فكرته الأساسية أن تصدر جهة موثوقة مجموعة ادعاءات عن شخص أو كيان بطريقة تسمح لغيرها بالتحقق من سلامة الاعتماد ونسبته إلى مصدره. قد تكون الجهة جامعة تشهد بنيل شهادة، أو مؤسسة مهنية تشهد بترخيص، أو جهة حكومية تؤكد صفةً في سجلها. يسمي النموذج الأطراف الثلاثة: المُصدر (Issuer)، والحامل (Holder)، والمتحقق (Verifier). لا تساوي هذه البنية قاعدة بيانات عالمية واحدة؛ بل تتيح انتقال ادعاء موثوق بين مؤسسات تختلف أنظمتها، بشرط اتفاقها على معنى الاعتماد وصلاحية من أصدره.3

لكن عبارة «قابل للتحقق» ليست مرادفًا لكلمة «صحيح». يلفت المعيار نفسه الانتباه إلى أن إمكان التحقق من الاعتماد لا يثبت بالضرورة أن جميع ما كُتب فيه مطابق للواقع. التوقيع الرقمي يستطيع كشف التلاعب بالبيانات وربطها بالمُصدر، لكنه لا يستطيع إعادة السنة الجامعية ليتأكد أن حامل الشهادة حضر محاضراته، ولا استدعاء الطبيب ليتحقق من جودة الفحص الذي وقعه. إذا كانت قاعدة بيانات المصدر خاطئة، فقد تنتقل المعلومة الخاطئة إلى العالم الخارجي في ظرف مشفر شديد الأناقة. لذلك يبدأ النظام من سؤال عن المؤسسة وإجراءاتها، لا من اختيار خوارزمية التوقيع وحدها.3

الإفصاح ليس عدم الربط

لنتصور شهادة مهنية تحتوي الاسم وتاريخ الميلاد ورقم العضوية وتاريخ الاعتماد والتخصص. تطلب منصة عمل التحقق من وجود ترخيص ساري المفعول في تخصص بعينه. الطريقة الأولى، وهي الأكثر شيوعًا في العقل الإداري، إرسال الشهادة كاملة. الطريقة الثانية إصدار نسخة جديدة تقل فيها المعلومات. الثالثة أن يحمل الشخص اعتمادًا مركبًا، ويكشف منه ما تطلبه المعاملة فحسب. تسمى الثالثة الإفصاح الانتقائي (Selective Disclosure). أما إذا أمكنه إثبات أن الترخيص سارٍ أو أن الدرجة تقع فوق حد معين من دون إظهار القيمة الأصلية التي بُني عليها الإثبات، فنحن نقترب من فئة أخرى من الأدوات هي براهين المعرفة الصفرية (Zero-Knowledge Proofs). تلك الفروق ليست مترادفات تسويقية؛ لكل واحدة منها حدود رياضية وأمنية مختلفة.

في نوفمبر 2025 نشر فريق هندسة الإنترنت معيار RFC 9901 الخاص بالإفصاح الانتقائي لرموز JSON الموقعة، المعروف باسم (SD-JWT). يسمح هذا الأسلوب للمُصدر بإنشاء اعتماد يضم ملخصات مشفرة لحقول، ثم يختار الحامل لاحقًا أي الحقول يكشف للمتحقق. في أبسط مثال، يستطيع أن يظهر صفة «طالب» ويخفي عنوانه ورقم هاتفه إذا كانت الحقول مصممة أصلًا للإفصاح المنفصل. هذا يحد كمية المعلومات التي تصل إلى الطرف الآخر، لكنه لا يثبت، بمجرد اسمه أو وجود التشفير فيه، أن كل تقديم جديد للاعتماد لا يمكن ربطه بالتقديم السابق.4

