Advancing a Versatile Interoperable Identity Infrastructure for Finance and Services in the EU

Draft — Release 10 Dec 2005 — Draft

This draft is released for review of scope, targeting, and editing in preparation for publication in the TWIST Standards library. Among other defects the figures and references are incomplete. Please direct your comments to the editors.

Editors:
Nick Ragouzis, Enosis Group <nickr@enosis.com>
Matthew Arrott, November Group <matthew.arrott@novgp.com>
Shaun Maine, Simplex Consulting <smaine@simplexconsulting.com>

Contributors:
Tom Buschman, Shell
Harry Leinonen, Bank of Finland
Jean-Yves Gresser, Black Forest Group

With this document we intend to open the dialog in the case for advancing a versatile identity infrastructure throughout Europe, one that would enable identity-aware interoperability across a wide range of services, markets, and stakeholder domains.

Much has been written about the needs of businesses, regulators, and consumers concerning finance, payments and other services. Various technologies have, as well, been broadly covered. This document is intended for an audience familiar with these matters; it does not recount them.

In the identity domain, however, here has been a tendency to define needs in terms of what technology is thought to be able to address, and to incrementally move technology forward without rethinking core assumptions concerning the services delivered. This document explores that gap.

In that pursuit we explore motivations for changing our approach to this problem. We touch on regulatory necessity, infuse a few select problem statements with the essence of this new approach, discuss the common characteristics in the domain.

To demonstrate the advanced nature of the state of the art, we chose as a model a particular family of identity technology. This technology is not itself the focus of the paper, but rather serves to show how a flexible and extensible technology might meet many of the use cases and requirements, and in a more potent fashion. Indeed, none of today's identity technology can meet even the expressed needs. Technology sharing these and other characteristics are required for meeting those needs, and must now be the attention of, both, active and rich adoption, and continued and farsighted design.

Aware of the shortcomings of existing conceptions of needs, of existing technologies, and of this paper itself, we end with suggestions for a working approach to fill these gaps.

Table of Contents

Appendix A: Regulatory Regime, Expanded

This appendix extends the discussion concerning regulatory necessity. Here we highlight (without much elaboration) the use cases and particular demands latent in the cited Directives, Regulations, and other actions.

1. **New Legal Framework** NLF, Consultation COM(2003)718:
    - removing the basis of the expense and burden objections for reporting by (especially) newcomers to banking transactions;
    - facilitating the joint satisfaction of 95/46/EC with exceptions related to Article 13(d) therein;
    - solution to the problem of non-interoperability in recognition of electronic signatures within existing context of variety in signature technologies, credentialing, and trust domains—offering an operationalization of these concerns (rather than forcing a resort to legislation) and extending current technologies while introducing a basis for innovation and competition;
    - effecting a realizable form of inspection for identity-commerce (derivative of Regulation (EC) 1/2003);
    - assisting in secure and identity-assured establishment of collateral arrangements and associated transfers expanding the form of evidence, removing procedural barriers and administrative burdens (as per Directive 2002/47/EC);
    - avoidance of single registrar solutions for unique identifier challenges, especially honouring Member state rights and controls on local identifiers (of all kinds, from natural persons to equity issues);
    - realizing objectives (including variety and responsiveness in services and vitality of competition) through removal of basis for objections seen in responses (e.g., in Oct 2002 responses MARKT/4005/2002) to number portability, and customer mobility (including handling within the identity network such concerns as standing orders—which could now also be transformed into dynamic orders) while, contrary to claims of degradation in ability to offer timely advice, improving "effective advice," the ability, in advance, to inform beneficiaries of costs, options and so on;
2. **Markets in Financial Instruments** MiFID, EU Directive 2004/39/EC (ISD2):
    - The briefing material for the recent (19Oct05) MiFID JWG make clear how challenges of meeting regulatory requirements in several areas arise when not working with an identity-aware, privacy-enabling infrastructure capable of securely managing multi-valued context-aware attributes, including for example the problem of party identification, and particularly not merely low-order and often fixed attributes (and not only at the time of initiating the business relationship), but dynamic and arbitrarily-extensible attributes, and facilitating context-dependent discovery with the ability to discern roles among other aspects;
    - the challenges of informing clients during pre-trade advice through post-trading, which when taken from at the Directive's broadest view is not merely the problem of sending the data, but of identity-enabling the exchange, to include conditioning on client's at-the-moment choice of notification mode and media, and moreover, to enable customers to insert themselves into negotiations for value-added information services (and joint social networking-style provisioning of such service), which then suggests that fully satisfying the Directive might require an identity-enabled template-based means for specifying instructions (offering options of re-use with multiple parties, perhaps with proxy options) related to selection of venue on

parameterized- or fixed-value terms for best execution along with appropriate consents;
- the necessity to deliver this while remaining consistent with requirements for auditing, regulation, and the security of the markets, which touches on other requirements highlighted here;

