Arias Cabarcos, P.; Almenárez, F.; Trapero, R.; Díaz-Sánchez, D.; Marín López, A. (2015). "Blended Identity: Pervasive IdM for Continuous Authentication". *IEEE Security & Privacy Magazine*, vol. 13(3), May/June, pp. 32-39.
DOI: 10.1109/MSP.2015.62

Blended Identity: Pervasive IdM for Continuos Authentication

Patricia Arias-Cabarcos and Florina Almenárez | University Carlos III of Madrid
Rubén Trapero | Technische Universität Darmstadt
Daniel Díaz-Sánchez and Andrés Marín | University Carlos III of Madrid

A proper identity management approach is necessary for pervasive computing to be invisible to users. Federated identity management is key to achieving efficient identity blending and natural integration in the physical and online layers where users, devices, and services are present.

Adoption of new computing paradigms is usually hindered by the security challenges they bring. In the pervasive computing field, an element of paramount importance still requires deeper research—identity management (IdM)—the management of individual principals, their authentication, authorization, and privileges within or across system boundaries. Mark Weiser's vision of a world in which technology becomes invisible to support people in their everyday lives is currently unrealizable without a continuous authentication system.[1]

The goal is to create ambient intelligence where network devices embedded in the environment, from clothing to cars, homes, and the human body, provide unobtrusive connectivity and services all the time, thus improving human experience and quality of life without explicit awareness of the underlying communications and computing technologies.

In this ubiquitous computing world, a change of context—for instance, users shifting location or new people appearing in the proximity—might involve new devices, services, and interaction possibilities. To gain access to pervasive services, users must often authenticate and expose different forms of their identity to the various services, which worsens user experience and conflicts with the goal of invisibility.

IdM technologies have evolved to cope with the increasing number of services that users might access; *federated identity management* (FIM) is the latest approach, wherein a common set of policies, practices, and protocols links users' electronic identity and attributes stored across multiple IdM systems. FIM's ultimate goal is to enable users of one domain to securely access data or systems of another domain seamlessly—single sign-on (SSO) being the most popular functionality. However, current federation technologies rely on preconfigured static agreements, which aren't well-suited for the open environments in pervasive computing scenarios. These limitations negatively impact scalability and flexibility.

A new identity model for open environments is necessary. Thus, our contribution includes:

- a definition of *blended identity*, which is the basis for applying FIM in open environments;
- a prototype risk-based architecture that extends and improves FIM to allow the creation of dynamic federations; and
- design and validation of the risk assessment methodology that constitutes the main pillar of our proposed architecture.

Our model enables continuous authentication so users can securely access services anytime and anywhere, with minimal interaction. The model is thus aligned with pervasive computing's basic goals: invisibility, flexibility, scalability, and personalization.

The Challenges of Pervasive IdM

When the first computers appeared, password-based authentication was the core mechanism of IdM IdM. This mechanism worked fairly well at that time, owing largely to how little data it actually needed to protect. However, with the advent of the Internet, the explosion of personal devices and online applications, and the increase in transactions, IdM became far more complex. Today, we're asked to prove our identities every time we board a plane; check in to a hotel; make a credit card purchase; and log on to a computer, smartphone, smart TV, or website. Therefore, users face a mental burden, known as *password fatigue*, which frequently leads them to devise strategies that degrade the security of their protected information. For instance, users might employ the "poor man's SSO" strategy, reusing the same passwords.

In the past decade, FIM frameworks and protocols, such as Security Assertion Markup Language (SAML), WS-Federation, OAuth, and OpenID, came on to the scene to ameliorate the problems related to password-based authentication and allow identity portability across disparate domains.[2] Successful implementations have been deployed in the Web domain, especially in the education and research fields and the social Internet arena. Despite this advance in IdM, important open issues remain.

Two influential works analyze IdM problems and formulate identity's seven laws[3] and flaws.[4] Both studies point out that two factors are indispensable: security aspects, such as privacy, minimal disclosure, and mutual authentication, and effective human integration, such as natural interaction and easy interfaces. Furthermore, they highlight trust establishment as key for scalability. Although FIM protocols can cover security aspects, usability and trust challenges are unsolved.

Whereas the research community has addressed IdM in pervasive computing, there's still scarce work in the context of applying FIM to it. Some proposals introduce mechanisms for SSO and seamless access control, but they're usually limited to a particular scenario or set of devices.[5,6] We need to evolve IdM one step further; the merging and usage of well-known FIM protocols seems a natural approach.