وهنا يقع أحد أكثر الالتباسات مكراً في السوق. يمكن لتطبيق أن يدعي احترام الخصوصية لأنه لا يعرض تاريخ ميلاد المستخدم، ثم يرسل في كل مرة الرمز الموقع نفسه أو بصمة ثابتة يمكن لموقعين متعاونين مقارنتها. سيكتشف الموقعان، ربما دون معرفة الاسم، أن الزائر الذي أثبت عمره هنا هو نفسه الذي أثبته هناك. يؤكد معيار RFC 9901 هذا القيد صراحةً: لا تستطيع آليات الإفصاح القائمة على الملخصات المملّحة، مثل SD-JWT، ضمان فصل المُصدر عن المتحقق في مواجهة متحقق متواطئ ينقل الاعتماد الأصلي إليه. لقد أخفينا الحقل، لكننا ربما احتفظنا برقم تسلسلي غير مرئي في الظاهر، يصلح لبناء سيرة جديدة للزائر.4

ولهذا يميز الباحثون بين ثلاث خصائص ينبغي ألا تتداخل في ذهن المصمم. الأولى هي تقليل الإفشاء: ألا يعرف المتحقق أكثر مما يحتاجه. الثانية هي عدم قابلية الربط (Unlinkability): ألا يستطيع متحققان الاستنتاج من المادة المشفرة وحدها أن العرضين يعودان إلى الاعتماد نفسه. والثالثة هي إثبات الحيازة أو الارتباط بالحامل (Holder Binding): ألا يستطيع شخص نسخ اعتماد غيره وتقديمه باعتباره اعتماده. قد يزيد تحصين الخاصية الثالثة من خطر إضعاف الثانية إذا استُخدم مفتاح ثابت معروف لدى الجميع. وقد يمنع النظام تقاسم الاعتمادات لكنه يتتبع كل استعمال لها. والنتيجة ليست تناقضًا يستحيل حله، بل مجموعة شروط تصميم يجب أن تُختبر معًا بدل الإعلان عن الفوز بإحداها وإسكات الحديث عن البقية.

ما الذي يثبته البرهان؟

الحل الرياضي الأكثر إثارة لا يبدأ باسم الإنسان، بل بقضية قابلة للحساب. لتكن قيمة خفية تمثل تاريخ ميلاده، وليكن تاريخ المعاملة معلومًا. المطلوب إقناع المتحقق بأن الفارق بين التاريخين يبلغ السن المسموح بها. يمكن تمثيل المطلب، على سبيل التبسيط، بعبارة من قبيل: توجد قيمة أصلية موثوقة تجعل الشرط «العمر لا يقل عن ثمانية عشر عامًا في يوم التحقق»

صحيحًا. لا يحتاج المتحقق إلى تلك القيمة نفسها إذا كان البرهان سليمًا. لكن شرطًا بالغ الأهمية يختبئ هنا: لا بد أن يثبت النظام أن تاريخ الميلاد الخفي جاء من مصدر موثوق، لا من تاريخ كتبه المستخدم لنفسه قبل لحظة واحدة. وإلا صار لدينا برهان رياضي بديع على معلومة مختلقة.

برهان المعرفة الصفرية يجمع، في صورته النظرية، ثلاثة مطالب. أن يقبل المتحقق البرهان الصحيح عندما تكون القضية صحيحة؛ وأن يعجز من لا يملك شاهدًا صحيحًا عن إقناع النظام بقضية كاذبة إلا باحتمال ضئيل تحدده الفرضيات الأمنية؛ وأن لا يكشف البرهان من الشاهد الخفي شيئًا يزيد على ما تكشفه صحة القضية نفسها. يسمّي الباحثون هذه الخصائص الاكتمال (Completeness)، والمتانة أو السلامة (Soundness)، والمعرفة الصفرية (Zero Knowledge). لكن النتيجة الثالثة لا تنفي أن جملة «عمري فوق الثامنة عشرة» تكشف معلومة فعلية عن صاحبها. إنها تنفي، ضمن النموذج الرياضي المعني، تسرب بقية الشاهد من البرهان. ولا تعالج وحدها صورة الوجه أمام الكاميرا أو عنوان الاتصال بالشبكة أو سجل المتصفح.5