3. **Industrial Policy**, COM(2005)474 and SEC(2005)1215 et seq:
   - The pivotal role identified for innovation and intellectual property development and protection is significantly dependent on cooperation within and among these enterprises, across sectors, and with external sources of innovation, which is, in turn, significantly dependent on secure identity-enabled services for the necessary collaborations;
   - acceleration of partnering and other enterprise reorganization and cooperation; faster integration of employees in multi-domain and multi-provider programs (e.g., training);
   - as a core feature of product and services designs, offering integration into the identity infrastructure; not solely in aerospace, defence, biotech, medical, or engineering sectors, but also in more traditionally staid domains, such as goods industries;
4. **Payer information accompanying funds transfer**, Proposal 2005/0138:
   - Removing priority to actual account numbers (vs traceable identifiers) while solving the chaining challenge, both in real time (going forward assurances) and in back-tracking;
   - removing the “technology” caveat for intermediates, while not preferring information forward-transport (which counter to suggestion impedes all-important chaining, while also increasing many other data risks);
   - including intrinsic services that enable separable, partitioned, access to elements of the records, on a rapid (near-instantaneous) access and historical basis protected through requirement for joint and multi-lateral keying; under the controlled conditions and terms, enabling chaining and mining across multiple identifiers and in preparatory and consequential transactions and activities;
   - unification with extra-Community payments;
5. **Entry and operation in credit business**, Proposal COM(2004)486 (adopted Oct05), esp. in respect to Act 1 and its annex but generally applicable throughout the discipline of regulatory capital:
   - With general attention to requirements from Basel II in respect to keeping pace with market developments and flexibility, establishing appropriate incentives for credit organizations to move toward more risk-sensitive approaches, to stimulate credit institutions to improve market strategies bringing particular attention to the necessity for real-time information flows within identity-aware and protected framework for, e.g., informing appropriate authorities of shareholder identities (in a way the authorities can directly act on such information) and significant holdings, collection and access to credit conditions of borrowers with granularity in privacy protections controlling information gathering and release (thereby removing barriers, both, to risk control and expanded perhaps innovative offerings) (more directly in CESR advice), providing secure and identity-assured means for a wide range of executory and regulatory activities such that the activities of the credit institutions can safely span the widest possible domains with capabilities for rapid action and reaction;
6. **Shareholder information and rights**, Giovannini Barrier 3, regard corporate actions, esp. in respect to investor rights and activities, including the benefits of offering shareholders effective direct voting and enhancing custodial bank proxy instructions;

- contact with shareholders, operational on various attributes and purposes yet privacy protected; related to directing and tracking proper communication of information and disclosures in pursuit of assuring freshness (moving from passive postings to directed active or push publication) and authenticity of disclosures conjoined while guarding against improper disclosures and uses of such information (CESR; Market Abuse Directive 2003/6/EC);

7. **Cross-Border Payments**, among other EC Regulation 2560/2001 and Commission's Consultative contribution of 19Oct05 MARKT/H3 D(2005), esp. regarding continued challenges with identifiers, marking both the need to resolve the problems in the IBAN-plus-BIC scheme beyond just Community banks (2560/2001 targeting *retail* charges as much as bank-to-bank operation), where a versatile identity infrastructure could allow essentially arbitrary customer-level identifiers, facilitating resolution to this challenge while also serving in issues of number portability, customer mobility, flexibility and further options in directing payments and settlements, providing access to delayed information, and so on;
   - as elsewhere, merely satisfying 'clear and timely' communications as compared to meeting the Directive's larger goal of using these communications to realize stronger competition for customers, and enabling customer choice and action (including seeking alternate solicitations) in such communications;

8. **Data protection**, in various respects, including directives and requirements deriving from the Data Protection Directive (95/46/EC), DPD, the Telecommunications Data Privacy Directive (96/77/EC) the Electronic Communications and Privacy Directive (2002/58/EC), including the perhaps most vexing long-standing challenge of balancing societal security with personal protections (for example the challenge of balance for DPD's Article's 6, 7, and 13) where a versatile identity infrastructure provides a way to successively move data out of the reach of inappropriate commercial uses, then a succession of types of data holding for security purposes, while also providing a de-identified yet still integral data source for managing network services; providing real-time management of unambiguous consent to directory information, including self-management and publishing of data limited only by customer choice (such choice being in any of the data dimensions, the requesting context, the automation of such as subscription to updates, customer election of data use solicitations, application of agency to such choice, and more);
   - ability to support a plurality of identifiers, including opaque or limited-time identifiers and anonymous service provision, within any context as part of a chained but not parlay-able service thereby providing further protections (in this way addressing, finally, the technical environment impediments mentioned as early as the European Commission WP6 March 1997, leading to still pervasive notions about the (im)possibilities regarding anonymity under Internet technologies, and the unhelpful embedding or direct association of extended attributes with PKI certificates);
   - beneficial reduction of the artificial distinction between natural persons and legal persons for legitimate interests, while increased protections against abuse by legal persons (the necessity of agency action on behalf of natural-person customers, for example);
   - consistent with variety in service offerings, personal choice and safety, and societal security concerns, enabling simultaneously-variable identity-conditioned (requestor, relying party, targeted identity, etc) responses to highly personal context data (such as presence, geo-location);
   - recognition that an identity infrastructure adds a new services layer that performs as though it is located between customer terminal equipment and any given end service,

forming a new kind of data class requiring protection and that is protected under the versatile identity infrastructure.