Blended Identity

Identity must be reformulated for FIM's application in pervasive computing. The seven laws and flaws fail to address the notion of convergence between the physical and online planes. This concern, coupled with proper handling of human interaction and trust management, leads to the concept of blended identity.

Identity has both a digital and a physical component. Some entities might have only an online or physical representation, whereas others might have a presence in both planes. IdM requires relationships not only between entities in the same planes but also across them.

Users move around the pervasive world carrying various personal devices that comprise a personal network (PN). This dynamic network changes when users are in motion, for instance, going from a smart home to a smart office. Devices join and leave, services appear and disappear, and access control must adapt to maintain the user perception of being continuously and automatically authenticated.

To accomplish this, federations must be established to create trust relationships between devices and services to securely exchange identity data. For example, when users log in to their smartphone, authentication is seamlessly transferred to the rest of their PN devices. When they move to the office, the smartphone's authentication isn't enough to access office devices, such as a printer or corporate Web services. Thus, another identity source—in this case, the online corporate database—must provide the users' job identity and extend and establish a federation with their PN for both physical and online access. All this should happen in the background beyond user consciousness.

Hence, there are several coexisting identity sources, called identity providers (IdPs), and several services requiring identity data, which service providers (SPs) offer. Roles can shift, and both physical devices and online providers can offer services. A universal IdP can't be assumed because SPs requires different identity assurances and attributes in different contexts. Furthermore, in pervasive scenarios, it's unrealistic to assume that interactions always take place between known entities or that an administrator has preconfigured the required trust relationships among every party to guarantee secure operations. Pervasive environments are dynamic, multiprovider, and multiservice. Preconfiguration isn't feasible because it simply doesn't scale.

Current FIM protocols suffer from limitations that make the described level of identity blending unattainable.[2] Nowadays, it's possible to achieve SSO only across online services in closed domains with a previously established trust relationship. In addition to these FIM protocols' lack of flexibility, they neglect the remaining possible relationships: SSO across devices in a PN, PN federations with other PNs or smart environments, SSO from physical devices to online services, and SSO from online services to physical devices.

To address these concerns, blended identity should efficiently combine the physical and digital planes to achieve IdM for pervasive computing. Users should authenticate automatically and continuously to the smart services and devices, whether online or in the digital or physical plane, and the environment should adapt and personalize accordingly.

Blended identity requires a natural interface and dynamic trust relationships. An easy-to-use interface should choose the best IdP automatically and authenticate users anytime and anywhere in continuously changing contexts. In addition, relationships between SPs and IdPs shouldn't be based only on preconfiguration. Establishing new trust connections based on risk assessment should be possible.

A Continuous Authentication System

Alternative proposals to achieve more streamlined authentication processes in pervasive computing environments are flawed (see the "Related Work in Pervasive Computing Authentication" section).

Our proposed solution has three big advantages. First, unlike several proposed models, it doesn't require users to carry a new device. Second, it leverages current FIM protocols for SSO, which are properly integrated and extended. Thus, it's easier to deploy than other solutions defining new protocols, and it's compatible with existing providers. Finally, when interacting parties are unknown to each other, a new trust relationship can be established based on risk assessment, providing greater flexibility and scalability.

Our model integrates different authentication sources and identity data naturally. Unlike other work, it dynamically establishes federations between previously unknown IdPs and SPs. This powerful feature has a potential positive impact on business ecosystems, because instant virtual enterprises could be created at any moment and share user data to offer personalized services. Users will be constantly authenticated across these services, enjoying a real ubiquitous experience.

Architecture

Figure 1 shows the architecture for implementing continuous authentication. Because it's based on FIM standards, it provides security services—that is, authorization, integrity, and confidentiality—and enhanced services and privacy mechanisms, such as SSO, single logout, account linkage, and transient and persistent pseudonym identifiers.[2] Furthermore, it meets the additional interface design and dynamic trust establishment requirements to realize the blended identity vision.

The architecture's main element is the users' primary device—any device that includes the modules that act as IdP or IdP proxy. When operating as an IdP, the device directly provides user identity data that doesn't require third-party attestation, for example, to authenticate against other devices. When operating as IdP proxy, it selects and reroutes authentication requests to the most suitable IdP and performs continuous SSO according to the operation flow we describe later. These requests can be processed in any FIM protocol through the FIM connectors module in Figure 1.