ثم إن كل شهادة قابلة للتوقيع ليست قادرة تلقائيًا على إنتاج أي برهان نريده. إذا شهد المُصدر مسبقًا بأن حامل الاعتماد «فوق 18»، فقد يكفي تقديم هذه الصفة الموقعة دون تاريخ الميلاد. أما إن لم يصدر إلا تاريخ الميلاد نفسه، فأداء إثبات مقارنة حسابية عليه من غير إظهاره يتوقف على مخطط التشفير وطريقة الترميز وإثبات علاقة التوقيع بالصفة. وقد تحتاج منظومة إلى اعتماد مشتق من المصدر، أو إلى بروتوكول برهان يناسب هذا النوع من الحساب. لا يجوز أن نضع شعار ZKP على شاشة ثم نفترض أن التحقق من أي شرط صار مجانيًا أو مضمونًا. المعضلة الهندسية ليست إخفاء الرقم فقط، بل إثبات مصدر الرقم وعلاقته بالشرط ووقت سريان الشرط.

في سبتمبر 2026 نشر W3C مسودة توصية مرشحة لتقنيات التوقيع (BBS) المستخدمة مع الاعتمادات القابلة للتحقق. تتيح تلك التقنيات اشتقاق أدلة مشفرة تكشف بعض الصفات وتحافظ على عدم قابلية الربط بين الأدلة المشفرة المشتقة، إذا استُخدمت وفق خصائصها. وثيقة سبتمبر لم تكن توصية نهائية؛ بل مسودة في مرحلة اختبار التنفيذ. وهذا تمييز مهم في أي سوق يحب أن يعرض التكنولوجيا الناشئة كأنها إجماع قياسي مكتمل. كما أن قوة عدم الربط في المادة المشفرة لا تضمن عدم الربط في التطبيق إذا قدم المستخدم معلومة فريدة مع البرهان، أو أضاف الموقع معرّفًا متكررًا في متصفحه، أو احتفظ بربط آخر خارج البروتوكول.6

حين يكشف السياق ما أخفاه التشفير

تتغير الصورة أكثر عندما ننتقل من الدليل إلى الإنسان. لو أظهر طالب من جامعة صغيرة أنه حاصل على تخصص نادر وأنه تخرج في دفعة محددة، فمن الممكن استنتاج اسمه من معلومتين صحيحتين حتى لو لم يحتو البرهان على أي هوية مباشرة. ولنفترض أن موظفًا يعمل في فريق من ثلاثة أشخاص فقط يثبت أهليته لاستخدام نظام حساس. ربما تكفي معرفة المسمى الوظيفي والتوقيت كي نعرف من استعمل الخدمة. لم تُخترق الخوارزمية هنا. إنما كشف التفاعل سياقًا ضيقًا يجعل المجهول معروفًا. لا ينبغي قياس الخصوصية فقط بعدد الخانات الفارغة في بطاقة رقمية، بل بحجم المجموعة التي ما زال صاحبها يختلط بها بعد الإفصاح.

وهناك مستوى آخر من المعرفة أشد صمتًا. قد لا يعرف موقعٌ الاسم ولا تاريخ الميلاد، لكنه يعرف عنوان الشبكة ونوع الجهاز وطريقة الحركة ووقت الزيارة. وقد يستخدم ملفات تعريف أو مكونات تحليل تجاري تربط محاولات الدخول باستعمالات سابقة. يمنع البروتوكول القوي ربط الأدلة المشفرة عبر المؤسسات، لكنه لا يمنع المؤسسة من تتبع الزائر بطرق أخرى. وهذه حقيقة تصح في الاتجاه المقابل أيضًا: يمكن أن تكون إجراءات حماية الشبكة والاحتفاظ بالبيانات ممتازة رغم استعمال اعتماد تقني لا يوفر عدم الربط رياضيًا. الخصوصية ليست شهادة تمنحها مكتبة برمجية، بل خاصية تُقاس من أطراف الخدمة كلها.

