Identity Infrastructures
Case Studies

Version 0.1

November 26, 2006

Foreword

In the IDWG we are looking for the underlying identity infrastructure to be serviceable for the TWIST applications/processes *e.g.* bank mandates, payments within SEPA, and supply chain.

The purpose of this document is to present actual cases and learn from them.

History

The ENI and the Bank of Finland cases were presented in a previous IDWG document from Nick Ragouzis: Advancing a Versatile Interoperable Identity Infrastructure for Finance and Services in the EU, Release 5 Dec 2005 — Draft.
More cases are welcome!

List of content

Links to E-Invoicing initiatives

"Goal: A standard invoice, used internationally by all industries would give a big push to the diffusion of e-invoicing but, as long as the invoice remains a multi-purpose document, industry differences will prevent reaching this goal. If, instead, the invoice is seen as a document with multiple interlinked segments to serve specific purposes (compliance with order, match with DDT, check prices, book and pay transaction, basis for financing more progress could be made.

NB A critical factor for the orderly take-off of e-invoicing and fiscal dematerialization is the presence of strong EIPP /ASP operators that concentrate data flows and offer corporates a gamut of dematerialization services.

Today, few operators exist in Europe which have the right size, the right business model and the lasting power to stay in business and cross the break even point…

This can be achieved through alliances of banks, IT companies, large corporates, who can bring to the ASP operator their high volumes from the beginning.

In some countries, like the Nordic states, critical mass has been reached but their business model is not applicable ,as is, to larger states.

The lack of interoperability of European CAs is another obstacle to the e-economy…

Use Public Administrations to kick-start the adoption process and use the right incentives to help the "innovators" (CAST)

ENI, the Sofid subsidiary and the ENI Transazioni E Rendicontazioni (ENITER) Platform

In 2005, and earlier, in 2003, Vito Umberto Vavalli, Director of Payments Systems Development and Advanced E-Services Management, Sofid SpA (Eni Group), wrote generously about their work in establishing a system for identifying counterparties so to enable the type of real time identification required for their intended straight through processing.

The ENITER systems for handling electronic transactions entered design in 2000, and so was begun before realization of many of the innovations discussed in this paper. According to the 2003 paper it had, by then, been performing ERP or accounting for 52 ENI companies and business units. Here we consider (briefly) the opportunities presented such a system by the presented modern, versatile interoperable identity infrastructure.

An overall observation is that this design held uppermost the tenet that there would be a central low-order mechanism tying together all parties to this processing: an ENI self-issued digital certificate. This was held as necessary for meeting regulatory, privacy and operational goals. As we shall see, a modern identity architecture can use this infrastructure (among other designs) while avoiding the fatal impediments (to interoperation, to privacy, to security) latent in such mechanisms.

Flexibility in credentialing; efficiencies in provisioning

As much as possible, a business would like to invest once, then harvest many times. This has been seen as nearly impossible in the domain of electronic credentials. Yet rather than accept the unpalatable repeated reinvestments, many potential partners and businesses have simply opted not to enter potential partnerships, or to limit them to a narrow and limited scope and domain. In a different accommodation, we have the common, and decried, scene of individuals carrying many (a handful, a dozen) smart cards and key fobs.

The solution lies not simply in smart cards or key fobs that can contain more credentials (perhaps in enough types and quantity for today; but what of tomorrow?) but rather also in separation of concerns between credentialing, domain, and transaction authentication, and the dynamic use of identity.

The key to re-using credentials, even in new applications, is to not use the ‘original’ credentials themselves as primary transaction authenticators. This involves moving the trusted third parties from a somewhat administrative role (certifying, maintaining reporting on validity) to an active participant in the transactions.

Thus, instead of laying down a new base credentialing domain for every application, you create an authentication overlay where parties from different credentialing systems are able to collaborate and communicate on specific activities, while otherwise keeping private and secure the use of these same credentials for other uses. This maintains efficiencies in provisioning (e.g., each party enters into contractual, not organizational (e.g., subsidiary) bindings and so manages its own investments in provisioning according to its expected returns), and opens possibilities for further such efficiencies and other opportunities (below).

Variety in authentication context, according to transaction context

As discussed above in “Characteristics of Emerging Identity Systems,” the identity system should facilitate the selection of appropriate credentials. From one perspective, earlier systems had one opportunity and one choice to make about credentials that would represent

suitable authentication, and such credentials were relied upon for authentication throughout the domain or transaction, without differentiation.

A modern identity infrastructure provides a way for parties and counterparties to differentiate on the context of the parties, the transaction class, and even the stage or content of the transaction. Such an architecture recognizes that any party may determine (say, on the basis of dynamic risk profiling) that additional or more stringent credentials are required to proceed, and provides a means to request such services. Or that the given credentials, characterized by credential class, will serve for some part of the service, but not all.

Further, the token exchange itself, referencing the credentials, can carry statements related to the business purpose and party agreements.

Multipurpose and blended credentials

One challenge of evolving systems is the problem of introducing new credentials into an existing credential fabric; the usual solution is to create a separate test system, or even a separate system requiring change over when customers wish to use these systems.

The identity system discussed here provides a way for multiple credential systems to overlap. Existing credentialing systems, and the resulting certificates, including the uses of digital signature gateways and certificate status services, can co-exist with other credentials. This allows a service to increase its credentialing requirement within the same infrastructure, moving from single factor to two-factor authentication, for example.