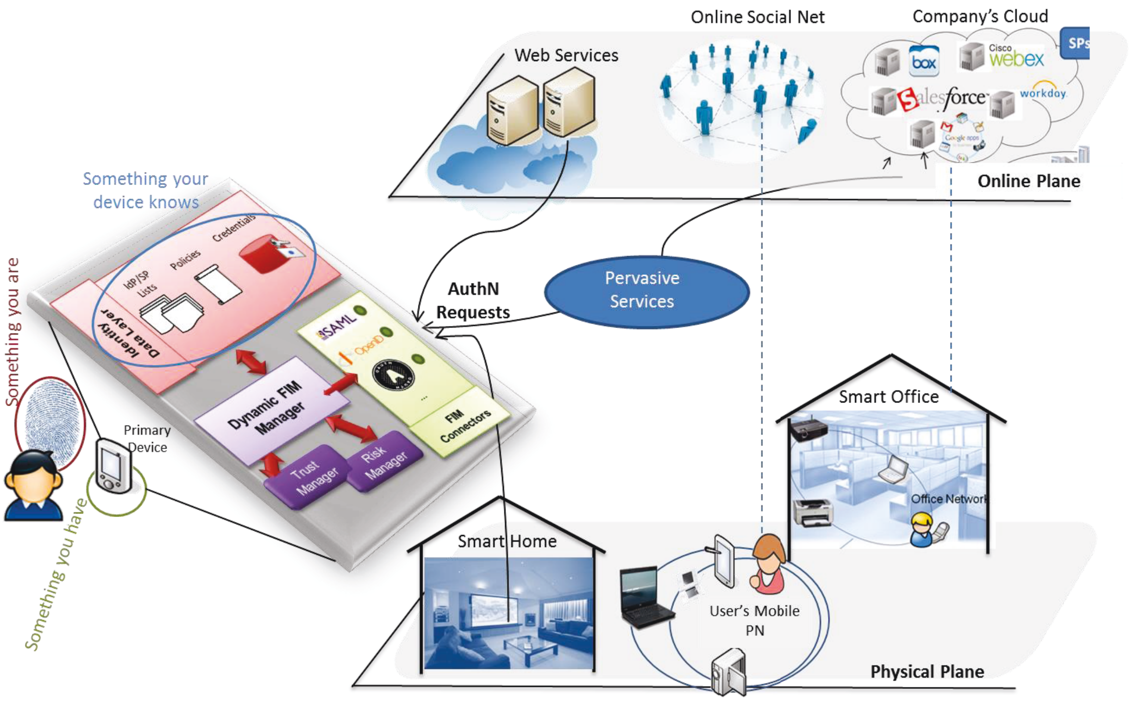


Figure 1. Architecture for blended identity implementation.User's carry a primary device with software modules to: detect authentication requests coming from any kind of device and service, determine the best identity source to authenticate the user, and create new trust relationships based on risk assessment.

To achieve such level of intelligence and automation, the primary device stores users' IdPs and the passwords, credentials, or tokens in a tamper-proof place (see the identity data layer in Figure 1). To unlock this knowledge and let the device authenticate users on their behalf, a biometric proof, such as fingerprint recognition, is given. This mechanism constitutes a simple interface that is always the same, is natural and easy, and requires only light user interaction. Thus, the proposed design is based on the common three-factor identity paradigm, which defines identity as being composed by something you have, something you are, and something you know. Our prototype blends these three features to construct a natural interaction process wherein the primary device represents something you have; biometrics provide something you are; and something you know, such as passwords, is transferred to something your smart device knows to improve usability and reduce users' mental overhead. This part of the architecture meets the first requirement for blended identity—a natural interface.

Another key software module is the dynamic FIM manager, which includes the trust manager and the risk manager. The trust manager gathers external information and reputation data (details of operation can be found in "fedTV: Personal Networks Federation for IdM in Mobile DTV"[7]). The risk manager computes the risk of collaborating with an unknown provider. Both trust and risk values are considered to decide whether to establish a relationship. This part of the architecture meets the second requirement for blended identity—dynamic trust relationships.

Operation Flow

Based on this architecture, our continuous authentication operation flow has four steps. First, because an SP's pervasive service requires user identity data for access control, it sends an authentication request to the users' primary device.

Second, the primary device executes an identity-matching algorithm to determine the most suitable IdP to answer the authentication request based on local policies, and then reroutes it.