الإبطال والحيازة ومفارقة الحالة الحية

تبدو فلسفة المخطط الأوروبي أكثر وضوحًا عند السؤال عن المصدر. إن اضطرت منصة إلى الاتصال بالجهة التي أصدرت اعتماد السن في كل مرة يزور فيها شخص موقعًا، فقد تصبح الجهة المصدرة شاهدًا على عادات استخدامه. يمكن للتحقق غير المتصل، أو الاعتماد على مفاتيح عامة وقوائم حالة مصممة بعناية، أن يخفف المشكلة. لكن الاعتماد قد يُلغى أو تنتهي صلاحيته، وقد يفقد صاحبه هاتفه أو تتعرض مفاتيحه للاختراق. عندئذ يحتاج المتحقق إلى معرفة أن الشهادة ما زالت نافذة. توصيات المعهد الأمريكي للمعايير والتقنية (NIST) الصادرة في مراجعة 2025 تشترط إتاحة وسائل لإبطال حزم الصفات، وتوصي بفترات صلاحية محدودة، وتنبه إلى أن خدمة التحقق من حالة الإبطال يجب ألا تُشعر المُصدر بأن اعتمادًا بعينه استُخدم لدى خدمة بعينها.7

هنا يظهر ما يمكن تسميته «مفارقة الحالة الحية». نريد شهادة يُتحقق منها من دون الاتصال بالجهة المصدرة حتى لا تتحول إلى أداة مراقبة. ونريد في الوقت نفسه أن يعرف كل متحقق فورًا إذا أُلغيت تلك الشهادة بسبب سرقة جهاز أو تغير أهلية أو إبطال ترخيص. لا يوجد حل سحري يجمع انعدام الاتصالات وزمن إبطال يساوي الصفر وعدم احتفاظ أحد بأي حالة. توجد هندسات ومقايضات: صلاحيات قصيرة، ودفاتر حالة عامة ذات حبيبات لا تعرّف الأفراد، وأدلة عدم إبطال مناسبة، ووسائل استرجاع وإعادة إصدار، وحدود مخاطر تختلف باختلاف الخدمة. حين تبيع مؤسسة اعتمادًا «لا يتصل بالمصدر أبدًا» ينبغي أن نسأل كيف تعرف أنه لم يبطل أمس.

والسؤال العملي التالي: من الذي يقف أمام شاشة الهاتف؟ إذا حصل شخص على دليل أنه بالغ ثم أرسله إلى صديق أصغر سنًا، فخصوصية البروتوكول لا تنقذ غرض التحقق. ولذلك تشتمل بعض التصاميم على ربط الحيازة بمفتاح خاص داخل جهاز محمي، وتطلب من المحفظة إجراء توقيع جديد استجابة لتحدٍّ فريد من المتحقق. أما التحدي العشوائي (Nonce) فيقلل إمكان إعادة استعمال رسالة قديمة، وربط الاستجابة بجهة محددة يمنع أخذ دليل أُرسل إلى متجر وإعادة تقديمه لمنصة أخرى. كل ذلك يحد انتحال الحيازة وإعادة الإرسال؛ ولكنه لا يكشف، من دون وسائل إضافية، إن كان الشخص الممسك بالجهاز هو نفسه الذي خضع للتحقق الأولي فعلًا.78

في هذا الموضع تصبح تجربة كاليفورنيا مهمة مرة أخرى، ليس لأنها حققت الحالة المثالية، بل لأنها تعيد التحقق إلى موضعه الطبيعي. تؤكد إدارة المركبات أن الرخصة الرقمية ليست مجرد صورة للبطاقة، وأن عرضها يجري من خلال التحقق الإلكتروني؛ وتوصي بألا يعرض المستخدم شاشة رخصته ببساطة ليفحصها الطرف الآخر بعينيه. إن التحدي الحقيقي أمام

