

Liability and Federated Identity: Much Ado About Nothing?

BY CAROL COYE BENSON



It would be very useful if some of these groups provided the guidelines that service providers will need to assess the quality of identity credentials supplied by identity providers.

As enterprises implement new identity management systems, interest grows in federated identity. For small “circles of trust,” existing business relationships—and existing contractual frameworks—are sufficient to build federated networks. But with eyes everywhere cast on the opportunity to create larger circles of trust, what business frameworks will be needed to support these large-scale federated networks?

While a multilateral business framework has many important aspects, liability transfer is the 800-pound gorilla everyone wants to wrestle. In a nutshell, liability transfer means that the identity provider, or authenticator, financially backs its identity assertions, effectively saying to a relying party, “I guarantee you this is Sally; if I’m wrong, I pay you.” I’m fascinated to hear how many people assume this is required—and that it’s just a matter of the right industry working groups issuing the appropriate rules.

I may be a lone voice here, but I just don’t see this happening. Clearly, there will be situations where an identity provider assumes some form of “identity liability.” But these are apt to be very small circles of trust where well-defined business relationships already exist. What I question are identity guarantees in large-scale circles of trust, where the link between the identity provider and the relying party is arms length at best. Although it’s nice to think that the fuzzi-

ness of the relationship demands a liability framework, it actually shows how impossible it would be to create one.

I believe large-scale identity federations will all operate with explicit disavowals of liability. The identity provider will, in essence, say to other members of the federation: “I think this is the person who claims to be Sally—for whatever it’s worth to you!” The lack of liability behind that assertion isn’t good or bad; it’s just the way it will probably work.

Why is this notion of identity liability—and its transference—so impossible? To answer that, let’s look at how credit card networks transfer liability from a merchant—the service provider who’s selling the goods and taking the risk of accepting the credit card—to the card-issuing bank. Three relevant characteristics of this network enable the transfer of liability:

- **Transactions occurring on the network have a precise value metric—the purchase amount. This makes determining the liability associated with the transaction extremely easy. (Credit card networks are very careful to ensure that the liability is never expanded to include non-precise, contingent damages beyond the purchase amount.)**
- **All network participants have agreed (with varying degrees of willingness, but that’s a different story!) to a significant body of operating rules**

"Credit Card Networks are very careful to ensure that liability is never expanded ... beyond the purchase amount"

that specify how the network operates and the circumstances that lead to the transference of liability for purchases—and its reversal when settling disputes.

- **The network participants share very high—although different—motivations to participate. The consumer gets ease of purchase and access to credit. The merchant gets the ability to sell with manageable risk. And the bank stands to earn very attractive profits from its card business—particularly those derived from the loans enabled by the card network.**

These characteristics are, of course, tightly interrelated. The specific metrics of the

transaction are necessary for the operating rules to be well understood and precise. The operating rules are necessary to manage the risks incurred by all network participants. And the profits are necessary to offset the costs of supporting the network and absorbing fraud.

When we look at the world of identity federation, we see none of these characteristics. With very few exceptions, identity transactions have no precise value metric—unless they're purchase transactions, but then why do we need another liability transference mechanism? The lack of precise metrics means that practical operating rules specifying liability transfer can't be meaningful. Are all iden-

tity transactions deemed to be worth \$100? \$1,000? Why? (People have discussed the idea of a dynamic negotiation of liability levels during an identity assertion—but I can't imagine that working in reality.) Finally, the parties to an identity transaction are unlikely to have motivations to participate in the network equal in strength to those of participants in a credit card network. Certainly, profits on the identity horizon aren't comparable to card-lending profits to support the costs of a liability transference network—much less the potential fraud.

Other payments networks—from ATM to checking to ACH—show variations of this model. Some provide liability trans-

"In large-scale federated networks, the parallels to payments networks collapse even further"

ference, but generally in situations where network rules allow the party assuming liability to tightly manage their risks. And all of these networks have, of course, the precise value metric of the actual transaction.

In the context of large-scale federated networks, the parallels to payments networks collapse even further. In general, payment systems don't inter-operate. If a bank takes a payment out of one system and enters it into another, the liabilities of a party to the first part of the transaction don't flow through to the party of the second part. If payments networks that have existed in electronic form for many, many years haven't yet figured out inter-system liability transfer—or needed to—I doubt very much that identity networks will. So, no, I don't think there will be "identity guarantees" in broad federated networks.

This isn't to say that members of these networks won't have responsibilities to perform with due diligence what they claim to do, or that they'll be without liability if they make errors or commit fraud themselves. But I think this will be sorted out among participants in the normal course of business—in the courtroom or the backroom—and not by an established framework for the federation.

Let's consider the issue from the point of view of the enterprise that enjoys an

established, authenticated relationship with a consumer—but whose primary business is not being an identity provider. The new identity protocols enable this enterprise to assert the identity of the consumer to another enterprise that provides complementary services. The identity provider is willing to do this either as a service to the (common) customer, or to get compensation (from the service provider), or for some combination of these motives. The identity provider has done its own form of due diligence in establishing its authentication credential with the consumer in the first place. It's now interested in asserting the consumer's identity on to the service provider, but the service provider is suddenly asking it to guarantee that assertion. What identity provider in its right mind would agree to accept any serious degree of liability in association with this? The company may be willing (indeed, should be willing) to disclose the nature of the registration process it used at the point of issuing an authentication credential. But should it agree to pay out cash if it's later shown that the process wasn't used correctly for Sally? I don't think so.

There will, of course, continue to be "professional" identity providers who are in the business of providing general-purpose identity credentials—the PKI certificate providers are a clear example of this. Some of them have flirted with warranties on identity, and even have some policies in place. But if you look closely at their policies, it quickly becomes clear that the warranties fall far short of the identity guarantee that some dream of for federated identity. I don't think these organizations give us models to follow for federation.

Many working groups—and some private companies—are beginning to tackle some of these issues. The Center for Strategic and International Studies (CSIS) is conducting meetings to stimulate more business ownership of these topics, and to encourage the participation of industry verticals.

I think all of these groups will have more luck—and make more progress—on the significant number of addressable issues (privacy issues and enrollment procedures, for example) if they can accept the fact that liability is a non-issue. Otherwise, they'll be mired in endless working group meetings trying to square the circle. A healthy dose of reasonable expectations is the tonic these groups need to succeed.

It would be very useful if some of these groups provided the guidelines that service providers will need to assess the quality of identity credentials supplied by identity providers. But these guidelines will merely help the service provider, who will still have to make the yes/no decisions itself. The service provider, after all, is the consumer of the identity transaction. And caveat emptor will still apply. ■

Carol Coye Benson is a consultant and analyst with Glenbrook Partners, where she directs the firm's identity management practice. With more than 25 years of experience in the financial services industry, she has been instrumental in the development of industry-wide authentication and identity initiatives for over the last 10 years, working with both financial institutions and their technology providers. She can be reached at carol@glenbrook.com.