Third, the selected IdP or the device decides whether to authenticate users against the SP. If the SP is known and a trust relationship exists, SSO messages are exchanged following the FIM protocol in use, and users are authenticated. If the SP is unknown, the IdP gathers publicly available information about it, including metadata, policies, and reputation; assesses risk; and decides on the fly whether to federate and share identity data. The reputation protocol is designed to avoid attacks from malicious nodes[8]; this has been investigated in related work.[9] Reputation and risk data are combined using fuzzy logic based on "E-commerce Trust Metrics and Models."[10] The complexity of the relationship between these two factors is tackled by linguistic labels that assign quantitative values from thresholds, allowing decision making about cooperation using conditional rules. We call this process of establishing a new trust relationship *dynamic federation*. SSO messages are exchanged following the FIM protocol in use, and users are authenticated.

Finally, authenticated users are granted seamless access to the pervasive service.

According to SSO standard protocols, an active IdP session is required to transparently notify the requesting SPs of the authentication state; otherwise, users are first queried for their credentials. This proposed architecture requires an active session only on the primary device, for instance, unlocked with a fingerprint or biometric proof. Whenever required, the device authenticates to the rest of the IdPs on behalf of users by sending their credentials.

Risk Assessment Methodology

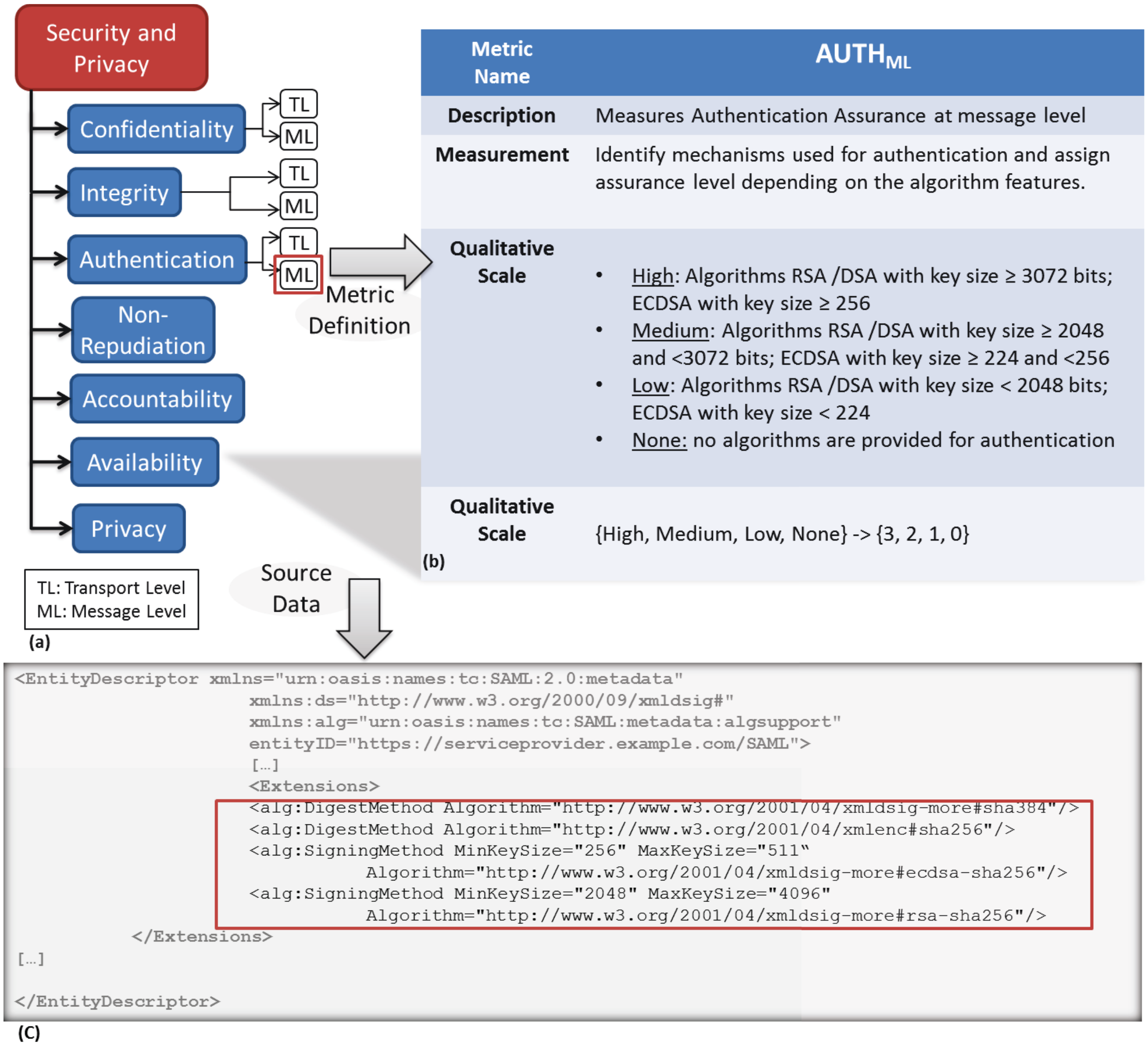
Deciding whether to federate an SP with an IdP isn't a trivial task. Risk assessment entails identifying, evaluating, and estimating of quantitative or qualitative risk levels related to a concrete situation; comparing these levels against benchmarks; and determining of an acceptable risk level. Decision-making techniques assist in this procedure; we propose a methodology that provides a meaningful numerical model based on multicriteria decision making, which uses multidimensional risk–based inputs to evaluate the federation's suitability.