المتاجر والقائمين على الخدمات هو تجهيز أدوات قراءة متوافقة، وفهم ما يُطلب وما يُستقبل، والتدرب على حالة فشل الهاتف أو عدم توفر القارئ. فما الفائدة من رخصة تحفظ الخصوصية داخل المحفظة إذا أجبر الموظف صاحبها، بسبب خلل الجهاز، على تسليمه صورة كاملة من الهوية؟1

من المختبر إلى المؤسسة

يستطيع المرء أن يتخيل تطبيقات أوسع، على أن تبقى افتراضات تصميم لا إنجازات تدّعي أنها حدثت. يمكن لموقع يعلن فرصة تدريب مقصورة على الطلاب أن يطلب إثبات قيد دراسي صالح من مؤسسة معترف بها. ويمكن لمركز أبحاث يتعامل مع بيانات حساسة أن يطلب إثبات إتمام دورة أخلاقية حديثة من دون نسخ الشهادة بما عليها من أرقام. ويمكن لمدينة أن تمنح مزية لسكان نطاق إداري معين من دون السؤال عن عنوان منزل دقيق إذا كانت الأهلية تتحدد بمجرد انتماء العنوان إلى منطقة. ويمكن لاتحاد مهني أن يؤكد صلاحية ترخيص ممارس من دون كشف رقم وثيقة أخرى. في كل هذه الأمثلة يُصبح معيار النجاح أن تُصدَر صفةٌ قابلة للفحص تناسب قرارًا بعينه، لا أن ننسخ المستند ونحذف منه ما لا يعجبنا بعد وصوله.

لكن الأنظمة التي تتعامل مع المال تفضح حدود الشعار بسهولة. عندما يفتح شخص حسابًا مصرفيًا ضمن نطاق يتطلب إجراءات عناية واجبة بالعميل، لا يمكن للمصرف أن يستبدل التزامه القانوني بمعرفة هوية العميل بجملة مجردة تقول «هذا الشخص فوق الثامنة عشرة». توضح إرشادات مجموعة العمل المالي (FATF) حول الهوية الرقمية، المنشورة في مارس 2020، أن استخدام الحلول الرقمية في إجراءات معرفة العميل يعتمد على مستوى موثوقية نظام الهوية ومخاطر العلاقة المالية، وأن التحقق الرقمي أداة لامتثال أدق، لا طريق للهروب من إجراءات العناية الواجبة. يمكن مع ذلك تقليل ما يُجمع من صفات لا تحتاجها المعاملة، أو التحقق من أهلية فرعية لدى طرف آخر من دون إعادة كشف جميع التفاصيل. الخصوصية لا تعني أن تتجاهل المؤسسة واجبها، بل أن تعرف أين يبدأ الواجب وأين تنتهي شهية الجمع.9

وهذا يغير بنية المنافسة بين الشركات. فالمنصة التي اعتادت جمع تاريخ ميلاد كل مستخدم وعنوانه ونسخة وثيقته تحت شعار «تسهيل التحقق» كانت تبني، في الحقيقة، أصلًا معلوماتيًا ضخمًا وخطيرًا قد لا يكون لازمًا لخدمتها. كل سجل إضافي يلزم تأمينه، وتحديد مدة الاحتفاظ به، وتفسير استخدامه، وإبلاغ الجهات المختصة أو الأفراد عند تسربه بحسب النظام المطبق. تتحول المعلومات من وقود تسويقي إلى التزام يصاحب المؤسسة لسنوات. أما الجهة التي تكتفي بإثبات أهلية موثوق، فقد تقلص سطح الهجوم على بياناتها، لكنها لا تُعفى من تأمين أدلة التحقق وقيود الجلسات وأحداث الاحتيال التي تحتفظ بها. الاقتصاد هنا لا يتعلق بحذف قاعدة بيانات فقط، بل باختيار مسؤولية المؤسسة المعرفية قبل أن تصبح تلك المسؤولية حادثًا أمنيًا.