From the point of view of security officers and the designers of new systems, they can utilize a blend of credentials and authentication methods according to the services desired. Two benefits are worth highlighting. One, a service provider could now introduce new services with less stringent credentialing requirements (such as information services) on the same infrastructure, or, alternatively, introduce services with more secure requirements. Two, service providers can use these overlapping and context-specific credentials to meet auditing, national security and policing, and privacy requirements simultaneously.

Protection of attributes; lifetimes of credentials

The ENITER platform is very specific about the attributes it requires and accepts; these are baked into the digital certificate. We have discussed above some of the challenges that arise should different credentials be required or desired. That same discussion applies to attributes.

It is often the case, however, that attributes are as valuable as the signatures themselves. Modern identity systems allow us to move attributes outside the domain of authentication credentials. Such an identity infrastructure allows designers to authenticate attributes separate from base credentials, and allows for their discovery, request, and exchange to be conditioned on particular operations and protected by separate mechanisms.

This lengthens the lifetime and increases the domain of utility of credentials, while providing greater privacy, yet attributes may be updated more frequently (departments, locations), their descriptive domains increased, and with contributions by various parties (not all attributes must derive from the same party as the “base” credentials—some may be verified by an even more authoritative and time-specific source).

This system also provides a more granular approach to auditing and policing: audits on transactions can contain only the necessary information, and requests for records can be met

with only the specific, authorized, data yet support chaining if additional authorizations are obtained. Further, freed from their dual duty, the signatures within these longer-living certificates can better meet the needs for long term storage of keys.

Building on existing credentialing and security investments

It should be apparent, but bears repeating that the 'versatility' of the identity infrastructure is not limited to the variety of applications and services, nor extensibility of mechanisms, nor its ability to evolve forward. The versatility also refers to the ability to incorporate and leverage a wide range of existing investments in directories, authentication and access systems, integrity assurance systems, privacy protection mechanisms, as well as business processes, relationships, and market mechanisms.

Restructuring Securities Processing, Bank of Finland Discussion Paper, Harry Leinonen

This is a substantial contribution addressing many aspects of securities processing. The few comments here are directed at contributions available from an identity infrastructure.

Overall, many comments from above apply here as well. For example, with the proposed identity infrastructure, solutions are available that would obviate the need for 'global' cross-tabulation tables for IBANs and custodians of every ICAN, including otherwise arbitrary structuring standards to facilitate such cross-tabulation.

Likewise, auditing can be step-wise rather than end-to-end, obtaining the improvements discussed above.

Balance in efficiency and market performance

While it is in general true that efficiencies are improved by a reduction in the number of systems, layers, and stages in processes, the method for proper choice of such a system is known for only very simple environments. Instead, designers typically prefer to include mechanisms contributing robustness and resilience in the face of variety and variation. This is what a versatile interoperable identity infrastructure can contribute. In particular, by introducing mechanisms as discussed above, the various CSDs and their customers can elect a range of structures, layers, and identifier systems as innovation, competition, and market forces suggest. In effect, rather than artificially reducing the variety in institutions, the goal could be that a wide variety, and unknown new types, could efficiently be supported.

Incremental, evolutionary independent adoption

Another capability offered through the identity infrastructure is that as organizations adopt this infrastructure they may use it to elect to use a range of identifiers (related to customers, accounts, processors, instruments, securities, and so on), from old, 'new,' and future (currently unknown) systems. This removes, at least for identifiers and credentials, a significant challenge to adoption of the overall improvements proposed: parties in various stages of readiness may share the same interfaces. Through methods similar to those discussed above the challenges of varieties in local security identifiers (ISIN) could be accommodated.

From a more philosophical perspective, we should also consider the time in which these decisions are being taken. We have reached the end of the phase of the single-purpose credential. This foretells a change similar to that when we reached the end of the phase for asynchronous serial protocols. From now on there will be a growing profusion of standards and recommendations. It is, therefore, no solution to choose underlying 'point' protocols (e.g., PKI)—one must choose extensible identity platforms capable of supporting many low-level mechanisms while also providing frameworks for specifying application-level services.

Straight-through processing via staged-processing

It bears repeating that a modern identity system removes the design criteria which had previously thought could only be solved by end-to-end sharing of credentials (and the related identifiers and keys). (The end-to-end sharing is often realized in a single, centralized, registrar, for example.) As discussed elsewhere, because this represented such an impediment to innovation and marketplace forces that substantial innovation have been applied to the problem with the result that we now have removed these criteria, and therefore we have cause to revisit the design of any system exhibiting design choices justified on that criteria.

Transaction security models

Although the main thrust of the current paper has been identity, such an infrastructure also has a significant role in security, in assuring the identities of the parties, in preventing a loss of message integrity, in ensuring confidentiality in messaging, and in providing suitable facilities for privacy, auditing, and appropriate policing. The features mentioned must also be able to be granular and subject to partitioning—preventing distribution of sensitive key, attribute, and credential data, to prevent collusion or malfeasance from both internal and external officials and participants. In an advancement over the Leinonen security model, the proposed identity infrastructure allows custodial systems and settlement modules to obtain subject confirmations from a variety of third parties, with the ability to securely assign (or prevent) the proxy of such confirmations. Further, as mentioned with respect to the ENI opportunities, different keys may be used as part of the identity system, the credential system, and message (and attribute), integrity and confidentiality.

Recouping investments

Leinonen gives appropriate attention to the problem of garnering sufficient return on these investments, pointing out that even some earlier 'legacy' investments remain shy of their targets. The changes Leinonen suggests are probably necessary for the public welfare, and therefore for each company in order to assure competitive parity. One mitigating consideration is that by basing these changes on a versatile identity infrastructure, businesses at all levels increase their opportunities to participate in identity- and attribute-aware commerce.