We use a methodology based on the multiattribute utility theory (MAUT), which compiles a list of aspects relevant for risk evaluation ($N = 1, \ldots, n$), a partial score g_i that indicates how good a provider A under evaluation is for each aspect N according to a measurement scale in the set of real numbers $S_i \in R$, and each criterion's specific importance in the context of the provider (W_i).[11] Index i numbers scores, weights, and scales ranging from risk aspect i=1 to risk aspect i=n.

We derived the list of aspects in our risk assessment methodology directly from a taxonomy tailored for FIM that was created by analyzing FIM specifications and the public survey of Research and Education Federations (https://refeds.terena.org/index.php/Federations).[12] This taxonomy considers a hierarchical-based approach with five high-level categories—security and privacy, knowledge, interoperability, service specific risks, and historical interactions—each with subcriteria in the lower levels of the taxonomy.

To assign the partial scores for a provider A $g_i(A)$, we defined a set of metrics related to every taxonomic category. In this article, we focus on assurance metrics that are the inverse of the probability of incurring in risk—that is, the higher the assurance, the lesser the risk, and vice versa. The process of defining the applicable metrics depends on the MAUT theory, which requires numerical values between 0 and 1. However, the assurance scale format is mostly qualitative: no, low, medium, and high assurance. To solve this issue, we mapped each qualitative value to a quantitative one (0, 1, 2, or 3), which we then normalized. The final result is a vector that represents the partial normalized scores for each subcriterion ($[g_1(A), \ldots, g_n(A)]$), which we call the *score vector*(SV).

Figure 2 exemplifies the quantification process for the security and privacy metric, including the mapping from the qualitative to quantitative scale. We obtained metric values based on the strength of the cryptographic algorithms in place, according to the National Institute of Standards and Technology's recommendations.[13] Figure 2c represents the source used to quantify the security and privacy metric that, in this example, is taken from a provider's SAML metadata.



Metric Name	$AUTH_{ML}$
Description	Measures Authentication Assurance at message level
Measurement	Identify mechanisms used for authentication and assign assurance level depending on the algorithm features.
Qualitative Scale	• High: Algorithms RSA /DSA with key size ≥ 3072 bits; ECDSA with key size ≥ 256 • Medium: Algorithms RSA /DSA with key size ≥ 2048 and <3072 bits; ECDSA with key size ≥ 224 and <256 • Low: Algorithms RSA /DSA with key size < 2048 bits; ECDSA with key size < 224 • None: no algorithms are provided for authentication
Qualitative Scale	{High, Medium, Low, None} -> {3, 2, 1, 0}

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
                      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                      xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"
                      entityID="https://serviceprovider.example.com/SAML">
                      [...]
                      <Extensions>
                      <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>
                      <alg:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                      <alg:SigningMethod MinKeySize="256" MaxKeySize="511"
                                Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
                      <alg:SigningMethod MinKeySize="2048" MaxKeySize="4096"
                                Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
           </Extensions>
[...]