ومن هذا الباب، تكتسب قواعد الاتحاد الأوروبي أهمية عملية. فالتنظيم التنفيذي الصادر في نوفمبر 2024 بشأن محافظ الهوية الأوروبية يتحدث عن نقل الحد الأدنى الضروري من البيانات إلى الأطراف المصرح لها، وعن فصل المعاملات بما يحد قابلية الربط بينها. ويفرض تصميم طلبات الصفات والتحقق من الجهات الطالبة ضمن إطار معروف. ليست المسألة أن التقنية وحدها تقنع الشركات بألا تطلب الاسم؛ بل أن طريقة التسجيل والحوكمة تسمح بالسؤال عمّا إذا كانت الجهة تملك سببًا مشروعًا لطلبه أصلًا. المعيار التقني يوفر وسيلة، أما القاعدة المؤسسية فتحدد متى يجوز استعمالها وبأي حدود.10

يبقى هناك قيد اجتماعي لا يختفي بقوة التوقيع. ماذا يفعل من لا يملك هاتفًا حديثًا؟ أو من فقد جهازه ومفتاحه السري؟ أو من تعذر عليه استخراج وثيقة أصلية بسبب تعارض في بيانات السجل؟ أو من يرفض تسليم هاتفه الشخصي لصاحب عمله؟ قد تتحول منظومة «الخصوصية المصممة مسبقًا» إلى بوابة إقصاء جديدة إذا صارت الطريق الوحيد إلى خدمة عامة. لذلك ينبغي تصميم ممرات بديلة معترف بها، واسترجاع آمن لا يسمح لمن يحتال على خدمة الدعم بالاستيلاء على الاعتماد، وآلية تصحيح لأخطاء المصدر، ومسؤولية واضحة عن رفض إثبات صحيح. ليست هذه إضافات إنسانية لطيفة إلى بحث في التشفير؛ إنها شروط صحة المنظومة عندما تغادر المختبر.

يمكن النظر إلى المؤسسة بوصفها ناشرًا لأسئلة لا لحقائق عن الناس. في كل تفاعل، يسأل نظامها: هل يحق لهذا الإنسان أن يفعل هذا الشيء الآن؟ حين يكون السؤال محددًا، نستطيع هندسة جواب محدود. وحين يكون السؤال غامضًا، تتسع قائمة البيانات احتياطًا. لذلك فإن أول خطوة في بناء خدمة تحترم الخصوصية ليست اختيار محفظة ولا التعاقد مع مزود براهين مشفرة، بل تفكيك القرار نفسه. ما الصفة التي تغيّر النتيجة؟ من يملك سلطة إثباتها؟ كم تبقى صالحة؟ وهل يكفي أن نعرف أن الصفة موجودة، أم يجب أن نعرف صاحبها الفردي لمنع تكرار المطالبة بحق واحد؟

المشكلة الأخيرة تكشف تحديًا في تصميم الإعانات والحقوق المتفردة. قد ترغب جهة في التأكد من أن المتقدم مستحق لصرف مساعدة مرة واحدة فقط، من دون إنشاء ملف عام يربط استعمالاته عبر خدمات أخرى. مجرد إثبات أنه «مستحق» لا يمنع شخصًا من تقديم الصفة عشر مرات. يمكن بناء معرف مستعار محدود بالنطاق أو رمز استعمال لا يتكرر ضمن البرنامج، بشرط أن لا يصبح هذا الرمز نفسه مفتاحًا عالميًا لتعقب صاحبه. بعض مخططات التشفير تتيح أشكالًا من الأسماء المستعارة المحددة بالنطاق، وتناقش مسودة BBS طرق اشتقاقها. لكن تصميم ذلك في خدمة عامة يتطلب اختبار منع الصرف المكرر في مقابل عدم الربط خارج البرنامج، وإتاحة حق مراجعة الأخطاء. فالسرية بلا قدرة على إنفاذ القاعدة قد تهدم ثقة الجمهور، والإنفاذ بلا حدود قد يهدم خصوصيته.6