</EntityDescriptor>
```

Figure 2. Quantification process for the security and privacy metric. (a) Part of the taxonomy that identifies security and privacy risk criteria. (b) Example metric definition related to the authentication at message level ($AUTH_{ML}$) taxonomic dimension. (c) A provider's SAML metadata containing the information used to obtain the $AUTH_{ML}$ metric.

The next step is to determine each criterion's importance with respect to the others. For this purpose, we used weights assigned by each provider according to its preference, expressed as a *weight vector* (WV). With this information, we obtained each provider's acceptable global risk score ($Agg(A)$) by aggregating all the weighted quantified criteria. Box C in Figure 3a shows this process. However, the problem isn't totally solved yet.

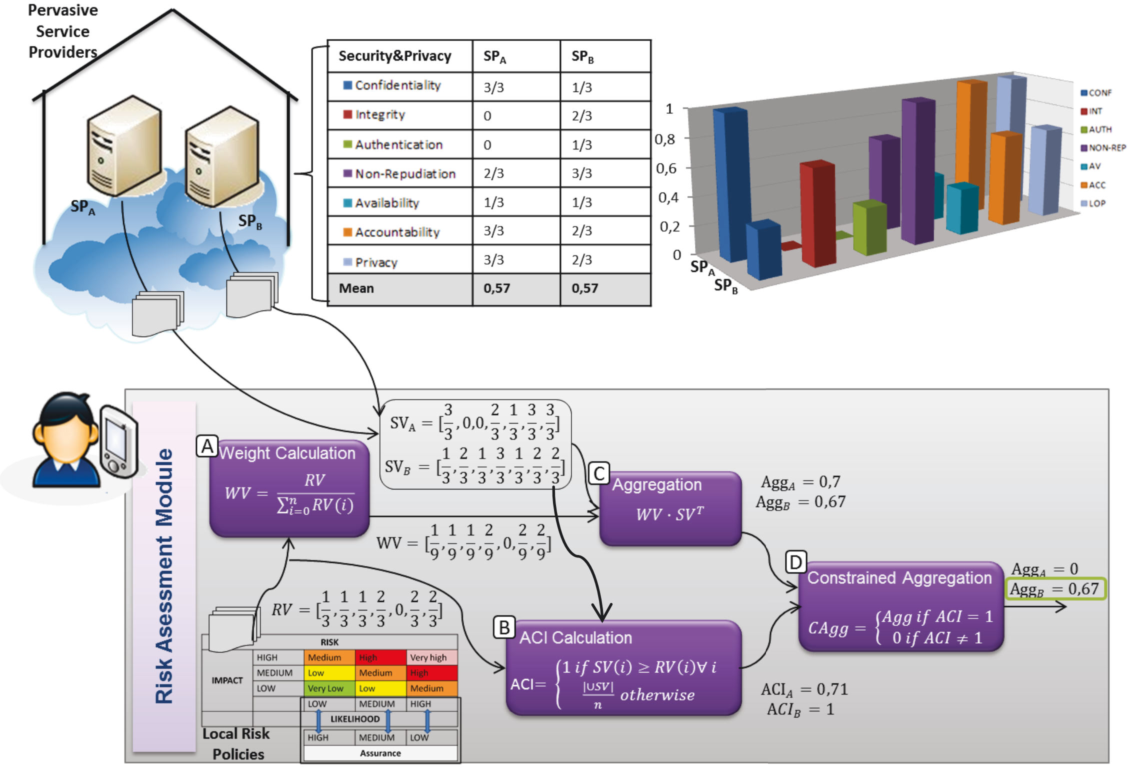
Because the obtained result is a balanced combination of the criteria, meaningful differences in partial scores might lead to erroneous assessments owing to compensation effects, which might hide relevant information in the final value. There's no guarantee that minimum requirements are satisfied with this initial approach.

To solve these issues, we designed a weighting mechanism based on reference vectors (RVs) that contain each criterion's minimum required values. RV's specific content varies by provider and depends on local risk policies. Following this vector notation, box A in Figure 3a shows how we obtain the WV using the RV as input and capturing each criterion's relative importance. For the sake of completion, we also defined the *assurance compliance index* (ACI), depicted by box B in Figure 3a.

The ACI indicates the degree of compliance with the minimum requirements; an ACI of 1 indicates that all requirements are fulfilled. Any other value gives us an idea of the degree of fulfillment of the requirements. In this last case, the ACI is computed as the number of metrics in a provider's SV that are greater than or equal to the minimum required value in the RV (denoted as |∪SV|) over the total number of metrics n. Taking the ACI into consideration, we also provide the constrained aggregated assurance value $CAgg(A)$ (see box D in Figure 3a), which discards providers that don't cover all the minimum requirements by assigning them a $CAgg(A)$ equal to 0.. On the contrary, if requirements are fulfilled, $CAgg(A)$ is equal to the global risk computed after applying the weighed summation. This final $CAgg(A)$ is the value that determines whether to accept a dynamic federation establishment.

Validation

To prove the presented ideas, we used a modular approach, implementing and testing the different parts of the architecture separately and integrated them in a fully working prototype. In our use case, we show the validation of the mathematical risk model underlying dynamic identity federation.



Pervasive Service Providers
SP_A
SP_B
1
0,8
0,6
0,4
0,2
0
SP_A
SP_B
CONF
INT
AUTH
NON-REP
AV
ACC
LOP
Risk Asessment Module
A
Weight Calculation
$WV = \frac{RV}{\sum_{i=0}^{n} RV(i)}$
$SV_A = [\frac{3}{3}, 0, 0, \frac{2}{3}, \frac{1}{3}, \frac{3}{3}, \frac{3}{3}]$
$SV_B = [\frac{1}{3}, \frac{2}{3}, \frac{1}{3}, \frac{3}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3}]$
C
Aggregation
$WV \cdot SV^T$
$Agg_A = 0,7$
$Agg_B = 0,67$
$WV = [\frac{1}{9}, \frac{1}{9}, \frac{1}{9}, \frac{2}{9}, 0, \frac{2}{9}, \frac{2}{9}]$
D
Constrained Aggregation
$CAgg = \begin{cases} Agg \text{ if } ACI = 1 \\ 0 \text{ if } ACI \neq 1 \end{cases}$
$Agg_A = 0$
$Agg_B = 0,67$
$RV = [\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{2}{3}, 0, \frac{2}{3}, \frac{2}{3}]$
B
ACI Calculation
$ACI = \begin{cases} 1 \text{ if } SV(i) \geq RV(i) \forall i \\ \frac{|\cup SV|}{n} \text{ otherwise} \end{cases}$
$ACI_A = 0,71$
$ACI_B = 1$
Local Risk Policies

Security&Privacy	SP_A	SP_B
🟦 Confidentiality	3/3	1/3
🟥 Integrity	0	2/3
🟩 Authentication	0	1/3
🟪 Non-Repudiation	2/3	3/3
🟦 Availability	1/3	1/3
🟧 Accountability	3/3	2/3
🟦 Privacy	3/3	2/3
Mean	**0,57**	**0,57**

		RISK		
IMPACT	HIGH	Medium	High	Very high
	MEDIUM	Low	Medium	High
	LOW	Very Low	Low	Medium
		LOW	MEDIUM	HIGH
		LIKELIHOOD		
		HIGH	MEDIUM	LOW
		Assurance		

Figure 3. Risk-driven provider selection. (a) The risk-driven provider selection procedure; (b) the two service providers under selection, SP A and SP B, with their metadata documents; (c) the quantitative values for the score vectors associated to SP A and SP B; and (d) provides a graphic representation of the score vectors.

Risk Evaluation

To test the risk model, we used SAML metadata documents in public repositories. We selected two providers, SP A and B, and inferred relevant risk-related features from their metadata. For simplicity, we present only the results for the security and privacy category's risk aggregation, but other criteria would be aggregated the same way.

Figure 3 shows security and privacy's risk aggregation for SP A and B both graphically and mathematically. Each subcriterion was evaluated against a four-level assurance scale ranging from 0 to 3; for example, a value of 2/3 means that the third assurance level is fulfilled. Figure 3c shows each SP's score levels, and Figure 3d shows important differences between each SP's security dimension values.

Assuming the evaluating entity—that is, the users' primary device acting as IdP—has the RV shown in Figure 3c, which leads to the associated WV, we can see that some dimensions have higher minimum assurance requirements than others. If the arithmetic mean is applied to aggregate the risk, then the two providers would have the same final security assurance value, even though they have different profiles and SP A clearly doesn't fulfill the minimum requirements. This fact is easier to understand by comparing the RV in Figure 3a with the depiction of providers' score vectors in the bar graph of Figure 3d.

If we apply the proposed aggregation formula to the weights from the RV, SP A still has better assurance than SP B. The selection of the best SP is performed correctly only after using the ACI. Thus, from this use case, we prove that the risk model fulfills the initial goal, providing a meaningful unique value that assists in automatic decision making.

Implementation Details

We developed a proof-of-concept IdM infrastructure based on open source software and worked with an SAML-based SSO scenario containing users and several providers. This infrastructure has been extended to implement the logic for dynamic identity federation. This logic modifies the original SAML flow, which directly rejects requests from unknown providers to allow real-time evaluation and decision making. The users' primary device is developed to comply with the SAML profile for mobile clients in an Android smartphone. For a richer set of IdPs, we programmed plug-ins for well-known online providers, such as Facebook. Thus, the primary device acts as both IdP and IdP proxy, letting users reuse their accounts.