ميزانية الإفشاء

ولكي لا تتحول هذه المبادئ إلى منشور علاقات عامة، أقترح اختبارًا هندسيًا أوليًا أسميه «ميزانية الإفشاء». لا أدّعي أنه معيار تنظيمي قائم أو نتيجة تجربة منشورة؛ إنه إطار تصميم قابل للتجريب. تبدأ المؤسسة بجملة واحدة تصوغ القرار المطلوب، ثم تعد لكل صفة حقلًا يبيّن سبب الضرورة، والمصدر، ومن يرى القيمة الأصلية، ومن يرى الدليل، ومدة الاحتفاظ، وإمكان ربط عمليات الاستعمال. بعدها تُجري تجربتين عدائيتين: تجمع سجلات متحققين افتراضيين وتبحث عن روابط متكررة، ثم تفترض تعاون أحدهما مع المُصدر لترى هل يمكن تحديد صاحب اعتماد بعينه من أثر التقديم. وأخيرًا تختبر إلغاء الاعتماد وفقد الهاتف وتكرار الطلب وفشل الشبكة. لا يُحتسب انخفاض عدد الحقول نجاحًا إذا أصبح التتبع ممكنًا من أثر ثابت آخر.

أما المقياس الأهم فلا يصلح أن يكون «كم نسبة المستخدمين الذين أكملوا التحقق؟» وحدها. ينبغي قياس نسبة القرارات الصحيحة من دون كشف بيانات زائدة، ونسبة الأدلة الصحيحة التي رُفضت، ونسبة الادعاءات الكاذبة التي قُبلت، والوقت اللازم لنشر الإبطال، ونسبة الحالات التي انتقلت اضطرارًا إلى كشف وثيقة كاملة، واحتمال الربط بين متحققين ضمن

نموذج تهديد محدد. وتحتاج هذه المقاييس إلى عينات تشمل أجهزة متواضعة ومستخدمين من فئات عمرية ومهارية مختلفة. من الممكن أن ينجح النظام في اختبار التشفير ويخفق في اختبار الخدمة؛ كما يمكن لواجهة شديدة السهولة أن تمنح اعتمادًا مزورًا ثقة أسرع مما كان يحصل عليه الورق.

ومع تقدم هذه المنظومات سيظهر سوق جديد، لكنه ليس سوق «بيع هويات» جديدة. هناك مُصدرون متخصصون في إثبات صفات، ومحافظ تتولى حماية مفاتيح الحامل، وأطراف تحقق تدير سياسة طلب الصفة، وجهات تضع معايير الثقة ومفاتيح المؤسسات المعتمدة، وأدوات لتقييم الخصوصية واختبار مقاومة الاحتيال. القيمة التي تستحق البناء حولها ليست معرفة مزيد من الأشياء عن الناس، بل القدرة على الاعتماد على قدر أصغر من المعرفة. وهذا يفسر لماذا لا يكفي إطلاق تطبيق لامع يحمل شعار «هوية لامركزية». قد تكون المحفظة على هاتف المستخدم، بينما تبقى القرارات كلها رهينة قائمة سماح يحتكرها مشغل واحد، أو بينما يتلقى المُصدر إشارة عن كل استعمال. اللامركزية في موضع التخزين لا تكفي إذا بقيت الرقابة مركزية في موضع القرار.

ثمة أيضًا إغراء فلسفي ينبغي مقاومته. سيقول البعض إن النظام الأكثر احترامًا للإنسان هو الذي لا يعرف عنه شيئًا مطلقًا. لكن الخدمة المسؤولة تحتاج أحيانًا إلى حقيقة موثقة وإلى إمكان محاسبة معلوم. والمطلوب ليس أن يُصبح كل مواطن شبحًا، بل أن تتناسب معرفة المؤسسة مع الحق أو الخطر الذي تديره. ففي بعض الأبواب يكون الاسم شرطًا مشروعًا، وفي أبواب أخرى تكون معرفته تعديًا معرفيًا لا وظيفة له. ومن الخطأ أن نحمّل براهين المعرفة الصفرية وعدًا بحل التعارضات القانونية والاجتماعية. قوتها أنها توسع حدود ما يمكن إثباته رياضيًا من دون كشف شاهد الإثبات كله. أما ما يجب إثباته، ولمن، ومن يحق له طلبه، فهي أسئلة لا يسع التشفير وحده أن يجيب عنها.