Pervasive computing requires a proper IdM approach so technology can actually transcend human consciousness. In this sense, FIM has great potential to achieve this goal and has been identified as a catalyst for the next Internet marketplace revolution.[14] If realized, improved IdM can lower barriers for plug-and-play Business-to-business (**B2B**), Business-to-consumer (**B2C**), and Consumer-to-consumer **(C2C)** integration, leading to highly dynamic online business ecosystems in which users have a seamless and personalized experience.

Our proposal constitutes a new step toward better IdM in pervasive environments. So far, we've successfully evaluated the risk aggregation model and tested the feasibility of establishing federations based on one risk dimension, and we plan to implement the whole model including all the risk criteria. We also aim to conduct usability studies that involve real users as well as performance tests for measuring overhead.

Acknowledgments

We thank the anonymous reviewers for their help to improve this article. Financial support from the Spanish Ministry of Education through the program "Estancias de movilidad en el extranjero "José Castillejo" para jóvenes doctores" (CAS14/00395) is gratefully acknowledged. The Spanish Ministry of Science and Innovation under projects CONSEQUENCE (TEC2010-20572-C02-01) and EMRISCO (TEC2013-47665-C4-4-R) partially supported this work.

References

1. M. Weiser, "The Computer for the 21st Century," *Scientific Am.*, vol. 265, no. 3, 1991, pp. 94–104.
2. E. Maler and D. Reed, "The Venn of Identity: Options and Issues in Federated Identity Management," *IEEE Security & Privacy*, vol. 6, no. 2, 2008, pp. 16–23.
3. K. Cameron, "The Laws of Identity," 13 May 2005; http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.
4. R. Dhamija and L. Dusseault, "The Seven Flaws of Identity Management: Usability and Security Challenges," *IEEE Security & Privacy*, vol. 6, no. 2, 2008, pp. 24–29.
5. E. Soriano, F.J. Ballesteros, and G. Guardiola, "SHAD: A Human-Centered Security Architecture for the Plan B Operating System," *Proc. 5th IEEE Int'l Conf. Pervasive Computing and Comm.*, 2007, pp. 272–282.
6. F. Stajano, "Pico: No More Passwords!," *Security Protocols XIX*, LNCS 7114, Springer, 2011, pp. 49–81.
7. F. Almenárez et al., "fedTV: Personal Networks Federation for IdM in Mobile DTV," *IEEE Trans. Consumer Electronics*, vol. 57, no. 2, 2011, pp. 499–506.
8. F. Almenárez et al., "Trust Management for Multimedia P2P Applications in Autonomic Networking," *Ad Hoc Networks*, vol. 9, no. 4, 2011, pp. 687–697.
9. Y. Sun, Z. Han, and K.J.R. Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks," *IEEE Communications Magazine*, vol. 46, no. 2, 2008, pp. 112–119.
10. D.W. Manchala, "E-commerce Trust Metrics and Models," *IEEE Internet Computing*, vol. 4, no. 2, 2000, pp. 36–44.
11. R.L. Keeney and H. Raiffa, Decisions with Multiple Objectives: Preferences and Value Trade-Offs, Cambridge Univ., 1993.
12. P. Arias et al., "A Metric-Based Approach to Assess Risk for 'On Cloud' Federated Identity Management," *J. Network and Systems Management*, vol. 20, no. 4, 2012, pp. 513 –533.
13. T. Polk, K. McKay, and S. Chokhani, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations," special publication 800-52, revision 1, Nat'l Inst. Standards and Technology, 2014; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf.
14. W. Steigerwald, P. Scholta, and J. Abendroth, "Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems," ETSI, 2011; http://www.etsi.org/deliver/etsi_gs/INS/001_099/004/01.01.01_60/gs_ins004v010101p.pdf