التواضع المؤسسي

تروي الرخصة الرقمية في كاليفورنيا قصة انتقال جزئي من البطاقة المكشوفة إلى الصفة المطلوبة. وتروي المحاولة الأوروبية قصة مؤسسات تحاول الفصل بين إصدار الثقة ومراقبة الاستعمال، مع مراحل تطوير ونشر لا ينبغي المبالغة في وصف اكتمالها. ويكشف معيار SD-JWT أن الإفصاح الانتقائي لا يعني بالضرورة تعذر تتبع الاعتماد؛ بينما تشير أعمال BBS إلى وسائل أعمق لحماية آثار التقديم نفسها، مع تمييز ضروري بين مسودة ومعيار نهائي. وتذكّرنا إرشادات NIST بأن الإبطال وحماية المفاتيح والأخطاء ليست حواشي على الهوية، بل جزء من صدقها. هذه الحالات لا تتنافس على لقب «الأكثر تشفيرًا»؛ إنها تكشف طبقات المسألة التي أخفيناها طويلًا وراء صورة هوية مصورة.

قد تقودنا هذه التقنيات إلى فضيلة نادرة في الأنظمة: التواضع المؤسسي. أن تسأل الخدمة عن القدر الذي يؤهلها لاتخاذ قرار، ثم تتوقف عنده. عندها لن يكون الإنجاز الأكبر أن يخفي الإنسان اسمه، ولا أن ينجح برهان معقد أمام معالج سريع؛ بل أن تتعلم المؤسسة الفرق بين حقها في التحقق وفضولها في المعرفة. أمضينا عقودًا نعلّم الأجهزة كيف تتعرف علينا في كل مكان. وقد حان الوقت لنعلمها مهارة أصعب: أن تصدقنا في أمر محدد، ثم تغلق الملف وتترك لنا بقية حياتنا.

المصادر والمراجع

[1] California DMV, Mobile Driver's License FAQs — صفحة رسمية جارية؛ تمت مراجعتها 9 نوفمبر 2026.

[2] European Commission, Blueprint for an age verification solution — النسخة الأولى يوليو 2025؛ الثانية أكتوبر 2025؛ جاهزية تقنية أعلن عنها أبريل 2026؛ تحديث صفحة 22 سبتمبر 2026.

[3] W3C Recommendation، 15 W3C, Verifiable Credentials Data Model v2.0 مايو 2025.

[4] RFC — IETF, RFC 9901, Selective Disclosure for JSON Web Tokens منشور، نوفمبر 2025؛ انظر §§4 و10.1.

[5] SIAM Journal on — Goldwasser, Micali, Rackoff, The Knowledge Complexity of Interactive Proof Systems Computing 18(1)، فبراير 1989.

[6] Candidate Recommendation Draft، 10 W3C, Data Integrity BBS Cryptosuites v1.0 سبتمبر 2026، وليست Recommendation نهائية.

[7] NIST, SP 800-63C, Digital Identity Guidelines: Federation and Assertions — النسخة النهائية Revision 4 لعام 2025؛ §5.4 المحافظ التي يتحكم بها المشترك.

[8] OpenID Foundation, OpenID for Verifiable Presentations 1.0 — مواصفة Final لعام 2025.

[9] FATF, Guidance on Digital ID — 6 مارس 2020.

[10] European Commission, Implementing Regulation (EU) 2024/2982 — 28 نوفمبر 2024؛ النص في EUR-Lex.

[11] NIST, Zero-Knowledge Proof, Cryptographic Glossary — مرجع اصطلاحي رسمي جرى الاطلاع عليه في نوفمبر 2026.